Findings and Recommendations for Wireless Network Plan

Prepared for City of Palo Alto
August 2015

Columbia Telecommunications Corporation
10613 Concord Street • Kensington, MD 20895 • Tel: 301-933-1488 • Fax: 301-933-3340 • www.ctcnet.us

Contents

Figures

Tables

1 Summary of Recommendations

Working in partnership with City of Palo Alto (City) staff, CTC Technology & Energy (CTC) conducted a comprehensive analysis of the long-term needs for municipal wireless services within Palo Alto. We examined a wide range of applications that could potentially be addressed through the implementation of one or more commercial wireless technologies.

We also examined various deployment scenarios, such as blanket citywide coverage through Wi-Fi technology; expanded targeting of Wi-Fi access at and around City facilities; and dedicated projects focusing on providing priority, high-reliability services to the City's critical infrastructure operated by the City's utilities (CPAU) and public safety agencies.

We recommend that the City consider focusing on municipal wireless implementation scenarios that address specific communications needs:

- **Expand the deployment of Wi-Fi coverage to City facilities and adjoining public areas.** The City's Information Technology Department successfully deployed Wi-Fi to 30 City facilities for public and internal City use; we recommend that the City continue to deploy Wi-Fi at other City facilities including those operated by the Community Services Department, smaller City buildings, and park and recreational areas.

- **Install dedicated wireless facilities to address the needs of the City's first responders and CPAU.** To address the City's high-priority internal needs, we recommend that the City consider deploying wireless infrastructure to support enterprise applications. For CPAU, these would include real-time monitoring and control of facilities that are not part of the existing fiber-optic network (e.g., pump stations, end of line monitoring). For public safety agencies, the wireless infrastructure would support mobile and portable communications for command and patrol vehicles, as well as incident command networks in the areas where existing commercial wireless services are often saturated due to a high concentration of public users (e.g., during sporting events).

- **Consider a citywide broadband wireless network for use by the general public.** A citywide public Wi-Fi deployment is technically feasible, but *only* in concert with the deployment of a citywide fiber-to-the-premises (FTTP) network. The existing fiber-optic infrastructure operated by CPAU has neither the capacity nor the coverage area to support a citywide wireless deployment without a major expansion.

  If, on the other hand, a citywide fiber-optic network were in place, it would provide a mechanism for backhauling traffic from the individual wireless access points with transmission speeds measured in gigabits. This type of system would have the capability and coverage area to provide service competitive with existing 4G and future 5G commercial wireless networks.

It is difficult to predict what technical standards will be employed by consumer devices for wireless communications in the future. The Institute of Electrical and Electronics Engineers (IEEE) Standards organizations continue to move forward on Wi-Fi platforms to support tablets and laptops. Commercial wireless smart devices will be adhering to other standards groups in the definition of the new 5G technology. And efforts are underway to merge, or at least bond, these two initiatives.

What *is* clear is that whatever technologies are deployed for wireless access at the hardware/equipment level will have a relatively short life for each cycle of implementation (based on history, typically from five to seven years *maximum*). On the other hand, investment in core wireless infrastructure—which includes mounting locations (poles, towers), electric power, and high-capacity backhaul links for access devices—will provide a foundation for much greater longevity for supporting the continual migration of wireless technology standards for access devices. That is, access device level technology evolves so rapidly that the City can likely expect that whatever technologies it deploys will become obsolete within a few years; the long-term investment is in core wireless infrastructure.

Wireless technology is not a competitor to FTTP technology in a market such as Palo Alto; rather, they work together in partnership. Wireless provides a mobility component to the fiber-optic backbone. Fiber-optic, in turn, provides the high-capacity backhaul extension needed to create a robust, high-capacity, low-latency wireless broadband network.

2 Executive Summary

This report identifies near-term, low-risk opportunities for the City to implement wireless broadband infrastructure to provide enhanced broadband services to its citizens and to support the City's internal (enterprise) communications needs.

Working closely with City staff, CTC Technology & Energy (CTC) examined existing municipal infrastructure and resources in detail—including fiber-optic backbone network connectivity, suitable mounting locations for wireless devices, and requisite powering. We also evaluated the City's maintenance support processes and staffing. This report complements the "Fiber-to-the-Premises Master Plan" report prepared by CTC.

Through our discussions with representatives of various City departments we produced a list of potential applications that might be addressed through wireless technology.

Based on this assessment process, our experience in similar markets nationwide, and our knowledge of wireless broadband technologies, we prepared four viable scenarios for the City's consideration and potential implementation. These independent scenarios—which can be implemented singularly or in combination—address a mix of public and internal City services (including municipal operations and public safety applications):

Scenario 1: Deploy Public Wi-Fi and Secure City Enterprise Network Access at City Buildings

In this scenario, the City would deploy Wi-Fi at all City buildings, and support free public access and secure enterprise network access for City employees. This option is basically an expansion of the Information Technology Department's original deployment (30 City locations are currently being served) to include all City buildings, the airport, parks, and recreational areas.

Scenario 2: Deploy Public Wi-Fi and Secure City Enterprise Network Access Citywide

In this scenario, the City would deploy "blanket" wireless coverage for public and City users. We envision a two-phase deployment.

Phase A: Provide public Wi-Fi to core City business and residential areas

- 100 Mbps shared among all users
- 400+ wireless access points
- Light pole mounted
- Leverage existing fiber
- Wireless mesh technology

Phase B: Provide public Wi-Fi to core City business and residential areas

- 1 Gbps shared among all users
- 600+ wireless access points
- Light pole mounted
- Fiber connected to each wireless access point
- Contingent on City upgrading fiber as part of a CPAU upgrade or FTTP deployment
- Three to five years after Phase A completion

Scenario 3: Deploy a Point-to-Multipoint Network for Secure City Enterprise Access

In this scenario, the City would deploy a citywide high-reliability, dedicated, critical-infrastructure broadband wireless network to support public safety, CPAU, Department of Public Works, and Traffic Engineering needs. As in the Police Department's Mobile Emergency Operations Center (MEOC) incident deployment, City Hall would serve as the core site for a point-to-multipoint deployment. Public access would continue to be delivered by local businesses and incumbent service providers.

Scenario 4: Deploy a Citywide Mobile Data Network for Public Safety Users

In this scenario, the City would create hot spots for public safety mobile data network access to augment existing wireless operations at key facilities and routes (schools, stadiums, business areas). The hot spots would provide radial coverage to first responders and other authorized users. The City would equip its public safety vehicles with exterior mounted antennas and mobile routers capable of acting as access points. As an initial step, access points could be deployed at CPAU's nine utilities facilities to provide coverage to a significant portion of the City. The City has more than 130 locations (including traffic signals) that are suitable access points, so this scenario has great potential for phased deployment.

To create a framework for understanding the pros and cons of these four scenarios, we provide background on municipal wireless projects nationwide (Section 3), an overview of wireless network architectures (Section 4), and a discussion of Wi-Fi technology and network operations (Section 5). We then discuss the City resources available to support a wireless network deployment (Section 6) and present a summary of the high-level needs assessment we developed with City representatives (Section 7).

Next, we describe the scenarios in detail (Section 8) and include cost estimates to construct and operate each (Section 9) using currently available equipment, based on preliminary system engineering. (Scenarios selected for implementation will require additional engineering studies and contractual documents in order to proceed to implementation.) In the final section of the report, we offer insight into future wireless innovations (Section 11).

3 A Review of the Municipal Wireless Landscape

This section examines a representative sampling of wireless initiatives that have been undertaken by selected municipal governments over the past decade. In each of these case studies, the municipality has deployed wireless technology to address the public's broadband communications needs and to meet municipal telecommunications requirements.

We selected these examples to illustrate a wide range of relevant implementation strategies and approaches to charting a citywide plan for deploying wireless services.[1]

The following wireless deployments were examined:

- Brookline, MA – Citywide wireless network for public access and public safety
- Lompoc, CA – Subscriber-based municipal citywide Wi-Fi network
- Port Angeles, WA – Citywide wireless network for public access and public safety
- Ripon, CA – Citywide mobile public safety network
- San José, CA – Limited area deployment for public access with a separate traffic equipment control network
- Santa Clara, CA – Citywide wireless network for public access and city utility

3.1 Town of Brookline, MA

The Town of Brookline, Massachusetts has a population of approximately 57,700 in a land area of approximately 6.8 square miles. The Town is served by a commercial wireless provider, Galaxy Internet Systems. Under a public/private partnership agreement negotiated with Galaxy, the company built and operated a citywide wireless system to serve the dual function of providing paid Internet subscriber service as well as an independent network to support public safety.

3.1.1 System Description

The Brookline network, installed in 2007, consists of a total of 330 wireless access points and employs mesh connecting network technology. Subscriber access is provided on the 2.4 Gigahertz (GHz) unlicensed wireless band. The backhaul[2] mesh operates in the 5.8 GHz wireless band. The 4.9 GHz licensed Public Safety spectrum is used by both police and fire. The police have a total of 25 vehicles and the fire department has 12. Each public safety vehicle has mobile routing used to toggle between the 4.9 GHz network and the Verizon commercial wireless network.

[1] Note that CTC's analysis included a national review of municipal subscriber-financed citywide Wi-Fi coverage networks, and did not yield any examples of systems that were fully financed through subscriber revenues.
[2] Backhaul is the connection between a network end point and a core site.

Wireless access equipment is manufactured by Strix Systems.[3] The 330 network access units are mounted on utility poles and other similar Town-owned structures. The mounting leases are a part of the community's contribution to the partnership with Galaxy.

3.1.2 Lessons Learned

Over the approximately five years that this project has been operational the Town's public safety team has been satisfied with the performance. For over a year the system has been operating without necessary maintenance support due to the fact that the system owner (Galaxy) is in the process of closing down its operations. All indications are that the system is working to the technical standards of performance that were anticipated as a part of the design and implementation.

Unfortunately, limitations in network throughput performance based on the now obsolete IEEE 802.11a/b technologies preclude subscriber support at a level currently desired by most of the subscriber base. This is an example of a scenario in which the technology functions to its design expectation, yet fails to address rapidly increasing customer expectations. Rather than invest in an upgrade of the technology, the system owner has chosen to abandon the operation and pursue other more lucrative opportunities.

3.2 Lompoc, CA

The City of Lompoc has a population of approximately 42,000 in a land area of approximately 7.2 square miles. The city constructed its wireless system in 2006 at a capital cost of nearly $4 million. The primary purpose for constructing the system was to provide fee-based Wi-Fi services to city residents. The system also supports public safety mobile data service and utility smart meter applications.

3.2.1 System Description

The Lompoc network (Lompocnet)[4] consists of a total of 215 wireless access points and employs mesh technology. Subscriber access is provided on the 2.4 GHz unlicensed wireless band. The backhaul mesh operates in the 5 GHz wireless band. Within the mesh, an additional point-to-point backhaul network provides dedicated links interconnecting core mesh access sites. Data speeds vary based on location in the network and signal strength; speeds are typically in the 700 Kbps to 3 Mbps range. The subscriber base is approximately 1,500 users, with about 80 percent paying $15 per month and the remainder paying an hourly access fee.[5]

[3] See press release at http://www.strixsystems.com/pr2006massachusetts.aspx

[4] http://www.cityoflompoc.com/lompocnet/Information.htm

[5] http://www.MuniWireless.com/2009/02/05/up-date-on-Lompoc Network/

3.2.2 Lessons Learned

The City has moved many of its internal telecommunications services from commercial carriers to the wireless network, and uses the wireless network wherever possible. Also, new services such as video surveillance are being considered. In evaluating performance it was noted that within certain building structures the attenuation of signals from the Wi-Fi access units degraded signal performance, encouraging subscribers to install external receiving/repeater devices with the assistance of system staff.

A subscriber-financed wireless network faces heavy competition from commercial cellular carriers and fixed fiber/wire/cable television providers. The commercial carriers deliver higher-speed services over a much greater area.

Finally, the rapid changes in technology dictate the need for a proactive program to update technology to address customer needs and expectations. Historically, municipal infrastructure projects have been associated with services such as water, power and gas utilities. Telecommunications is an entirely different ball game.

3.3 Port Angeles, WA

The City of Port Angeles is located approximately 100 miles northwest of Seattle. The City is a harbor border crossing with Canada on San Juan Straights, south of Victoria, BC. The population of the city is 20,100. The City of Port Angeles, like Palo Alto, operates its own electrical utility and has a backbone fiber-optic network.

In May of 2013, Port Angeles completed a citywide broadband wireless network funded in part by a grant under the American Recovery and Reinvestment Act of 2009 (ARRA) Broadband Technology Opportunities Program (BTOP). The City received $2.6 million as a sub-grantee of the Northwest Open Access Network (NoaNet),[6] which received a total grant of $54.4 million.[7]

---

[6] NoaNet is a statewide broadband fiber optic service provider that provide whole state-wide networking services. NoaNet is owned jointing by participation municipal utilities.

[7] CTC assisted the city in developing the BTOP grant, prepared the system-level RFP to purchase the system, and provided technical oversight throughout the construction process.

Figure 1: Port Angeles, Washington – BTOP-Funded Wireless Network Project

The primary goal of the Port Angeles project was to provide high capacity, dedicated broadband wireless coverage to the City's public safety staff. A secondary objective was to provide lower-cost citywide Wi-Fi to the public, selected anchor facilities defined under the ARRA grant, and underserved Native American communities. In developing the business plan for the network, the city chose to make the Wi-Fi service available to the public on a subscription basis indirectly through the services of a third-party ISP for marketing, customer support, and Internet access.

The City's wireless network was designed for the purpose of providing mobile coverage to public safety patrol vehicles over approximately 80 percent of the City's 10.7-square-mile land area.

The network provides client (user) access through two independent wireless networks employing both the 4.9 GHz (licensed) and 2.4 GHz (unlicensed, public) wireless bands. The 4.9 GHz spectrum has been reserved by the FCC for the exclusive use of the local public safety entities and other associated agencies with a public safety focus, such as utility infrastructure.

In order to establish reliable network coverage to users throughout the City, the initial network deployment was comprised of 239 wireless access points installed at locations to maximize wireless coverage to targeted areas. Each of the access points is interconnected to the core backbone network either through direct connection to the City's broadband fiber-optic network or through a wireless mesh link.

3.3.1 System Description

The following paragraphs describe the major components used in the City's network.

3.3.1.1Wireless Access Points

All users access the Port Angeles network through one of its 239 wireless access points. Wireless links in UHF[8] and SHF[9] spectrum are used to provide a digital communications path between the user (client) and the access point. This network supports fixed and mobile users.

Dedicated radio frequency spectrum is provided in three separate bands:

1. The 4.9 GHz public safety band supports communications between public safety vehicles (e.g., police cars, fire trucks) and fixed network locations.

2. Access to the public network is in the unlicensed 2.4 GHz wireless band, which is used universally to support both business and home users through commonly available IEEE[10] 802.11n equipment. Nearly all consumer laptop computers, tablet devices and smart phones contain internal hardware and system software to operate in this band.

3. The wireless access points form a wireless mesh using the 5.8 GHz wires band, which serves as backhaul both between access points, and from the access points to the City's fiber-optic network.

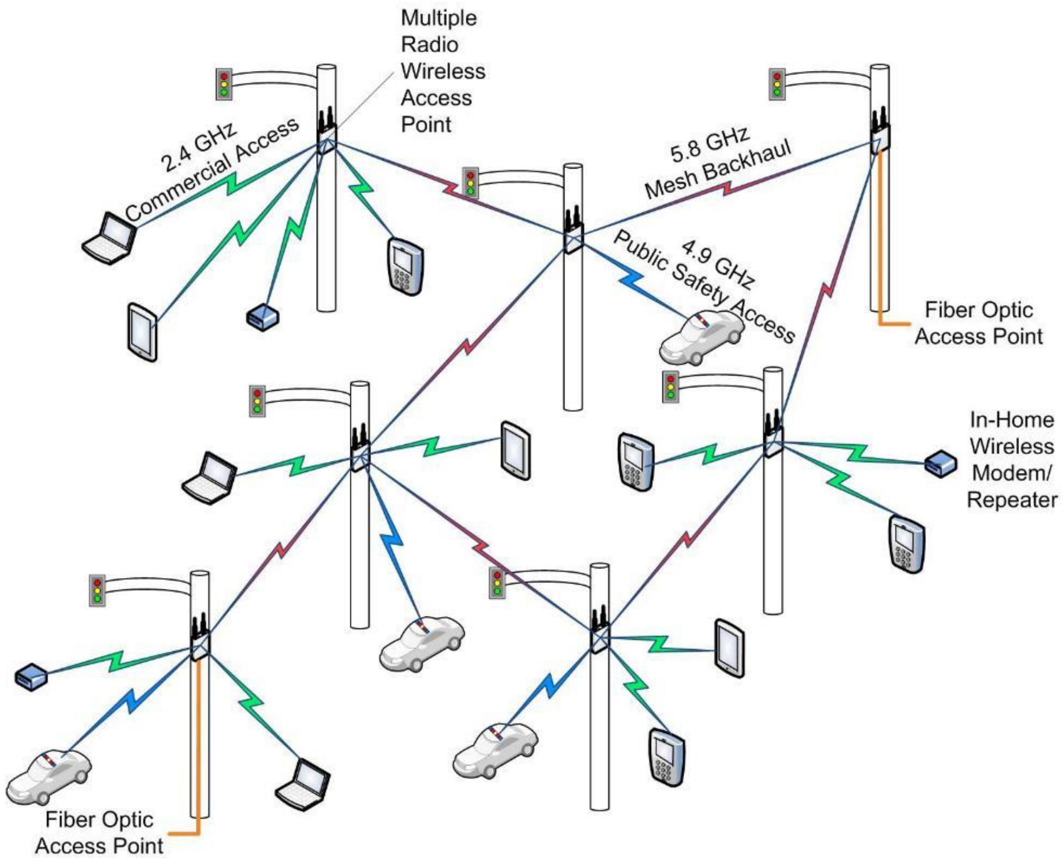
Figure 2 graphically illustrates the network operation and functionality.

[8] Ultra High Frequency (300 MHz – 3GHz)

[9] Super High Frequency (3 GHz – 30 GHz)

[10] Institute of Electronic and Electrical Engineers, Inc. is the international professional organization which has spearhead network standardization among manufacturers for more than four decades.

Figure 2: Network Overview of Port Angeles Wireless Network Infrastructure



Low-power wireless equipment available for 4.9 GHz and 2.4 GHz for this type of network deployment exhibit limited range primarily due to radio signal absorption created by structures and foliage that attenuate the direct line-of-sight radiation between network components. In general, the range of most applications is limited to the direct optical line of sight of not more than 250 to 300 feet from the access point.

In addition to the wireless links between the users and the access devices, there is an independent backhaul wireless link between the individual wireless access points and the fiber-optic network.

Figure 3 is a photograph of one of the Port Angeles wireless access points mounted on a streetlight. The majority of the access units are mounted on either streetlights or utility poles. The power to operate the unit is obtained either from the streetlight wiring or an added circuit on the utility pole. The devices are typically mounted at a nominal height of 20 feet above ground. Based on field testing, this mounting position appeared to provide the best compromise between distance coverage and providing sufficient signal in the immediate vicinity of the mounting structure. Placing access points at a higher elevation created additional interference at adjacent sites.

Figure 3: Wireless Access Point Mounted on Street Light

Figure 4 below illustrates a typical Port Angeles wireless access point. The electronic component box, on the extreme right, houses the wireless radio transmission electronics for each of the wireless bands. The vertical elements above and below the housing are antennas used to communicate with public safety vehicles and fixed commercial users. The units employ 802.11n multiple access antennas—referred to in the industry as multiple input, multiple output (MIMO) technology that continuously selects the best transmission path between the user and the access unit. The panel antennas located between the access unit and the pole are directional antennas used to communicate with adjacent access points through the 5.8 GHz wireless mesh.

Figure 4: Wireless Access Point (Detail)

Depending on the access point's physical location within the mesh network, the access unit may be connected directly to the backbone fiber-optic network. For mesh-only connected units, the physical length between hops and the number of hops varies throughout the system based on the placement of the access point and the location of existing fiber-optic interconnection points.

The City's long-term strategy to enhance network performance includes adding access points to expand the coverage area and adding fiber access points to decrease the number of hops within the network to the nearest fiber access point. The current implementation was developed as a balance to minimize construction costs and maximize service area within a constrained capital budget.

Figure 5 below is a City map illustrating the location of the wireless access points. The blue circles indicate the location of the wireless access points; the sites with the outer red circles are fiber network interconnection points.

Figure 5: Locations of Wireless Access Points in Port Angeles

The map in Figure 6 illustrates the backhaul connecting the wireless access points. It should be noted that wireless backhaul mesh is a dynamic, computer-managed infrastructure. Path routing changes in real time to maximize throughput, so Figure 6 illustrates the backhaul routing taken at a particular moment in time.

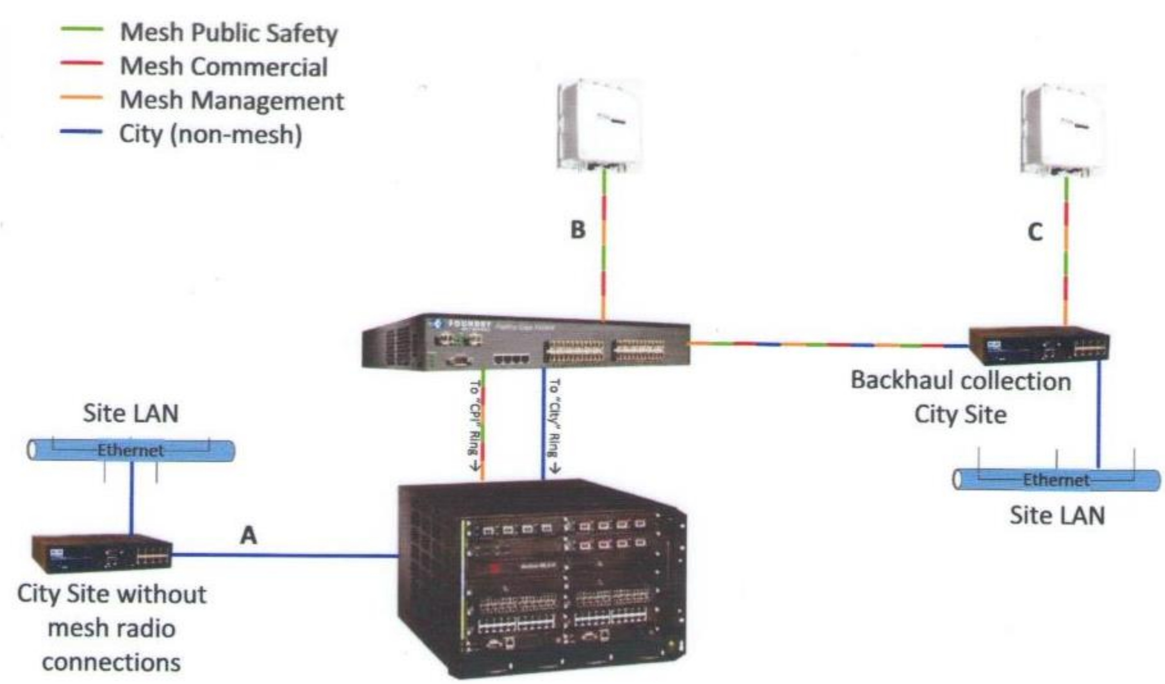
Figure 6: Backhaul for Wireless Access Points in Port Angeles

3.3.1.2 Virtual LANs and Interconnection

The individual Port Angeles wireless access points are connected to the network control center through a fiber-optic network owned and operated by the local system integrator, Capacity Provisioning Inc. (CPI). Traffic from each of the devices travels back to the facility through virtual local area network pathways, called VLANs or virtual LANs. These individual segments separate traffic between the various applications, such as public safety, public subscriber service, and network monitoring and control. This permits both the segmentation and separation of services and at the same time provides the necessary security between the individual networks. The VLAN capability will permit the public access network to provide "open access" to multiple Internet service providers (ISPs)—a requirement of the BTOP funding.

Figure 7 illustrates the VLAN concept and how it is used in the Port Angeles network. As can be seen in the figure, the green lines represent the transmission of public safety data, the red line indicates the commercial network, the yellow line identifies network management, and the blue line shows dedicated City services within the existing CPI fiber-optic network. The virtual LAN concept provides a mechanism for clearly separating individual services while multiplexing or combining on a common transmission line.

Figure 7: Functional Diagram of the VLAN Infrastructure



The CPI monitor software oversight of the instantaneous performance of any wireless system varies due to changes in path loss, traffic loading within any particular segment, and interference from other RF-emitting devices.

A real-time performance tool created by the City's contractor provides a valuable oversight mechanism for weeding out specific network problems associated with one or more of the access points; it provides network managers with the tools to tune and align components to maximize network performance. It also provides network planners with quantitative measurement for determining which locations need to be addressed with direct fiber access points as the network expands.

3.3.2 Network Operations

The public safety network is managed jointly by the City and its vendor, CPI. The public 2.4 GHz network is operated as a commercial venture with network support from CPI. The network as designed and built has the capability to support additional ISPs.

3.3.2.1 Public Access Network Specifics

The Port Angeles public network is designed to provide efficient low-cost services to the general public and commercial users. It is intended primarily as a service for home and small business applications, and is targeted toward the general public on the move.

At the time the network project was completed, only one Internet service provider, OlyPen, had entered into an agreement with the City to provide public Internet access over the network. OlyPen is an established local ISP that has provided other forms of Internet access on the Olympic Peninsula since 1996.

OlyPen's Metro-Net Mobile Service uses the network's 239 wireless access points; it is a Wi-Fi service over most of the City that is similar to the wireless hotspots available to the public in many airports, coffee shops, restaurants, and hotels.

OlyPen's Metro-Net Fixed-Point Internet service is similar to cable, DSL, and other forms of fixed broadband Internet services, in that a device commonly referred to as customer premises equipment (CPE)—in this case, an externally mounted wireless transceiver—is installed by the company at the customer's residence or business. (See Figure 8.) There is no need for a cable TV connection or telephone line to obtain a service.

Figure 8: Exterior-Mounted Customer Premises Equipment (CPE) Unit

3.3.2.2 Public Safety Network Specifics

The public safety network is focused on providing high-speed, low-cost network services to vehicles. While the wireless network provides services throughout most of the pertinent areas in Port Angeles, the high priority and on-demand service requirements of the public safety community require additional facilities to augment the wireless service.

Installed in each of the City's public safety vehicles is a mobile routing device that continuously examines signal quality from both the City's wireless network and the available commercial wireless services. The router dynamically provides the most cost-effective and reliable service by switching between the City network and the pay-as-you-go commercial network as needed.[11] (See Figure 9.)

The mobile router is an important component in the network because public safety vehicles are regularly operated outside of the City of Port Angeles. Public safety service obligations to the public do not stop at the City line—and, in fact, many of the staff are constantly traversing City boundaries.

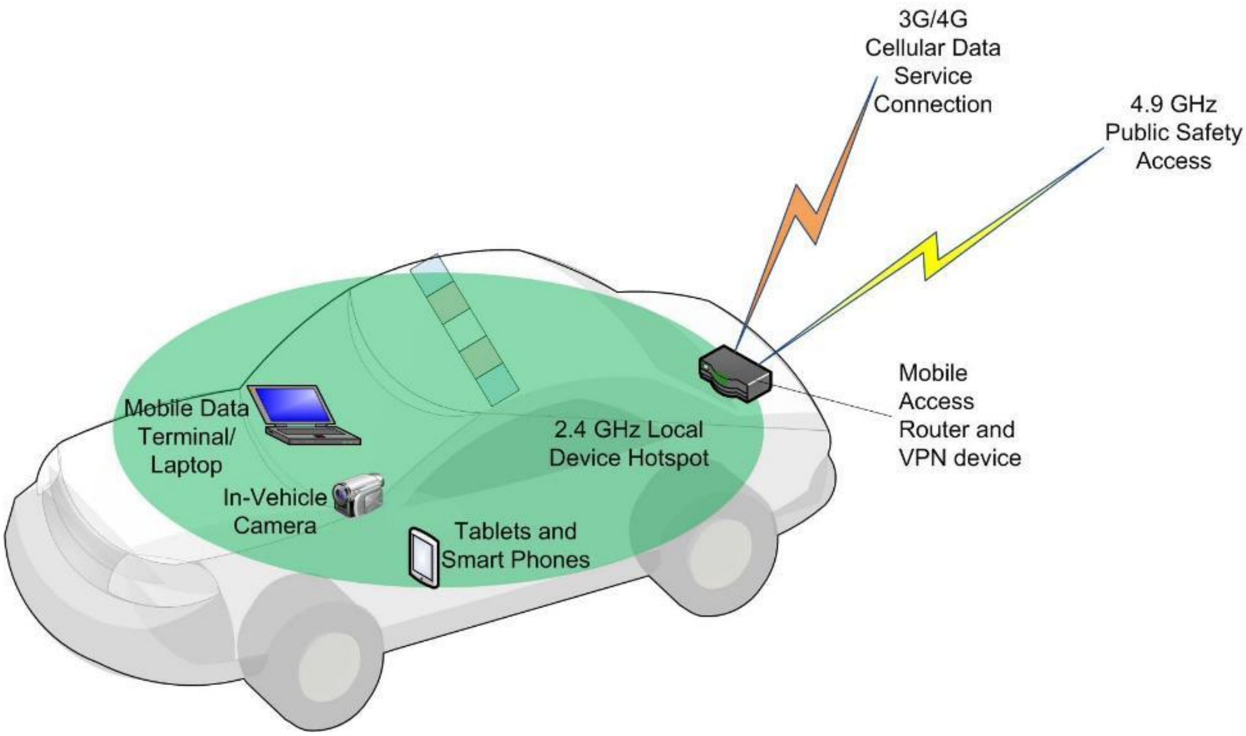
Further, there are also areas within the City where wireless coverage is not always reliable. The long-term goal for the project is to isolate and reduce the dead spot areas, through repositioning the access points or adding access points as funding permits.

Commercial 4G services are available to all public safety vehicles, patrol vehicles have a very high probability of accessing either or both the commercial services and the City wireless network. Ongoing work is focused on refining and expanding this network to improve coverage in critical areas, while the network management team's ongoing adjustment and tweaking of the internal vehicular routers aims to provide more or less continuous wireless coverage with the 4.9 GHz service to minimize access to pay-as-you-go services within the City limits.

Public safety vehicles are also equipped with a mobile router device that provides connectivity back into the Port Angeles network. The router ensures that all data between the public safety vehicle and the Port Angeles network is transmitted securely via built-in VPN.

[11] Typically wireless users on commercial networks pay a fixed fee for a defined amount of data service. Beyond that point services are paid for on a metered basis.

Figure 9: Illustration of Public Safety Mobile Router Function



Within the public safety vehicle and 100 to 200 feet from the vehicle, a secure 2.4 GHz hotspot provides connectivity to other Wi-Fi enabled devices. This hotspot can provide connectivity for mobile data terminals, laptops, in-vehicle cameras, and other network-connectable devices.

3.3.3 Lessons Learned

The Port Angeles network performance has clearly addressed the public safety users' requirements. Patrol officers routinely use the in-vehicle real-time video surveillance capability to assist officers on patrol.

The City's Information Technology department was not an active participant in the wireless project. Staff concluded that because of the manner in which the system was configured to support the public Wi-Fi implementation, the network did not provide adequate security to support critical City applications. This precludes the use of the network to support any City enterprise network and Utility SCADA requirements.

Finally, the revenues received from retail Wi-Fi users have fallen short of expectations.[12] There is a daily "free" offering that is popular and draws users. Experience to date is that the third-party commercial ISP did not aggressively pursue the retail market for consumer services. This Wi-Fi service directly competes with DSL services provided by the ISP.

[12] A specific dollar amount is not publicly available.

3.4 Ripon, California

The City of Ripon, California has a population of approximately 14,200 over a land area of approximately 5.5 square miles.

3.4.1 System Description

This Ripon system was installed to support public safety applications within the city. It was constructed in 2005 and operates in the 2.4 GHz unlicensed band. It employs proprietary Motorola Mesh electronics (a product that has been discontinued). There are a total of 52 wireless access points providing coverage over most of the city. There are a total of 81 client devices comprising a mix of mobile vehicles, video cameras, and SCADA devices. The system has been in operation for approximately 10 years.[13]

The Ripon Police Department's IT department operates the system and can support the limited maintenance that it requires. It has proved to be a valuable tool to support day-to-day public safety applications. The system relies totally on the mesh infrastructure to interconnect all the wireless access points.

3.4.2 Lessons Learned

This Ripon system was designed to serve a specific application and is maintained and operated by the user group. Public safety staff seems to be very satisfied with the overall operation. They are proposing to upgrade the system to new technology since the original system hardware vendor Motorola no longer supports this product. The 10-year lifespan goes well beyond expectations in wireless technology. This particular product represented a good mix for a relatively small community focusing on specific requirements and goals.

This an example of a successful, standalone wireless project targeted to a single user group (public safety) that is managed and operated by the user group. The equipment selected appears to have met all the design performance requirements of the users. As in many technology-based projects, simple is good.

3.5 San José, CA

The City of San José has two interesting, ongoing wireless initiatives. Recent deployment of public wireless has been installed in limited areas of the city's downtown business center for both public access and enhancements to parking.[14] Public access is also available at the convention center and the airport. This installation uses high-performance 802.11n technology

[13] Information provided by Ripon PD IT department staff

[14] Joint press release City of San José, Lenka Wright & Mark Riscaro Ruckus Wireless June 4, 2014 City expands service to SJC Airport and convention center.

A separate system is being installed for communications and control purposes with the city traffic signals.[15] This is a standalone telemetry system independent of the public access network.

3.5.1 System Description

The San Jose Wi-Fi system provides free Wi-Fi public services in limited multi-block areas in the downtown core business areas. The vendor has installed and maintains equipment serving the targeted outdoor areas, the city convention center, and the airport. The equipment used for traffic signal control is independent of the wireless network and is operated and maintained by the City's traffic engineering organization.

3.5.2 Lessons Learned

As a part of this recent downtown San Jose wireless network deployment, high-capacity IEEE 802.11n technology was installed to increase throughput performance up to 200 Mbps and expanded coverage. Wireless is a rapidly developing technology; typically new generations of equipment have a practical maximum useful life of five to seven years. This is particularly true for the access point hardware which is installed in the field. Other elements of the system such as broadband backhaul to interconnect to control centers and the physical mounting structures used for the access points have practical lives of 20 to 30 years. As has been demonstrated by the cellular industry, there is a constant need to redeploy new in-field electronic equipment to capitalize on ever-expanding throughput capacity requirements for users and address changes in communications technologies (e.g., enhanced signaling and encoding) and expanded spectrum resources resulting from FCC efforts to reclaim SHF spectrum.

Deploying separate wireless networks for public wireless access and for the traffic signal application has merit. The design for each network can be tailored to meet the specific operating requirements and performance specifications for each of these services. A single universal wireless network generally may not cost-effectively address all of the specific requirements of various user groups within the municipality. A generic area-wide backbone wireless network may have merit for certain deployments. In many cases, it unfortunately may not address all users adequately.

3.6 Santa Clara, CA

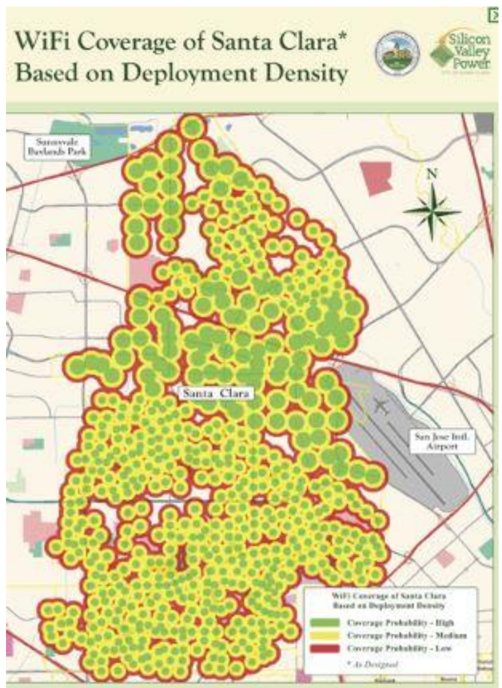
3.6.1 System Description

The Santa Clara system is a general-purpose citywide system that provides free Wi-Fi coverage to citizens and supports control monitoring functions for the city's utility. The system operated by Silicon Valley Power (SVP MeterConnect) provides coverage within the city limits over approximately 19 square miles. There are a total of 600 access points in a mesh network to

[15] Public release, Proxim wireless, Reducing congestion on the streets of San José with Wireless Traffic Control

extend the coverage of existing fiber-optic deployment. Figure 10 is a map posted on the City website showing the areas of coverage.[16] Portions of the infrastructure of the system were purchased through a distressed sale of installed assets by the city utility from a defunct commercial provider for approximately $200,000. It was upgraded and expanded in 2013 at a cost of approximately $2 million. Separate SSID accesses are available to the public, government, and public institutions. The City estimates there are approximately 5,000 unique public users. Public access is provided up to 3 Mbps.

Figure 10: SVP MeterConnect Coverage Area



3.6.2 Lessons Learned

As noted in so many systems, the public will use free Wi-Fi service on a regular basis. Santa Clara does not have a fee-based service; all public access is free. Traffic depends on a variety of factors which include speed, reliability, and other available services. The network is operated by the City municipal utility. Estimated annual operating costs, in addition to the capital cost, are approximately $200,000 per year. A substantial portion of this is mesh radio software licenses and maintenance.

For the longer term, future upgrading of the system to support newer, higher-capacity services will require a substantial investment in fiber-optic transmission plant.

---

[16] Santaclarafreewifi.com

3.7 Implications to Consider for Palo Alto Wireless Deployment

Our review of the selected municipal wireless projects provides some insight on deployment issues that might be addressed in formulating a Palo Alto wireless plan. In this review of municipal projects we focused on projects targeted to support public safety, cities with an existing fiber-optic infrastructure, and in some cases cities that operate their own electrical utility.

We note that, in the projects described above, there are several recurring findings—specifically a set of common findings within the municipal wireless community. Our industry review, while clearly limited in scope, reveals that there is a core thread that supports some rather practical, common-sense guidelines for wireless deployment:

- None of the municipal or commercial projects that we examined were able to develop a sufficient revenue stream to make the undertaking a viable business proposition. The public appears to appreciate the availability of free high-speed Wi-Fi; if you build it and give it visibility, the public will use it. For example, logins in Port Angeles increase substantially during periodic free periods. On the other hand, when the public is asked to pay for service on an ongoing or subscription basis, there appears to be a very small customer base.

  Should the City elect to move forward on deploying a subscriber-financed citywide Wi-Fi coverage model, we strongly recommend that the City first undertake a systematic consumer demand study to determine the interest in a Wi-Fi product, the performance parameters anticipated by users, and the subscription rates that users are willing to pay for the service. (We note that the City invited residents to participate in an online survey about wireless service options in July 2015; at the City's request, the results of this self-selected survey are included as Appendix D.) In our nationwide review of municipal subscriber-financed citywide Wi-Fi coverage networks, we did not find any systems that were fully financed through subscriber revenues.

- The practical deployment of Wi-Fi services requires a high-capacity connection between the access points through an expansive, dedicated high-capacity broadband backhaul network.[17] This backhaul network can use either wireless or fiber-optic technologies (and in many cases, a mix of both technologies). In Palo Alto, the existing CPAU fiber-optic infrastructure does not have sufficient citywide points of presence or the requisite capacity to support citywide implementation of a public Wi-Fi network.

[17] Backhaul networks connect wireless access points to the core network management system.

- Should the City choose to move forward on implementing citywide Wi-Fi coverage, the most cost-effective and efficient manner for deployment would be to do so in concert with an aggressive citywide fiber-optic expansion project, as set out in the city's FTTP deployment study.[18]

- Finally, a word of caution: Consumer-targeted wireless technology continues to evolve rapidly; wireless electronic equipment generally incorporates significant performance upgrades in three to five year intervals. It is difficult to predict what technical standards will be employed by consumer devices for wireless communications in the future. Any practical deployment for wireless technologies associated with consumer devices needs to take this into account. That said, investment in core wireless infrastructure—which includes mounting locations (poles, towers), electric power, and high-capacity backhaul links for access devices—will provide a foundation for much greater longevity for supporting the continual migration of wireless technology standards for consumer access devices.

  For each wireless deployment scenario, a comprehensive business plan needs to be developed for upgrading access equipment at regular intervals. In contrast, much of the core infrastructure such as the mounting structures (e.g., utility poles and streetlight poles) for the access devices, power equipment, and backhaul networks, typically will be operational for 20 to 30 years.

[18] This would entail with an estimated capital investment of approximately $77.6 million.

4 Wireless Network Architecture

Three general types of wireless topology are commonly employed in the system-level architecture of network design: (1) point-to-point communications, (2) point-to-multipoint communications, and (3) blanket (area-wide) coverage. Generally each of these technologies is used to construct wide-area municipal networks. This section examines the fundamentals of each topology and how they are implemented in practical networks.

4.1 Point-to-Point Communications Links

The point-to-point topology supports a communication link between two points. Typically this is bidirectional and is configured to support data rates, availability, and security levels required for the specific application. For wireless communications, equipment is mounted at an elevation such that there is a line-of-sight path between the two points in the network. The height of the emitting and receiving antennas needs to be at a level above ground and generally clear of trees, buildings, and other objects that might absorb or reflect radio signals along the path. Lower frequency systems operating in the 700 Megahertz (MHz) UHF range not only provide a direct signal but also can support reliable extended coverage beyond clear line of sight. New technologies such as MIMO supporting multiple antennas permit extended range through the use of multiple input and output antennas.

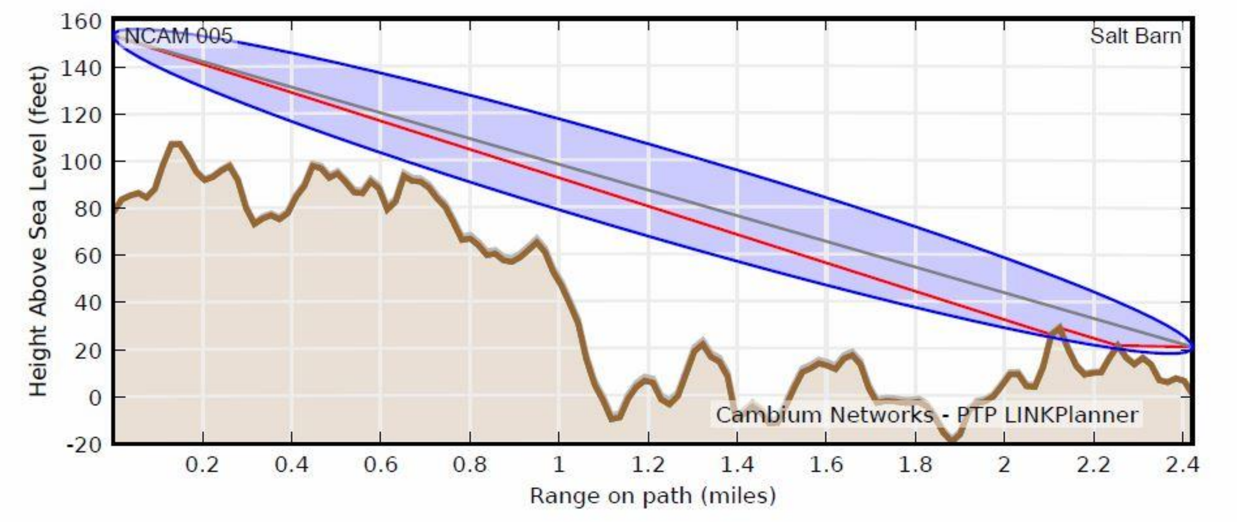
A wide variety of point-to-point products available from various manufacturers operate in both licensed and unlicensed spectrum in the 2.4 GHz to 5 GHz range; these products can support bidirectional point-to-point IP-based links and data rates in excess of 100 Mbps. These devices support full error detection and data encryption algorithms. Typically the devices include an integrated radio and antenna as a single package for mounting on buildings and towers. Many are small and can be comfortably mounted on existing urban hardware such as traffic signals, utility poles, and streetlights.

In order to support a reliable, point-to-point wireless link it is common to mount devices at elevations of 20 to 75 feet[19] above ground, positioned to avoid nearby obstructions. Depending on terrain, foliage, and other obstructions, point-to-point infrastructure will provide reliable communications links at distances up to 2.5 miles operating in spectrum from 2.4 GHz to 5 GHz. Figure 1 illustrates a simple point-to-point link connecting one fixed antenna located 70 feet above ground to a second site 20 feet above ground. This terrain profile analysis does not include amounts for clearance of buildings and vegetation; rather, it represents a starting point for an infield walkout evaluation to determine the existence of site-specific path coverage issues.

---

[19] Subject to local zoning ordinances containing restrictions and requirements on heights and mounting structures.

Figure 11: Sample Point-to-Point Link Analysis



4.2 Point-to-Multipoint Communications Links

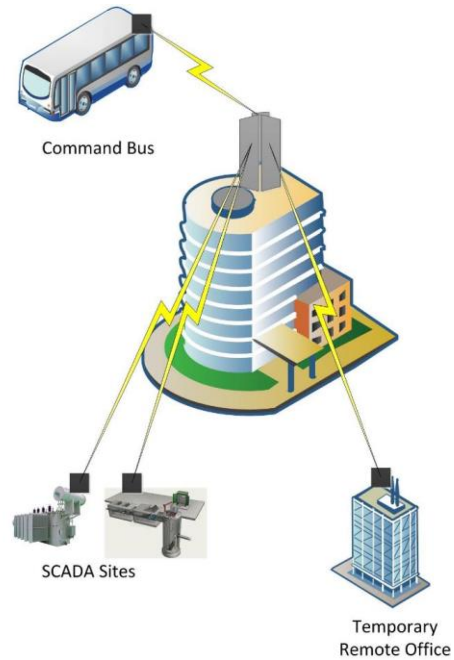
Point-to-multipoint deployments build on the point-to-point topology by adding additional sites to the network. One or more sites serve as the core site. The core or hub site is located in a position where it is able to communicate with all of the sites within the point-to-point network. All of the individual service points must be able to support a reliable point-to-point link between the hub site and the service point. This generally requires a detailed investigation to determine the most suitable location for the core hub site. Generally this is located in an elevated area, typically an existing tower, building, or other such structure that provides for the highest suitable height above the average terrain of the area encompassing all of the individual service points.

Since the hub site represents a single point of failure for the entire network, it generally includes hot standby backup core communications equipment that automatically switches an operation in the event of failure of the primary equipment. Individual site equipment installations may or may not be backed up based on network priorities. Figure 12 illustrates a typical point-to-multipoint network. Here, practical applications include communications to a parked public safety command van, links for temporary work sites or offices, and Utility SCADA sites.

The point-to-multipoint network is generally the basis for wide-area deployment. For example, if the point-to-point range between any two devices is two miles or less, the area served by a hub site would be limited to a radius of two miles from the hub site. In order to expand coverage, in areas where there exists a robust fiber-optic network infrastructure, wireless hub sites are interconnected by fiber. In Palo Alto given the existing fiber-optic infrastructure, direct fiber-optic interconnection would be the preferred option.

In situations where fiber-optic interconnection is not available the options include extended point-to-point wireless links utilizing narrow beam antennas at higher elevations or so-called mesh technologies that repeat and forward data traffic between hub sites.

Figure 12: Point-to-Multipoint Example



4.3 Blanket Coverage

Blanket coverage addresses the requirement to provide a minimum level of interference-free wireless service throughout a defined coverage area. This coverage is typical of the type of service being provided by commercial wireless carriers such as Verizon, AT&T, Sprint, and T-Mobile. The service providers place base station facilities that communicate directly with user devices (often handheld or mobile devices, in locations that vary with the time of day).

In order to provide this coverage, the commercial carriers have invested large sums of money in acquiring spectrum resources from the FCC, building towers, and developing an extensive backhaul system to integrate each of the transmission tower facilities into an area-wide network. Generally the towers are shared by the various commercial cellular providers and distributed antenna system (DAS) operators, and are often leased from companies that focus on tower facilities as revenue-producing investments.

There are alternatives to the traditional commercial wireless carriers for providing localized blanket wireless coverage. Blanket coverage networks can be installed in targeted areas and provide services within the specified areas that can rival traditional carrier 4G services in both cost and performance. This type of implementation would no doubt focus on short-range high-capacity wireless access devices located within the target service area. Most consumer devices such as tablets, smartphones, and PCs include Wi-Fi capability. Newer devices support both 2.4 GHz and 5 GHz technologies. They support data transmission rates in excess of 50 Mbps. The range of modern Wi-Fi wireless access points is typically 200 to 300 feet.

Figure 13 illustrates a conceptual approach to providing coverage within a defined area of Palo Alto's central business district. As can be seen in the figure, access devices located at intersections might be mounted either on traffic signals or on utility or light poles in the area.[20] Each access point serves a limited area and provides sufficient signal intensity to communicate with low-power mobile devices such as tablets and smartphones. Different colors for the coverage areas for each of the access points indicate differing channels for communication to minimize interference between adjacent sites and to enhance the overall capacity of the system.

In this illustration, the wireless access point provides point to multipoint infrastructure to communicate with the subscriber unit. Backhaul of information from the wireless access point would be provided via individual point-to-point fiber-optic links to a core management center. To minimize fiber deployment, optical multiplexing technologies[21] might be employed to permit the integration of the backhaul link onto individual shared fiber lines with each site utilizing differing optical wavelength.

Figure 13: Conceptual Approach to Providing Downtown Palo Alto Coverage

[20] It should be noted that while on the surface it might be a simple matter to add equipment to the traffic signal infrastructure, there are numerous, unique challenges associated with each potential access site. Planning will need to be coordinated with traffic engineers and in some cases specific locations may prove to be unusable.

[21] For this type of application, optical splitters are used to separate individual optical channels much like the travel lanes on a highway. By employing optical multiplexing the same fiber can carry the backhaul of a dozen or more sites.

5 Wi-Fi Technology

5.1 Transmission Evolution

Since its introduction in 1997, Wi-Fi technology has become synonymous with wireless Internet. The technology is based on protocols and techniques from the IEEE 802.11 standard. Standards-based technology ensures the interoperability of equipment from different vendors. The introduction of various improvements or versions of the 802.11 standard has resulted in the improvement of speeds from 2 Mbps to the 100 Mbps+ speeds that are available today in Palo Alto.

The two main unlicensed frequency bands used for municipal wireless applications are the 2.4 GHz and 5 GHz bands permitted under §15 of the FCC rules. The 5 GHz band contains three separate sub-bands (5.1 GHz, 5.3 GHz, and 5.8 GHz). There is also a separate 50 MHz allocation in the 4.9 GHz band which is reserved for licensed public safety applications. The 2.4 GHz frequency band is the most widely used, and is therefore most susceptible to interference from other devices that use the same frequency—such as Bluetooth, microwave ovens, and cordless phones. The 5 GHz band generally can support transmission rates of greater than twice as fast as 2.4 GHz, primarily due to additional spectrum bandwidth and lower interference levels employing 802.11 based network equipment. However, as distance increases, signal strength falls off more rapidly at 5 GHz than 2.4 GHz.

The original version of the 802.11 standard (802.11-1997) is now obsolete. The versions of the standard that are still in use (listed in order of evolution) include 802.11a, 802.11b, 802.11g, 802.11n, and, most recently, 802.11ac. Wi-Fi devices are certified by the Wi-Fi Alliance to operate according to one or more of these versions. Individual manufacturers often support products that in general adhere to 802.11 standards and also have proprietary aspects.

The following is a summary of the 801.11 versions used in open architecture deployment.

5.1.1 802.11a

The 802.11a version of Wi-Fi operates in the 5 GHz spectrum with a channel size (bandwidth) of 20 MHz. It was first defined in 1999 and later redefined in 2012. It uses a technique called the Orthogonal Frequency Division Multiplexing (OFDM)[22] scheme, which is also used by other technologies such as digital subscriber line (DSL), long-term evolution (LTE), and Data over Cable Service Interface Specifications (DOCSIS). It has physical layer data rates of up to 54 Mbps

[22] The OFDM scheme spreads aggregated IP traffic over a number of much smaller "channels," or subcarriers, these small channels are "orthogonal" to each other in the sense that they can be efficiently placed into much larger spectrum blocks without interfering with each other in spite of less guard spacing between them.

utilizing modulation[23] techniques such as 16 QAM[24] and Forward Error Correction (FEC) coding.[25]

5.1.2 802.11b

This version operates in the 2.4 GHz spectrum and was introduced in 2000. It uses Direct Sequence Spread Spectrum (DSSS) techniques that were previously deployed in 802.11-1997. It has a signaling data rate of up to 11 Mbps using different modulation schemes. The Complementary Code Keying (CCK) modulation is used for the 11 Mbps data rates. In the 2.4 GHz spectrum in North America there are only three standard 20 MHz channels that do not overlap with one another.

5.1.3 802.11g

Introduced in 2003, this version operates in the 2.4 GHz spectrum using OFDM, which results in higher physical layer data signaling rates of up to 54 Mbps (with 16 QAM). It uses 20 MHz channel allocation. The 802.11g standard is dynamically compatible with 802.11b. In a mixed standard environment where an 802.11b/g access point serves a client device with only 802.11b capabilities, creating compatibility could effectively lower the speed of the 802.11g network to that of the 802.11b.

5.1.4 802.11n

The 802.11n version, which was approved in 2009, operates in both the 5 GHz and 2.4 GHz bands and is able to obtain much higher data rates due to multiple factors:

- Increased channel sizes by bonding two 20 MHz channels, which nearly double the data (bps) available
- Implementing higher-order data encoding rates to 64 QAM
- Advanced antenna techniques such as multiple input, multiple output (MIMO) and beamforming. MIMO involves the splitting of data into multiples spatial streams that are

---

[23] A modulation scheme spreads data on a carrier signal by using different combinations of the amplitude and/or phase of the carrier signal.

[24] The number “X” in the X-QAM modulation refers to the number of possible combinations in the modulation scheme—the combinations of distinct types of changes in amplitude and/or phase in a signal. More speed requires higher-order modulation schemes, but higher-order schemes are more sophisticated to design and build and more sensitive to noise and imperfections in the signal. In a 256-QAM, there are 256 combinations changes in amplitude or phase. 256 is also 2^8, and 256 combinations can be depicted mathematically in the full range of combinations of eight digits of “0” or “1.” In a 256-QAM (2^8-QAM) channel of a given bandwidth, the theoretical capacity is [channel width in bps] x 8.

[25] A coding scheme determines the number of data bits versus error correction bits being transmitted within a packet.

transmitted from multiple antennas at the same time on the same frequency channel (up to four streams in the case of 802.11n).[26]

- Use of packet aggregation to improve the efficiency of the MAC layer packet transmission
- Better error correction techniques such as Low Density Parity Check (LDPC), which in turn make data transmission more spectrally efficient—that is, allows more data (bps) within the limited amount of spectrum (Hz)
- Shorter guard interval resulting in a 10 percent speed improvement

In the 5 GHz band implementation, there are nine standard 20 MHz channels in North America. 802.11n is downward compatible with other versions of the 802.11 standard and is generally the level of network implementation found in existing commercial and government enterprise networks.

5.1.5 802.11ac

The 802.11ac version was published in December 2013. It operates only in the 5 GHz spectrum band, which has greater spectrum availability (and therefore a greater number of channels) and is less susceptible to RF noise than 2.4 GHz. Physical layer data rates of up to 1.3 Gbps are possible through 802.11ac.

This throughput is achieved through the following methods, which build on 802.11n:

- Larger channel sizes by greater channel bonding up to 80 or even 160 MHz [27]
- Denser encoding schemes such as 256 QAM up from 64QAM in 802.11n
- Implementation of higher-order MIMO antennas with the availability of up to eight spatial streams
- Enhanced low-density parity check (LDPC) error-correcting codes
- Implementation of Multiuser MIMO (MU-MIMO) where a Wi-Fi access point is able to use its antennas to transmit multiple frames to different client devices, at the same time and over the same frequency channels. In contrast, 802.11n only had Single User MIMO (SU-MIMO)

---

[26] The MIMO streams travel to the receiving antennas following multiple paths. Multiple copies of the signals arrive at each antenna with slightly different timing which can be used to reinforce each other. This improves the signal to noise ratio, reliability and range.

[27] The use of 160 MHz in the United States is still under review.

- Optionally, shorter guard interval (for a 10 percent increase in speed)
- Optionally, enhanced beamforming techniques

Theoretically, a 1,300 Gbps physical layer data rate can be achieved by employing an 80 MHz bandwidth data transmission stream using 256 QAM encoding and three spatial streams at 5/6 coding.

802.11ac devices are now being introduced into the market. These are compatible with existing 802.11a/n deployments. For the 2.4 GHz band, 802.11n will continue to provide the maximum throughput.

5.2 Achievable Network Data Throughput Rates

While the standard addresses the physical layer (Layer 1) data rates for each of the versions of the 802.11 standard, the actual, practical data transmission are substantially lower than the bit transfer rates. A major part of the modifications in each version affected the physical layer while the same Media Access Control or MAC layer (Layer 2) protocol, called Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA), was in place. The MAC also uses messages called request-to-send/clear-to-send (RTS/CTS) to help avoid collisions with clients connecting with the same access point. Because of these types of overheads and the error correction required, the efficiency of the MAC layer ranges between 60 percent and 70 percent. The actual throughput available on each of these technologies is therefore 70 percent or less than of the physical layer (Layer1) data signaling rate.

As with many radio-based technologies, the external conditions (such as the line of sight and interference) greatly affect the operation of wireless devices. The effective data rates available on a wireless network are also a function of many other factors such as:

- Signal strength over noise (S/N) at the receiver or the network interface device[28]
- Signal to interference (signals in the pass-band over the internal receiver noise)[29]
- Availability of multiple channels or channel bandwidth for channel bonding

Increasing the channel bandwidth results in a reduction of the range of the system as the same transmission power is split across a larger number of subcarriers. Also, in high noise environments, a 40 MHz channel bandwidth adapts to use 20 MHz bandwidth. Higher-order modulations and coding schemes are dependent on greater signal strength for operation. This

[28] Devices employing adaptive modulation technology may operate with low S/N levels of 10 dB but to achieve full advantage of 256 QAM encoding throughput requires an additional 22 dB of signal for a 32 dB S/N (over 100 times the receiver signal level to obtain full data rate throughput).

[29] Interference from other RF energy devices (e.g., wireless access units, radar, microwaves and consumer devices).

means that the highest data rates are usually available only at close proximity to the access point where signal strength is the highest. This is considered to be adaptive modulation and coding to ensure that most optimum mode of transmission is used.

The improvement of data speeds due to MIMO is directly proportional to the number of spatial streams. But, more spatial streams require more antennas and consume additional power. Therefore, it may not be possible to implement this fully on mobile devices with limitations on hardware and power. For instance, an 802.11n radio provider may advertise 300 Mbps speed. When we examine this:

- The channel size has to be 40 MHz
- This is the data rate at the highest modulation rate; with a MAC efficiency of 60 percent of the actual throughput, the data rate will be 170 Mbps
- MIMO operation is required

Table 1 provides a simplified overview of pertinent operational parameters associated with the evolution of the 802.11 equipment used in the deployment of municipal wireless technology. The 802.11 standards are the product of more than a decade of planning, drafting, and negotiation among network architects, equipment designers, manufacturers, and government radio frequency regulators.

Table 1: 802.11 Version Summary[30]

Version	Frequency	Max Modulation Rates (Mbps)	Typical Data Rates (Mbps)[31]	Modulation	
802.11a	5 GHz	54	20	OFDM	16QAM
802.11b	2.4 GHz	11	5	DSSS	CCK
802.11g	2.4 GHz	54	20	DSSS, OFDM	16QAM
802.11n	5 or 2.4 GHz	600	170	OFDM	64QAM
802.11ac	5 GHz	1300	TBD	OFDM	256QAM

[30] IEEE Std 802.11 for wireless local area networks (WLANS) as well as enhancements to the existing medium access control (MAC) and physical layer (PHY) functions. IEEE Standards 2008-2011.
[31] Half duplex transmission rates, typical only one device is transmitting at a time using a common spectrum.

5.3 Network Security

Security is an integral component of any networking technology, including Wi-Fi. The oldest security protocol for Wi-Fi is the Wired Equivalent Privacy or WEP. It is no longer considered sufficient, but 64 bit and 128 bit WEP are still in use. The WPA protocol was introduced in 2003 with an encryption technique called TKIP. Currently, the latest version of WPA (called WPA2) is the recommended technique for Wi-Fi security along with an encryption technique called Advanced Encryption Standard (AES). There are other methods that can be used to improve Wi-Fi security such as MAC Filtering and Wireless Intrusion Protection Systems (WIPS).

5.4 Signal Propagation and Interference Rejection

The physics of radio frequency propagation results in unavoidable wireless propagation loss that is a function of distance. This ultimately results in lower speeds at the edge of an access point's coverage area due to the reduction in signal strength.

For example, 2.4 GHz UHF and particularly 5 GHz SHF networks have very limited ability to penetrate the walls of buildings and other dense objects like tree limbs, and even dense leaves. In the case of an outdoor deployment, certain types of construction such as stucco and high-efficiency windows, in particular, block signal penetration into and out of buildings. The performance of outdoor networks is impacted by vegetation, hills, buildings, building materials, and other obstructions because the UHF and SHF devices require close to line-of-sight transmission for optimum operation. A technically savvy user will tend to use and install devices in locations that minimize loss, have lower interference levels, and have multipath signals. For the casual user, reliability issues can be frustrating. (This is one good reason that a citywide Wi-Fi deployment would not be a substitute for wired Internet service in most residents' homes.)

With the ubiquity of unlicensed RF-emitting devices in homes and businesses, the environmental RF interference levels in 2.4 GHz and 5.8 GHz bands is very high. Unfortunately, the common technique used to improve the performance is increasing the number of access units, which only exacerbate the problem by increasing interference.

In the planning phase of any wireless network for a controlled area, RF spectrum analysis equipment enables the designer to discover the sources of existing interference. Interference mitigation techniques (including channel planning allocation and smart access devices that support on-the-fly, dynamic channel assignment) can be utilized to improve performance. The current 802.11n standard supports advanced techniques of mitigating interference such as antenna arrays with beamforming which enable wireless device with advanced technology to automatically detect and steer transmissions to the clearest signal path.

6 City Resources to Support Wireless Deployment

As a part of this study, we examined key elements of the existing City infrastructure to determine the feasibility of using existing City assets in whole or in part to construct wireless infrastructure. As an example, the City has more than 100 traffic signals that are connected by fiber-optics; these have the potential to form a practical foundation for mounting, powering, and interconnecting wireless access points to create a targeted blanket network in the core central business area.

In this section we examine the City's existing resources and the suitability to support wireless deployment. Resources examined include:

- Fiber-optic infrastructure
- Suitable municipal building mounts
- Street lights and traffic signal mounts
- Utility facilities (substations, towers, and similar structures)

As with any infrastructure deployment, mounting access points would require an evaluation of the impacts on City infrastructure and an awareness of potential public concerns. This includes security of facilities like electric substations; potential complications related to mounting on traffic signals; and the visual impact of new equipment on street lights and municipal buildings. It would also require sensitivity to consumers' apprehension about issues such as radiofrequency (RF) radiation in public spaces like parks.

6.1 Fiber-Optic Backbone Requirements

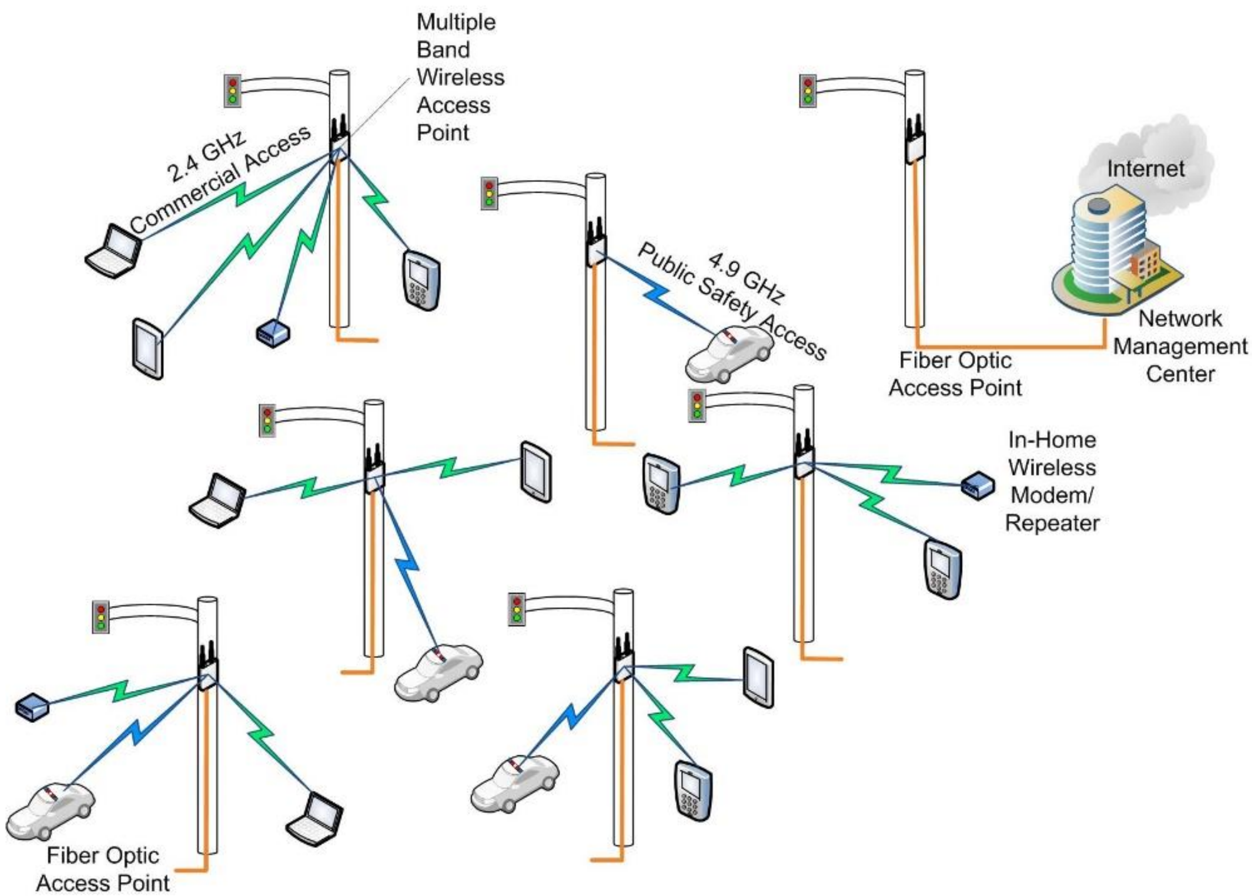
In order to implement a citywide open access Wi-Fi network, the City's wireless system will require an extensive backbone network to interconnect each of the individual access points to a central control and distribution center. Assuming that the client or user devices are typical smartphones, tablets, and laptops, the consumer access units will need to communicate with the user devices in either the 2.4 GHz or 5 GHz bands. A practical network will need to support the IEEE 802.11 standards, which encompass several iterations of changes in security, throughput, and coverage.

A typical consumer expects that a device will interconnect to the network with a minimal amount of changes in the configuration of the user device. The technology employed in Wi-Fi generally supports coverage in an outdoor environment of up to 300 feet from the wireless access point. This distance can be reduced based on a variety of factors such as foliage, interference, number of users, and the overall sensitivity and power level of the user device.

This limitation in coverage creates the need for a large number of wireless access points to cover a relatively small area. For example, a rule of thumb might be a requirement for 40 to 50 access points per square mile. Palo Alto's core residential area and commercial business zone—the area in which the majority of residents would be served—is approximately 11.5 square miles. (This excludes industrial parks and the larger Foothills preserve areas.)

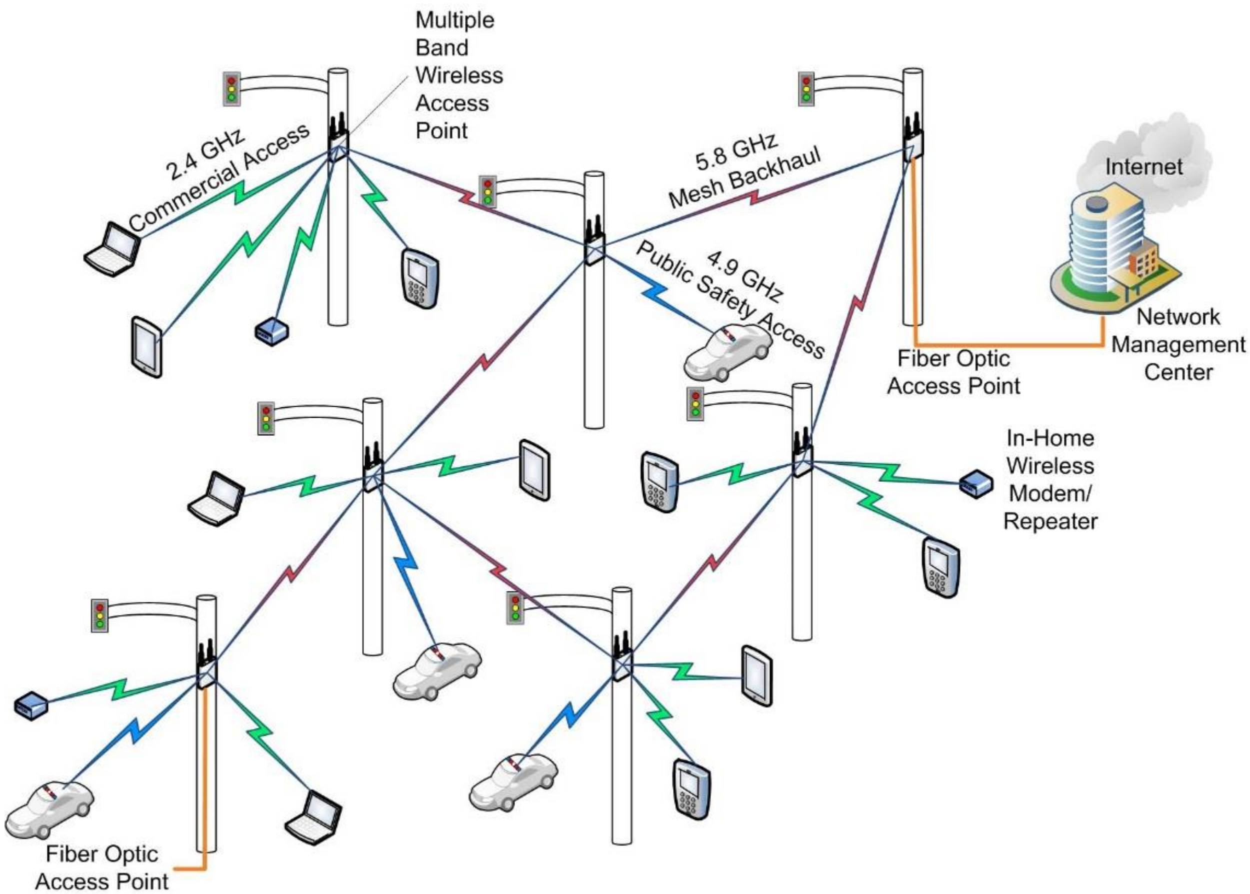
Each of the wireless access points requires connectivity back to the control or management center. There are generally two alternatives to support this so-called backhaul link. The first is to directly connect each of the hundreds of access points directly back to the center through an extensive fiber-optic network. Figure 14 illustrates a directly connected wireless network.

Figure 14: Sample Directly Connected Wireless Network



Alternatively, a hybrid connection can be developed using a mix of a limited number of fiber-optic links interconnecting a so-called mesh network that provides a wireless link between adjacent access points (Figure 15). This approach requires fewer fiber-optic links and reduces the overall capacity of the network, because the total wireless capacity is divided between services provided to the end-user and supporting the backhaul link to the control management center.

Figure 15: Sample Wireless Mesh Network



In addition, each backhaul link, often referred to as a "hop," introduces a delay in transmitting the signal from one point on the network to another. The delay, referred to as latency in the industry, reduces the overall suitability of the network to support certain key functions such as voice over IP (VoIP) and video. One other factor to consider is the fact that the equipment employing mesh technology is generally proprietary in nature, which means that the user or service provider is limited to one source for hardware and software support.

We examined the fiber backbone in the existing Palo Alto network and determined that the existing fiber infrastructure is suitable to support the deployment of the citywide fiber-optic network using mesh technology. Our review of the existing fiber infrastructure confirms that there is sufficient fiber in place that, with the addition of short fiber extensions for existing splice points, the existing fiber could enable rapid deployment of sufficient fiber-connected nodes to support mesh technology requirements established by equipment vendors. The fiber strand count is nominal and should not affect existing capacity within the fiber network to impact the Utility's dark fiber leasing business.

Our review of the fiber-optic maps indicates that in general, within one mile of any location in the City south of the Foothill Expressway, there is a fiber-optic cable suitable for interconnecting the access points with the mesh technology. Naturally, practical design would focus on strategically locating the fiber-connected nodes or access points to existing fiber-optic splice locations. For example, there is a significant availability of fiber-optic cabling along Middlefield Road that could be used to interconnect access points along this road and also to extend fiber from Middlefield Road to other parallel streets.

The capacity of wireless technology will continue to grow as more sophisticated encoding technology is brought into the open 802.11 standards or, potentially, into future standards for commercial user equipment. The FCC continues to work with the industry to expand available spectrum in both the 4 GHz and 5 GHz bands. This increase in spectrum and enhanced technology will continue to enable higher-capacity services to end-users—and in turn will necessitate construction of high-capacity fiber-optic backhaul networks to provide capacity between wireless access points and the core management system.

Should the City move forward with the FTTP initiative, consideration should be given to integrating the backhaul requirements for a modern high-capacity wireless network into the design and construction of the FTTP network. The cost to install drop connections to a wireless access point will be far lower than for the City to construct a dedicated fiber-optic backhaul network for the purposes of supporting a high-capacity wireless network.

6.2 Installation Options for Wireless Access Devices

The reliable coverage area for wireless access points operating in the unlicensed 2.4 GHz and 5 GHz bands is limited to distances of less than 300 feet when communicating with consumer-grade electronics in devices such as smartphones, tablets, and laptops. The attenuation[32] caused by buildings, trees, foliage, and weather conditions further limits service areas. There is, however, a beneficial aspect of the small service footprint. Because fewer users occupy a given service area, the access points can provide a generally high level of throughput to each user. In fact, a growing trend in the commercial wireless industry is to reduce the service size for each antenna site, because the carriers are restricted to a specific amount of RF spectrum at the user location.

In Palo Alto there is a ready supply of mounting structures suitable for mounting wireless access points. The most obvious are streetlights and traffic signals. These locations fall within the public right-of-way, generally are substantial enough to mount the small radio transceivers that communicate with the user, and have a primary power source with uninterruptable power

[32] Attenuation is a reduction of signal strength.

supply (UPS) backup for the access point equipment (usually 25 W or less). Typically, wireless access devices are mounted at an elevation of 18 to 20 feet above ground, to provide a good compromise between the users located near the device and those at the periphery (typically 300 feet from the device).

The current generation of outside wireless access units that would be used to provide blanket City coverage include integrated, weather- and environmentally protected housings and are intended to be bolted or banded to a wide range of light poles, traffic signals, and building exteriors with minimal visual clutter. Access units designed to be used for fiber backhaul applications typically have integrated antennas and are available in a form factor less than 9×9×10 inches. The weight for the entire package is less than five pounds.

Access units for mesh deployment are larger due to the additional radios within each housing. These devices have a somewhat larger form factor—typically in the 12×8×5-inch range without antennas—and weigh less than 20 pounds. Figure 16 is a photograph illustrating a typical wireless access point installation for a mesh system. (As with any installation on a pole, the City would need to calculate the acceptable load for each pole prior to installing an access point.)

Figure 16: Typical Wireless Access Point Installation for Mesh System

7 Palo Alto Requirements Analysis and Stakeholder Input

The following sections of this report analyzes and presents recommendations on the City's requirements and options for deploying wireless technology to support specific broadband communications needs identified by the project team. This analysis represents a continuation of the City's commitment to providing services to citizens and local businesses, and enhancing the communications resources supporting first responders and other City employees.

7.1 The Need for Wireless Broadband

This requirements study for wireless broadband within Palo Alto not only addresses the needs of residents, businesses, and government employees, but also examines the ever-expanding communications systems requirements of our modern society.

In general, most people are familiar with wireless networks; they connect our devices to the Internet service within our residences, and connect our voice calls to the public telephone network. In addition to these very basic functional networking services, there are an ever-expanding variety of electronic devices that require so-called machine-to-machine communications links[33] to control centers and to other equipment associated with the devices. City of Palo Alto Utilities (CPAU) is very familiar with this technology—the department long ago installed fiber-optic cabling to interconnect its command and control centers to devices that monitor and control external facilities such as power substations and water treatment plants (i.e., supervisory control and data acquisition, or "SCADA").

Typically, machine-to-machine links interconnect distributed equipment that monitor status such as temperature, water level, intrusion, or possibly fire. Alarms are detected either locally or at a core facility; supervisory personnel are alerted to the malfunction via the network. Often, the machine-to-machine links will provide sufficient information that the problem or issue can be addressed or at least mediated remotely. This saves time, staff resources, and the potential expense of dealing with major repairs caused by an inability to sense or detect abnormal operation.

As part of the requirements analysis, we examined the City's potential needs to expand wireless infrastructure—or the utilization of existing wireless communications resources—for the purpose of providing additional services to citizens, delivering public services in a more cost-effective manner, and leveraging the City's existing broadband assets. To do this, we met with representatives of departments and divisions that provide a wide range of services to City residents, including the City Manager's Office, the City's Public Safety departments (Police Department, Office of Emergency Services, and Fire Department), the Transportation Division,

[33] Often referred to as the "Internet of things."

and the Community Services, Information Technology, Utilities, Planning and Community Environment, and Public Works departments.

We also examined opportunities for providing enhanced consumer wireless services to the general public, both citywide and within targeted areas. We note that the City's Information Technology department has already taken the initiative to install modern high-capacity wireless networks within most of the City's major buildings. Modern wireless networks provide secure, user-friendly communications links to support a wide variety of smartphones, tablets, laptops, and computer peripheral devices.[34] Technologies deployed by the City's Information Technology department provide users with network transmission speeds in excess of 100 fold over earlier wireless networks.

Our findings and recommendations cover a wide range of applications and services that will advance the deployment of technology, particularly to enhance citizen services and to support the City's first responders.

In light of the City's complementary ongoing study of FTTP network deployment options, we note that the wireless broadband technology we explore in this report does not compete with fiber-optic broadband networks in complex urban environments such as Palo Alto. Rather, wireless technology supplements the City's backbone fiber assets and the services delivered over that fiber. Should the City elect to move forward on citywide deployment of a high capacity Wi-Fi service, ***a mandatory requirement will be that a citywide FTTP network*** be in place to provide backhaul links from hundreds of wireless access points to a network management and control center with eventual linking to the Internet.

By its nature, fiber-optics requires rigid or physically fixed points of attachment to a network—and transports information point-to-point. In contrast, wireless technology enables mobile networking. Mobility might involve communications with devices in motion (such as for public safety applications) or devices that need to be moved to different locations within a defined area (such as in business, or in a home where residents are using tablets or laptops).

We are increasingly becoming a mobile society when it comes to communications. Early communications systems such as the telegraph and telephone were confined to fixed points of access and termination. It is hard to believe that it has only been a few decades since consumers first had the ability to take their communications systems on the move. No doubt the traditional landline will eventually disappear from the home or office and be replaced by personal communications equipment.

[34] Consumer equipment interfaces with the City's wireless network over 2.4 GHz and 5 GHz unlicensed spectrum using the international standard IEEE 802.11 protocols. These protocols have been developed over the past two decades and continue to provide upward mobility in terms of performance, security, and overall reliability.

The requirement for portability and ability to access network resources from any location in the City is the driving force for implementing broadband wireless services. Indeed, while most Palo Alto residents acquire broadband services to their home through a physical cable (e.g., from a cable modem or fiber-optic provider), they also generally employ wireless networking technology within their premises to link all of their individual devices to the network. The same requirements noted in the consumer electronics world are also quite prevalent in both business and government work environments.

7.2 Stakeholder Input

As previously noted, we gathered insight and input from a wide range of City departments and divisions. The following sections detail the City's current uses of wireless technology and its short- and long-term needs for additional wireless infrastructure and applications. These needs (which are listed in Appendix A) inform the deployment options described in Section 8 below.

7.2.1 Information Technology

The City's Information Technology Department has completed the installation of enhanced wireless networking access equipment in 30 of the major City buildings that provides public access to citizens; the wireless access is generally available in the adjoining property areas, as well. This network supports both public access and access for authorized City staff to the City's enterprise network. Table 2 provides a list of City sites that currently have facility-wide Wi-Fi service. A total of $180,000 has been invested in constructing the 30 buildings' networks. The yearly operating cost for the service is approximately $13,500.

The buildings that currently have service display the "OverAir Wi-Fi Hotspot" emblem throughout the facility (see Figure 17). The equipment used to provide this service is consistent with the current level of technology for providing high-capacity, secure, and reliable services.

Figure 17: OverAir Wi-Fi Hotspot

As is the case with much of the equipment associated with Information Technology, there is a relatively short user technology timeframe for this wireless equipment. In other words, while the equipment may still be operational and fully functional over possibly a decade, the combination of the movement of technology to new generations of hardware, the development of new software, and the lack of cost-effective long-term support from equipment manufacturers requires fairly frequent equipment replacement cycles—typically at five- to seven-year intervals. Fortunately, this type of upgrade generally only involves the wireless access devices—hardware that is typically located in the false ceilings of buildings or other locations that are accessible to the technical support team.

The Information Technology Department also provides public Wi-Fi service on community properties associated with the City. For example, Figure 18 is a photograph of an access point located in the City Hall Plaza area. An outdoor access point device typically provides service to an area several hundred feet in diameter from the unit. Distances vary based on the equipment used, the number of other access units in the vicinity, and the end-users' devices. (Consumers' smartphones, tablets, and laptops are generally restricted in power and overall sensitivity, and hence tend to be the limiting factor with regard to overall service area associated with wireless access points.)

Figure 18: Wi-Fi Access Unit in Palo Alto

Table 2: City Sites with Facility-Wide Wi-Fi

Site Name	Address
Cogswell Plaza (outdoor)	264 Lytton Av
City Hall	250 Hamilton Av
Fire Station 1	301 Alma St
Fire Station 2	2675 Hanover St
Fire Station 3	799 Embarcadero Rd
Fire Station 4	3600 Middlefield Rd
Fire Station 5	600 Arastradero Rd
Fire Station 6	711 Serra St (Stanford)
Children’s Theater	1305 Middlefield
Art Center	1313 Newell Rd
Lucie Stern Community Center	1305 Middlefield
Junior Museum & Zoo	1451 Middlefield
Cubberley Comm Center (partial)	4000 Middlefield
Baylands Interpretive Center	2775 Embarcadero Rd
Children's Library	1275 Harriet St
Municipal Service Center - Bldg. A	3201 East Bayshore Rd
City Hall - King Plaza (outdoor)	250 Hamilton Av
Municipal Service Center - Bldg. B	3201 East Bayshore Rd
Development Center	285 Hamilton Av
Downtown Library	270 Forest Av
College Terrace Library	2300 Wellesley St
Municipal Service Center – Bldg. C	3201 East Bayshore Rd
Utilities	3241 E. Bayshore
Foothill Interpretive Center	3300 Page Mill Rd
Utilities	1005 Elwell Ct
Utilities	1007 Elwell Ct
Water Quality Control Plant	2501 Embarcadero Way

Site Name	Address
Animal Services	3281 East Bayshore Rd
Mitchell Park Library and Community Center	3800 Middlefield Rd
Main Library	1213 Newell Rd

7.2.2 Community Services

Palo Alto's Department of Community Services operates the City's community centers, parks, sports fields, and numerous specialized centers citywide. Not all of the facilities operated by Community Services have modern high-capacity wireless services like the sites listed in Table 2, which have service provided by the Information Technology Department. The Community Services staff have requested that free, open public access be installed at all of the facilities operated by the department to provide the level of services that citizens expect from Community Services.

Many of the Community Services facilities are on or near the City's existing fiber-optic network and therefore could be connected to equipment similar to that deployed in City Hall. The department staff requested that a multi-year capital program be established for implementing broadband services at all department facilities. The tables below identify the department staff's priorities for implementation.

Table 3: First-Priority Community Services Sites

Facility	Ownership	Address
Rinconada Pool	City	777 Embarcadero Road
Pearson-Arastradero Interpretive Center	City	1530 Arastradero Road
Cubberley Fields	City & PAUSD[35]	4000 Middlefield Road, T-2

Table 4: Second-Priority Community Services Sites

Facility	Ownership	Address
Municipal Golf Course	City	1875 Embarcadero Road
Baylands Athletic Center	City	1900 Geng Road, off Embarcadero
El Camino Park	City	1 El Camino Real
Greer Park	City	1098 Amarillo Street
Lytton Plaza	City	202 University Avenue
Mitchell Park	City	6 East Meadow Avenue
Rinconada Park	City	777 Embarcadero Road

[35] Joint shared use with Palo Alto Unified School District (PAUSD)

Facility	Ownership	Address
Stanford – Palo Alto Playing Fields	Stanford University	El Camino at Page Mill Road
Ventura Community Center	City	3990 Ventura Court
Baylands Nature Preserve (incl. Byxbee)	City	2775 Embarcadero Road
Esther Clark Preserve	City	Old Trace Road
Foothills Park	City	33 Page Mill Road
Pearson-Arastradero Preserve	City	Arastradero Road at Page Mill Road

Table 5: Third-Priority Community Services Sites

Facility	Ownership	Address
Bol Park	City	Laguna between Barron and Matadero avenues
Boulware Park	City	39 Fernando Avenue
Bowden Park	City	Alma Street at California Avenue
Bowling Green Park	City	474 Embarcadero Road
(Juana) Briones Park	City	Arastradero at Clemo Street
Cameron Park	City	211 Wellesley Street
Eleanor Pardee Park	City	851 Center Drive
El Palo Alto Park	City	El Camino Real at Alma Street
Heritage Park	City	Homer at Waverley
Hoover Park	City	2901 Cowper Street
Hopkins Creekside	City	Palo Alto Avenue from Emerson to Marlowe streets
Johnson Park	City	Everett and Waverley
Kellogg Park	City	Waverly at Embarcadero Road
Mayfield Park	City	23 Wellesley Street
Monroe Park	City	Monroe and Miller Avenue
Peers Park	City	1899 Park Boulevard
Ramos Park	City	8 East Meadow Avenue
Robles Park	City	4116 Park Boulevard
Scott Park	City	Scott Street at Channing Avenue
Seale Park	City	31 Stockton
Terman Park	City & PAUSD[36]	655 Arastradero Road
Wallis Park	City	Grant Avenue at Ash Street
Weisshaar Park	City	2298 Dartmouth Street
Werry Park	City	23 Dartmouth Street

[36] Joint shared use with PAUSD

7.2.3 City of Palo Alto Utilities

Palo Alto operates its own utilities, including electric, gas, water, wastewater, and fiber-optic services. City of Palo Alto Utilities (CPAU) has been a nationally recognized leader providing quality utility services to citizens and businesses since 1896.

With regard to telecommunications, the utility-deployed fiber-optic technology is a backbone transmission medium used to control and monitor critical utility infrastructure on a citywide basis. Wireless technology enables the utility to expand the reach of its fiber footprint to support a wide range of monitoring devices citywide. Wireless technology can be installed more rapidly and at a lower cost than fiber-optic technology, particularly for applications to address temporary locations or sites that are currently being supported by underperforming technology such as leased copper lines and antiquated point-to-point radio systems. It can also be used to support emerging customer monitoring and control systems associated with smart grid technology.

CPAU previously commissioned EnerNex Corporation to conduct a study of requirements for the utility to capitalize on emerging smart grid technologies.[37] One of the areas of analysis in that report focused on the need for backhaul communications capability to monitor and control field devices. Wireless technology is one of the options for backhauling information from customer premises equipment in real time to determine and control operation. In addition, in applications where the utility chooses to install equipment supporting open telecommunications architecture, a broadband wireless system might prove to be an attractive alternative.

Future planning for both wireless and fiber-optic deployment should be performed in concert because they are dependent on each other. To be effective, wireless access points need cost-effective connection points to the fiber-optic backhaul. Fiber technology can leverage the quick, low-cost deployment attributes of wireless to provide seamless network connections to support many City and commercial applications.

The utility is currently piloting several projects associated with smart grid deployment. Our review of the pilot projects indicates that the existing implementations employ proprietary telecommunications technology developed by the vendors and integrated as a part of the service packages. The systems currently under evaluation link to the pilot test area through commercial wireless services.

With regard to near-term requirements, CPAU needs to upgrade certain existing links from

[37] "Assessment of Smart Grid Applications in Palo Alto and Two-Year Smart Grid Related Work Plan for 2012 and 2013," City Council Staff Report, City of Palo Alto, Feb. 13, 2012. http://www.cityofpaloalto.org/civicax/filebank/documents/41569

legacy radio equipment and dial-up (telephone line) monitor and control equipment. The links in question include:

- Existing radio links (Foothills sites)
  - Power line monitor/closure control
  - Water utility facilities
- Four existing dial-up lines to water storage/control sites outside of fiber coverage footprint
- New SCADA telemetry monitoring and control for electrical distribution equipment (monitor end-of-line voltages, open/closure control)
  - College Avenue
  - Emerson Street
  - Other applications for future deployment include remote cameras to monitor construction areas, water levels, and general security requirements at key facilities

7.2.4 Planning and Community Environment Department – Transportation Division

The City's Transportation Division "enhances safety and mobility in Palo Alto's transportation system while protecting environmental resources and preserving the community's quality of life."[38] The Transportation Division's responsibilities range from traffic operations and parking management to public transit services and regional transportation activities.

Our discussion with Transportation Division staff indicated the need for communications network facilities beyond the areas served through fiber to connect monitoring devices associated with the deployment of new services targeted toward monitoring traffic flow, enhancing bicycle safety, and improving central city parking. Specifically, the division needs an ability to transfer information in real time from selected sites for both bicycle traffic and parking status. The communications infrastructure should enable communications from sensors located along bike paths and within designated parking areas such as city parking lots and buildings. The division's overall goals are to provide citizens with real-time information on parking status and to gather long-term data focused on enhancements to both bike paths and parking areas.

Other applications for the network are to expand the locations where traditional automobile traffic monitoring equipment can be cost-effectively installed outside the footprint of the

[38] "Transportation," City of Palo Alto website, http://www.cityofpaloalto.org/gov/depts/pln/transit/

existing fiber-optic network. These devices support the real-time monitoring of traffic counting and turning-vehicle backups, and measuring travel times and vehicle densities on given routes.

7.2.5 Public Works Department – Engineering Services Division

Public Works oversees diverse responsibilities that range from construction and maintenance of public facilities, streets, sidewalks, and storm drains to the oversight of construction work done within the City. To assist the department and this work, the ability to place video cameras for remote construction observation can facilitate oversight of both construction and project status. Strategically placed monitoring equipment will improve the efficiency of the department's inspection staff by enabling real-time status monitoring and enabling inspection staff to deal with issues as they developed. The goal here is to improve the overall efficiency of construction oversight and minimize disruption.

7.2.6 Public Safety Departments: Police Department, Office of Emergency Services, Fire Department

The City's public safety departments have requirements for citywide and adjacent jurisdictional voice and data communications services. For example, the Police Department operates the Public Safety Answering Point (PSAP) for law enforcement, Fire/ambulance, Public Works, Utilities, and Stanford University. By the very nature of public safety communications, these systems must have a high degree of availability, have a defined quality of service, be highly reliable, and function independently of commercial service demands.

In addition to traditional voice radio systems, there is an ever-growing demand (in Palo Alto and nationwide) for data communications to support first responders. This is a key driver of any wireless deployment in the City. The use of commercial cellular providers has greatly improved public safety operations for day-to-day operation. Unfortunately, during critical demand periods, the availability of such networks and overall throughput becomes limited.

While existing commercial services continue to provide new capabilities, commercial providers are not able to simultaneously meet first responder and public user demand during emergencies. When too many users (first responders and citizens) are attempting to use the same commercial communications services, those networks can become overloaded. This can also happen as a result of sheer overloading by the high density of users in a given geographical area, such as during a major sporting event or public demonstration. (During an interview, City staff provided examples of the network overload phenomena often associated with Stanford University activities.)

Congress has taken action to address public safety's unique mobile communications needs nationwide. The federal First Responder Network Authority (FirstNet), which was created by the Middle Class Tax Relief and Job Creation Act in 2012, is working with state and local governments to develop a national network to "build, operate and maintain the first high-speed, nationwide wireless broadband network dedicated to public safety."[39] We note that FirstNet is a long-term solution that will complement the City's efforts, but not replace the need to meet its own local communications requirements.

Palo Alto's first responders have taken positive steps to address deficiencies within the departments' data communications network. The Police Department is taking steps to improve overall services through the implementation of two separate initiatives.

7.2.6.1 Wireless Point-to-Multipoint Prototype

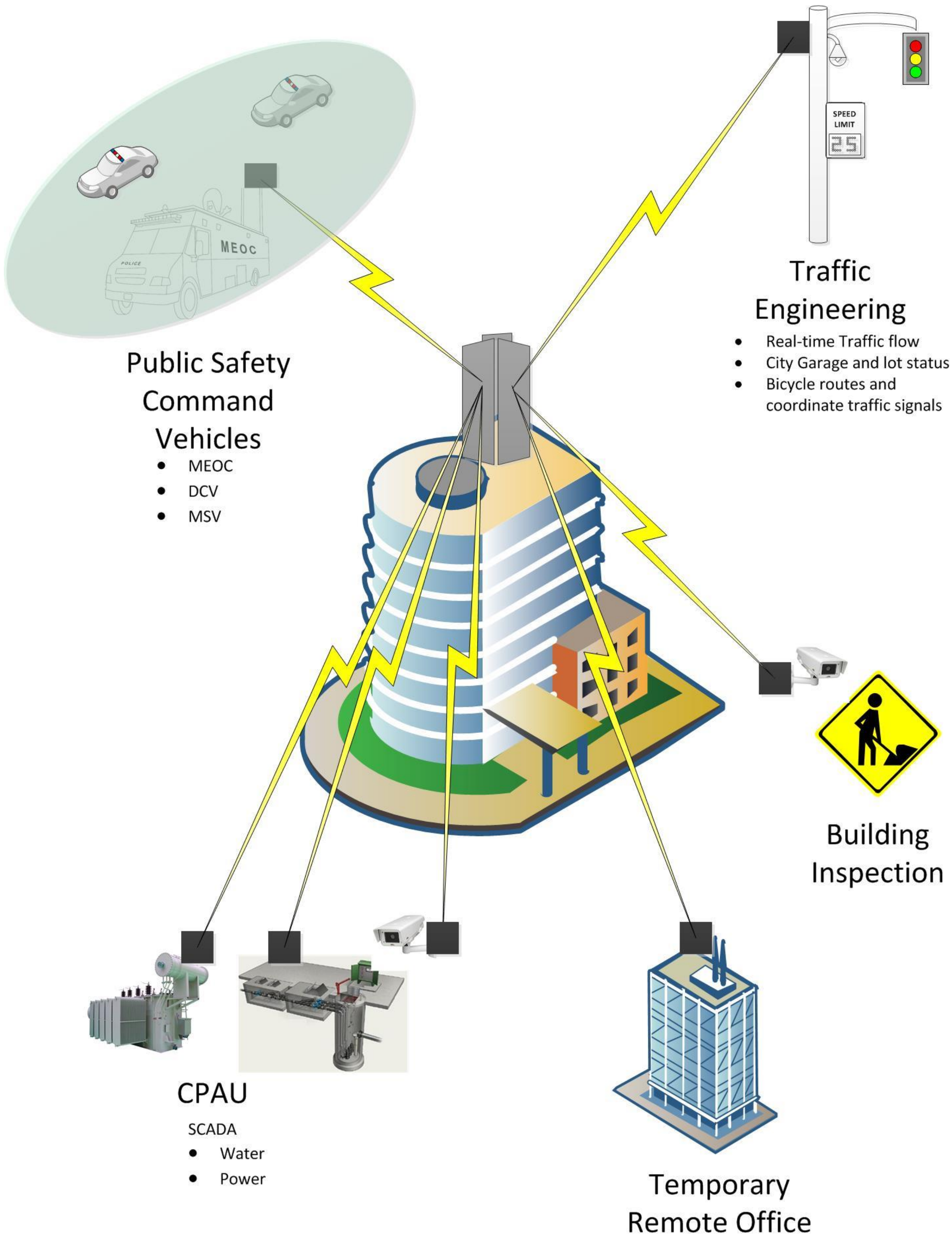
The first initiative involves the use of the public safety Mobile Emergency Operations Center (MEOC), a state-of-the-art standalone command vehicle, and several other command vehicles that are linked by a high-capacity broadband wireless network for mobile command post operation. This prototype system maintains a base station (access facility) on the City Hall rooftop, which communicates through a point-to-multipoint link to the remote vehicles within a defined arc of the city. The system, which has now been validated through field testing in operational deployment, will need to be expanded to provide 360-degree citywide coverage.

This same service can be expanded to address the point-to-multi-point requirements presented in the preceding paragraphs for CPAU, the Planning and Community Environment Department–Transportation Division, and the Public Works Department–Engineering Services Division.

Figure 19 below illustrates the operation of a core-based point-to-multipoint high-capacity broadband wireless system like the one being implemented by the Police Department.

[39] "About FirstNet," First Responder Network Authority, http://www.firstnet.gov/about

Figure 19: Private Point-to-Multipoint Wireless



This illustration includes the concept of adding other core infrastructure users to the network to expand the overall usefulness of the project to other critical service providers within the City government. For example, some of the requirements elicited from CPAU, Transportation, and Public Works can be addressed by expanding the existing network without impacting overall system capacity. Further, expansion of the existing Police network through the addition of equipment at the core City Hall site to provide solid 360-degree coverage from this location will enhance the operation not only for public safety, but additionally for other critical infrastructure operation applications.

Under the current architecture all of the core equipment is located at a single facility, which is potentially subject to failure through a building structure failure or major fire. For this type of deployment, consideration should be given to a backup or auxiliary site in the Foothills to backup or augment the single core site.

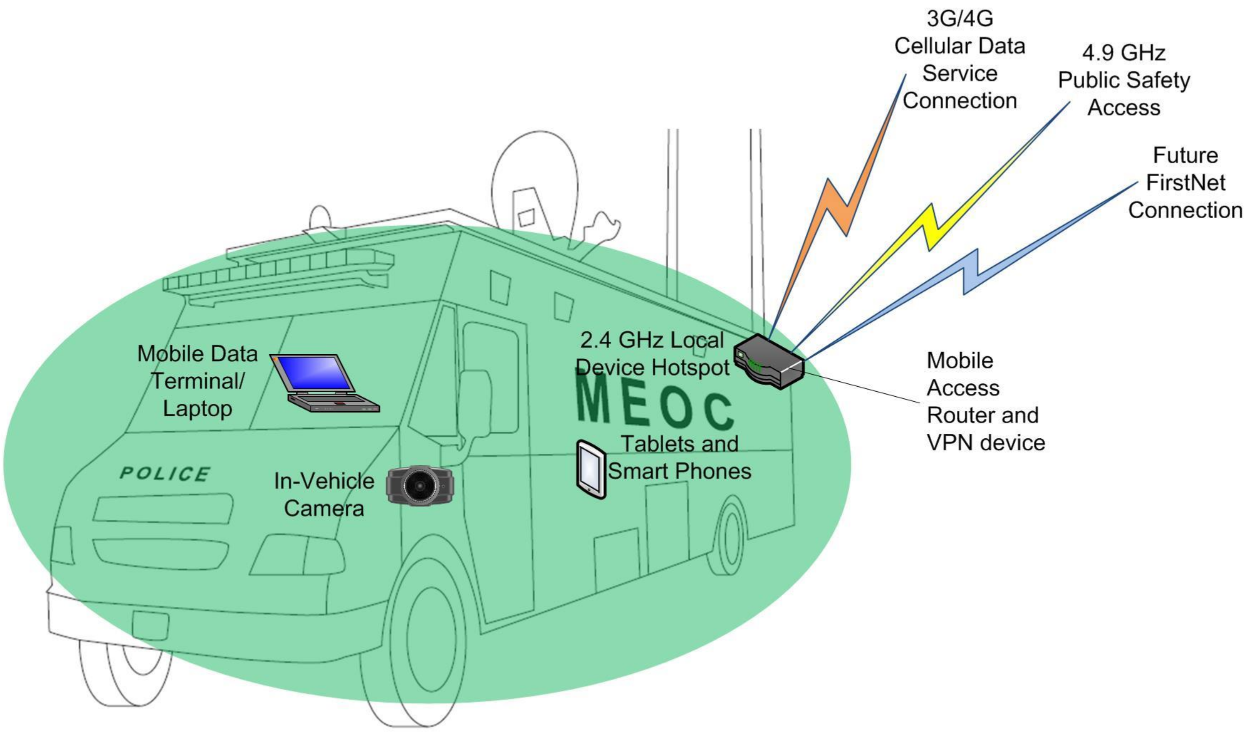
7.2.6.2 Public Safety Mobile Data Network

The City's first responders have an ever-increasing demand for information in the field, including timely access to information while traveling to an incident. Expanding requirements for video communications can and often does overload commercial networks, particularly with multiple vehicles operating on site.

In certain situations, such as parades, sporting events, and other pre-planned activities, the command vehicles can serve as an access point for interconnection to a vast array of networking resources. The Police Department has been deploying smart mobile router devices that permit the vehicles to interconnect to the most desirable network connection. Figure 20 below illustrates the overall concept.

The router can continuously monitor available networks and resources—which might include leased services from AT&T or another provider, public Wi-Fi, and other services such as the 4.9 GHz broadband services used to support the command vehicle. In the future the same device will be able to communicate with FirstNet.

Figure 20: Command Vehicle as Mobile Access Point



Over the two decades that the City's fiber network has been operating in Palo Alto, a large number of access points have been provided to support various municipal functions such as control equipment for utility operations and traffic signaling, links to public buildings, and other similar applications. These sites offer the potential for locating wireless access points to communicate exclusively with public safety vehicles supporting both Police and Fire department operations.

Another implementation scenario to consider involves deployment of access points at either critical locations within the City or along pertinent transportation routes. We anticipate that initial deployment will leverage to the maximum degree possible existing network access points. Generally we found as a part of our evaluation that existing fiber-optic broadband services for City use are located near or coincide with the areas where there is potentially the highest need for public safety support (e.g., the downtown University Avenue business area, Stanford University, and major thoroughfares).

8 Potential Palo Alto Wireless Deployment Options

Based on our research and analysis, we have developed four general options for addressing the City's communications needs with wireless broadband deployment. The scenarios are generally independent of each other and targeted to address specific needs uncovered in the requirements analysis. They are targeted toward specific user groups and areas of deployment, and offer a range of coverage opportunities (distinguishing between public and governmental access). These scenarios could be deployed singularly or in combination.

We present a system-level overview of each scenario below. We address the potential capital and operating costs for these deployment scenarios in Section 9.

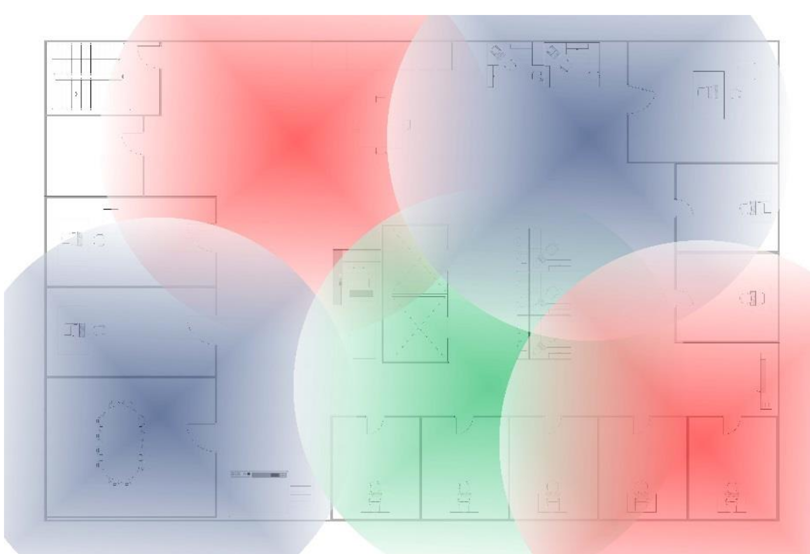
8.1 Scenario 1: Deploy Public Wi-Fi and Secure City Enterprise Network Access at City Buildings

In this scenario, the City would deploy Wi-Fi at all City buildings and support both free public access and secure enterprise network access for City employees. This option is basically a continuation of the Information Technology department's ongoing efforts at the 30 locations which are currently being served.

Residents and visitors would be able to access the network with any consumer-grade smartphone, tablet, or computer. The network would deliver state-of-the-art Gigabit service (1 Gbps) at each access point, and would be 802.11a/b/g/n/ac compatible.

The access points would be installed to serve a defined target area with a minimum signal level of -65 dBm and sufficient capacity to simultaneously serve a number of users equivalent to 70 percent of the facility's maximum capacity.

Figure 21: Wi-Fi Access in City Buildings – RF Radiation Map



8.2 Scenario 2: Deploy Public Wi-Fi and Secure City Enterprise Network Access

As in Scenario 1, the City would deploy Wi-Fi and support both free public access and secure enterprise network access for City employees. Rather than only blanketing City buildings, however, the City would make the service available either citywide or in targeted areas. This option would be more expensive to deploy, operate, and maintain than Scenario 1.

We envision a two-phase approach:

Phase A: Provide 100 Mbps blanketed public Wi-Fi to core City business and residential areas

- 400+ wireless access points
- Light pole mounted
- Leverage existing fiber
- Wireless mesh technology

Phase B: Provide 1 Gbps blanketed public Wi-Fi to core City business and residential areas

- 600+ wireless access points
- Light pole mounted
- Fiber connected to each wireless access point
- Contingent on City upgrading fiber as part of a CPAU upgrade or FTTP deployment
- Three to five years after Phase A completion

Residents and visitors would be able to access the network with any consumer-grade smartphone, tablet, or computer. The network would deliver Gigabit service at each access point, and would be 802.11a/b/g/n/ac compatible.

The access point would be installed to serve a defined target area with a minimum signal level of -85 dBm. In order to provide modern high-speed service, the access points would need to be installed at intervals of 500 feet or less within the defined coverage area. The access points would be installed to minimize visual clutter and would have backup power.

In this scenario, Palo Alto would be matching or exceeding the level of service available in many public locations nationwide. The nearby cities of Mountain View,[40] Santa Clara, and San José have implemented Wi-Fi coverage within designated areas to support access to both the public Internet and municipal communications activities. Nationally, many communities have deployed citywide Wi-Fi either under municipal funding or in partnership with a commercial provider.

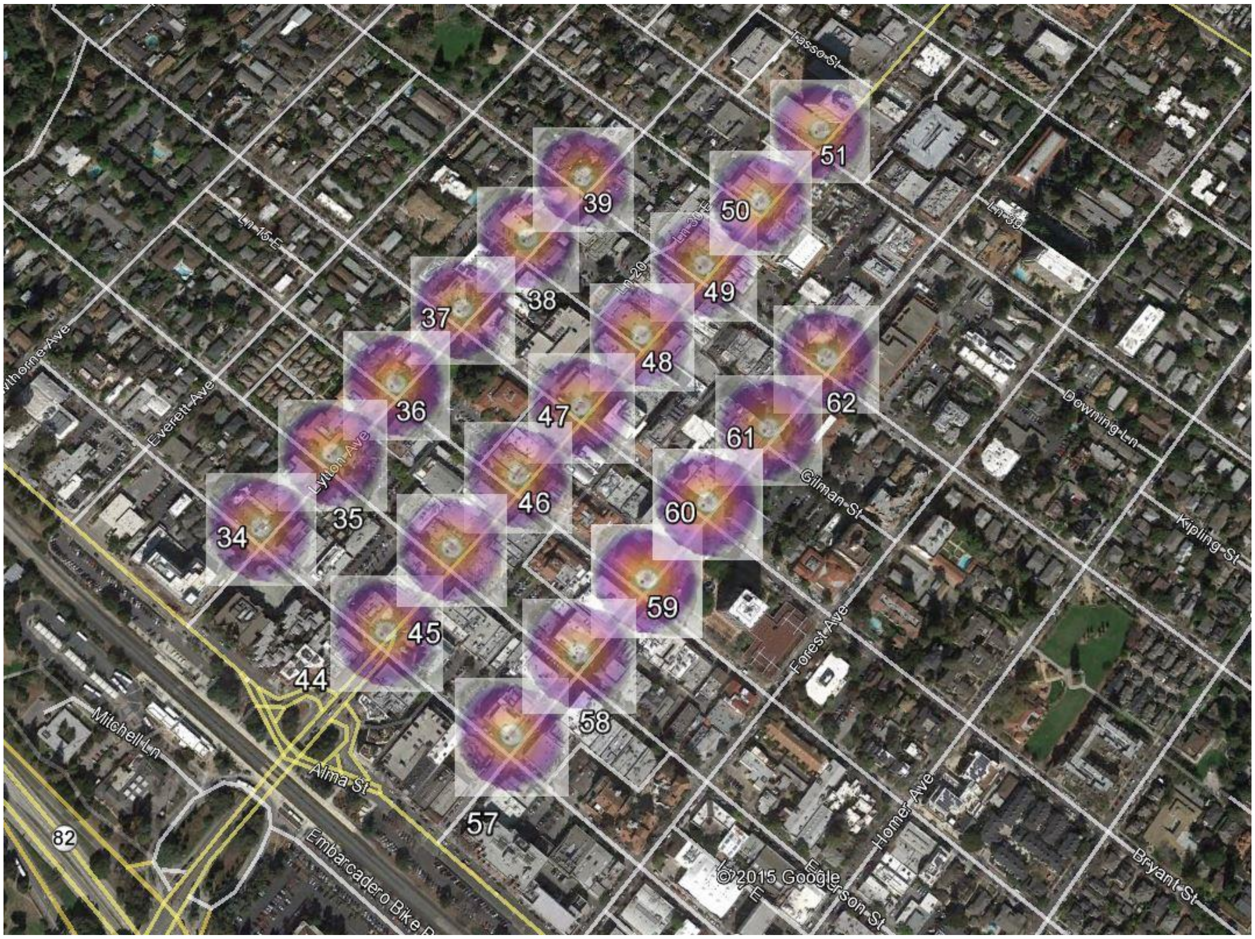
These services have generally been well received by the public—but we have been unable to find any municipal implementation projects that represent an economically viable standalone business opportunity. The public clearly will use available free Wi-Fi. However, when asked to pay for the service in a public space, many consumers have little interest. Consumers often will pay for such services in confined/restricted facilities such as on an airplane, at an airport, or in a hotel. In contrast, the blanket services often referred to as "amenity communication services" are expected to be provided free of charge.

Figure 22 illustrates how a blanket Wi-Fi network might be operated in a target location such as the central business district along University Avenue. This particular exhibit assumes placement of the wireless access points coincident with traffic signals; the City's traffic signals are connected to the backbone fiber-optic network and these locations are suitable for mounting wireless devices and interconnecting through the City's existing power/communications infrastructure. (See Section 6 for details on potential issues related to deploying access points on existing public infrastructure.)

In order to provide proper signal levels to consumer smartphones and tablets, and additionally to provide signal penetration into nearby buildings, a substantial number of access points will be required. Based on our experience in other similar communities, we estimate that the City would need 35 to 40 access points per square mile to provide adequate signal levels.

[40] For more details on Wi-Fi in Mountain View, see http://mountainview.gov/depts/it/wi_fi.asp

Figure 22: Illustration of Targeted Wi-Fi Deployment in Downtown Palo Alto



As a part of our requirements assessment, we discussed the desirability of a universal broadband wireless service with the City's Manager of Economic Development in the City Manager's office. Based on this meeting there have been no specific requests from the business community or the general public for wireless services. We note that a significant number of Palo Alto businesses offer free Wi-Fi service to patrons (see Figure 23). Additionally, broadband carriers such as Comcast and AT&T have installed and operate Wi-Fi access points for their customers in many areas of the City. (Figure 24 and Figure 25 are maps showing the locations of Comcast and AT&T Wi-Fi services in the downtown University Avenue business corridor.)

Given the availability of these services, it appears that commercial businesses are at least partially addressing the public's need for Wi-Fi access (though the City's need for wireless enterprise access remains unmet).

Figure 23: Local Businesses Offering Wi-Fi[41]

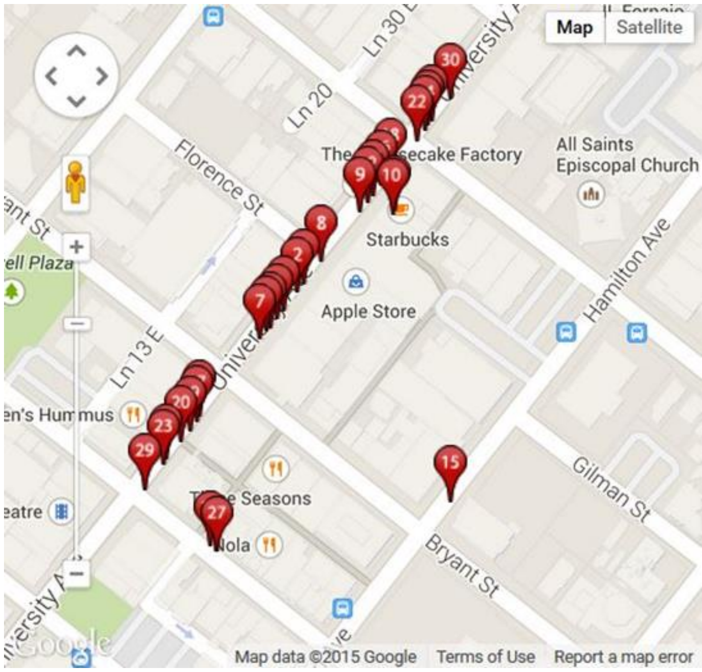
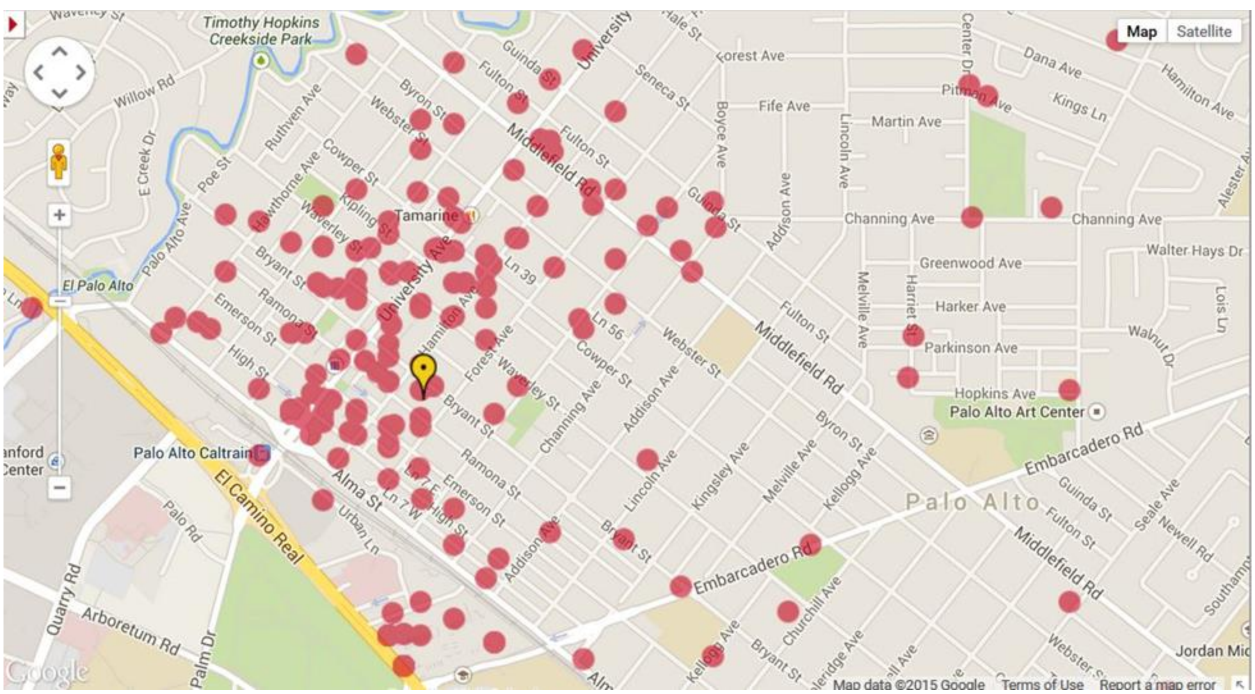
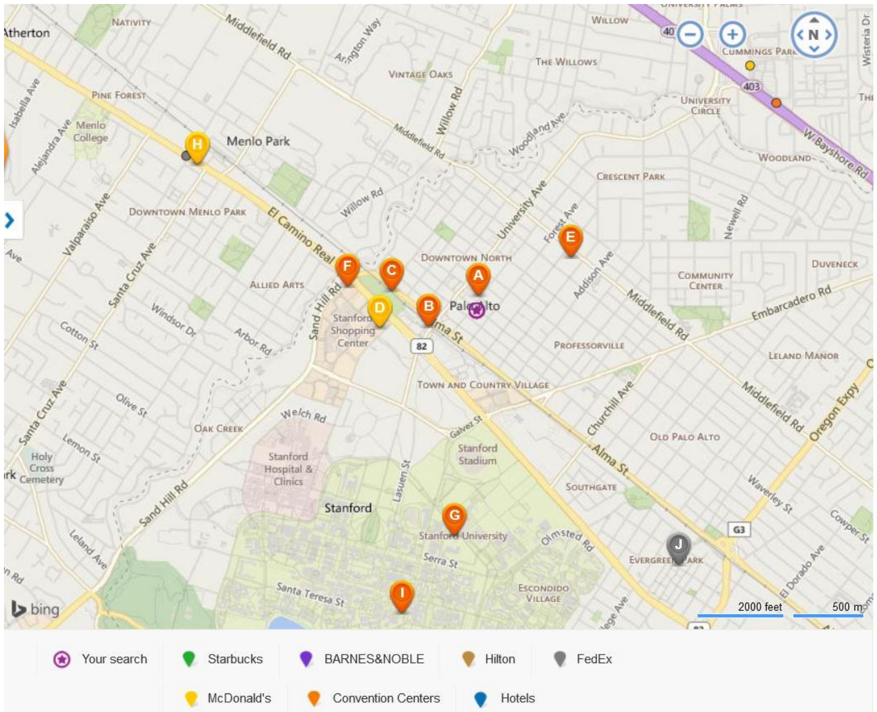


Figure 24: Comcast Wi-Fi Locations



[41] Source: www.openwifispots.com

Figure 25: AT&T Wi-Fi Locations



It should be noted, too, that other cities' implementations of municipal Wi-Fi services generally did not develop the anticipated level of acceptance. Part of the problem with those deployments related to the speed and reliability of earlier Wi-Fi technology compared to commercial wireless options. In the same timeframe that those cities implemented municipal Wi-Fi, the commercial wireless carriers successfully deployed 3G and 4G data access technologies that have developed a high degree of consumer acceptance based on cost, performance, and the convenience of essentially universal service. In contrast, many municipal Wi-Fi deployments served only a limited area—and performance in many cases fell short of user expectations as discussed earlier in the case studies in Section 2.

For the public in general, the simplicity of using a single network for voice and data has proved to be very appealing. However, with the wide deployment of smartphones and tablets, and particularly the emphasis on video and multimedia presentations, requirements for cellular capacity and bandwidth have become significant issues for users and service providers. Most cellular service providers limit the amount of data available through a basic smartphone contract. Customers that exceed the capacity limit are forced to pay extra fees for service.

Recently companies like Republic Wireless and Google have arrived at an innovative solution to address the demand issue and, at the same time, potentially reduce consumer costs.[42] The

[42] Ryan Knutson, "The Race over Wi-Fi Phones: Google learns from Republic Wireless, which is trying to turn the business on its head," *Wall Street Journal*, May 6, 2015.

concept, which is rather simple, involves using a smartphone that senses available Wi-Fi services and automatically switches away from the consumer wireless service provider networks (e.g., AT&T, Verizon, Sprint, T-Mobile) to take advantage of the free Wi-Fi connectivity. (See Section 11.2 for more details on this technology.)

Assuming this device is accepted by consumers and can move into the existing environment, it will create demand for access to high-capacity, low-latency Wi-Fi network connectivity. Indeed, Wi-Fi phones in the hands of millions of users might create a demand for a level of Wi-Fi service both in capacity and reliability that far exceeds the type of infrastructure that currently exists within the primary business areas of cities nationwide.

8.3 Scenario 3: Deploy a Point-to-Multipoint Network for Secure City Enterprise Access

In this scenario, the City would deploy limited wireless technology to meet only its internal needs; public access would continue to be delivered by local businesses and incumbent service providers (see Section 8.2).

In this scenario, as in the Police Department's current prototype, City Hall would serve as the core site for a point-to-multipoint deployment. The line-of-sight range for the wireless access would be 20 or more miles, operating on 4.9 GHz licensed public safety spectrum (see Figure 19).

Client access devices would be carrier-grade, proprietary fixed/portable equipment capable of throughput at 5 Mbps, 10, Mbps and 100 Mbps. Typical performance characteristics for a point-to-multipoint deployment would include:

- Vendor proprietary MIMO protocol
- Adaptive modulation
- Maximum latency of 5 msec.
- Four to six sector antennas and core
- 125 Mbps /sector
- 5/10/20 MHz channel
- GPS synchronization
- Guaranteed Quality of Service

8.4 Scenario 4: Deploy a Citywide Mobile Data Network for Public Safety Users

In this scenario, the City would create hot spots for public safety mobile data network access. The hot spots would provide radial coverage to first responders and other authorized users over a distance of 1,000 to 1,500 feet. As an initial step, access points could be deployed at

CPAU's facilities (see Figure 26 below) to create eight hot spots and provide coverage to a significant portion of the City.

These access points would operate on 4.9 GHz licensed public safety spectrum using 802.11a technology. The targeted performance levels would be a minimum 54 Mbps @ -84 dBm and a minimum 6 Mbps @ -94 dBm. Mesh functionality would be an option.

The City would equip its public safety vehicles with exterior mounted antennas and mobile routers capable of acting as access points with a minimum 27 dBm signal.

Figure 26: Illustration of Public Safety Mobile Network Deployment

In addition to the CPAU facilities, however, the City has more than 130 locations (including traffic signals) that currently have fiber network access, power, and mounting structures—and that are suitable access points for supporting connectivity to mobile public safety vehicles (see Figure 27 below). This scenario, then, has great potential for phased deployment. Depending on the City's needs and budget, the next phases of deployment could be either at fixed points (e.g., Stanford Stadium) or along priority routes (e.g., University Avenue).

This option for wireless deployment would directly address the Police Department's needs for reliable communications citywide, and would eliminate the conflict between first responder communications and public communications during emergencies or large events. This deployment would also help cover areas of Palo Alto where the incumbent cellular provider has insufficient coverage.

Figure 27: Candidate Access Points for Public Safety Mobile Data Network

9 System-Level Design and Cost Estimates for Wireless Deployment Scenarios

In this section we review the user requirements determined as a part of our user assessment and present a preliminary system-level engineering design and cost estimate for implementing each of the four scenarios developed. We assume that these representative designs will undergo a detailed final review as a part of the City's evaluation of this report by participating departments. These designs were developed to provide decision-makers with a baseline of potential costs, a definition of services provided in each scenario, and a list of anticipated benefits from the implementation.

In preparing these estimates we have worked closely with City staff to draw from internal databases and the expertise of the staff. Once a decision has been made regarding which projects or scenarios are to be implemented, a more detailed study or review of the basic data will be required, along with the preparation of a bid request to identify a qualified system integrator to construct the selected systems.

9.1 Scenario 1

This scenario presents a strategy to implement both public wireless access and secure enterprise network access for City employees at City facilities. This option represents a continuation of the Information Technology department's ongoing efforts at many City locations. The capital amount required for deployment at additional City sites will depend on the number of sites, and will presumably be comparable to the City's costs for its previous deployments at major City buildings.

This model assumes that the City would systematically deploy Wi-Fi at all City buildings, and would provide both free public access and secure enterprise network access for City employees. The access points would be installed to serve a defined target area with a minimum signal level of -65 dBm and sufficient capacity to simultaneously serve a number of users, equivalent to 70 percent of the facility's maximum capacity. The wireless access would also extend outside of buildings to a limited area in the vicinity.

9.2 Scenario 2, Phase A

This scenario presents a strategy to implement public wireless coverage citywide or in defined areas using 802.11g/n technology. This is a near-term implementation scenario, utilizing to the maximum extent existing fiber infrastructure. It can be deployed as an initial implementation strategy to meet citywide coverage goals. The subsequent upgrade (defined in Scenario 2, Phase B) can be implemented to increase throughput and be integrated into future FTTP deployments.

9.2.1 Basic Assumptions

This model assumes that the existing City infrastructure will be used to deploy this network to the maximum extent possible. Specifically, fiber-optic backbone cable will be connected at strategic locations using existing fiber splice points. The number of connections to the fiber backbone will be determined on a cost basis. Mesh technology will be employed to interconnect access points that are not directly fiber connected. There will be a ratio of greater than or equal to 9 to 1 of unconnected to connected access points.

All access points will be mounted on existing city-owned light poles, traffic signals, or other similar structures that permit mounting at a level of approximately 20 feet above ground and have existing AC power.

The system will be constructed to meet performance specifications under IEEE 802.11 g/n. The estimated useful life for this technology is five years.

For the purpose of equipment replacement it is assumed that the useful life for any electronic equipment is seven years or less. Fiber-optic cabling, access points mounting equipment, and hardware has a useful life of 30 years.

For purposes of this estimate we assume a coverage area of 11.5 square miles. This is our estimate of the area containing most of the City's contiguous residential neighborhoods and commercial business areas. It excludes park and preserve areas west of the City proper in the foothills and the large commercial corporate office parks. Coverage signal intensity is targeted to support smartphones, tablets, and laptops within the 11.5-square-mile service area. Due to the high density of large trees in residential areas, reliable in-building service may require users to install external receiving equipment with regeneration capability within the structure.

This network will support client equipment operating in the 2.4 GHz and 5 GHz unlicensed Wi-Fi bands.

9.2.2 Financial Summary

We estimate the capital cost to construct the infrastructure for this deployment to be approximately $4.7 million, and the yearly operating expenses to be $600,000 (assuming operation on a subscription basis at $20 per month, with a minimum of 2,550 customers).[43] Full financial projections for this scenario are included in Appendix B.

The table below provides a summary of projected capital costs for this scenario.

[43] Note that in our review of the Wi-Fi industry, we have found no systems in any similar markets that have achieved this level of subscriber penetration.

Table 6: Scenario 2-A Financial Summary (Capital Costs)

Item	Cost
Fiber Access Points	$2,645,000
Backup power	$345,000
Fiber Core Electronics	$55,500
Fiber to splice (new)	$502,500
Installation	$728,750
Engineering & Oversight	$384,910
Total	*$4,661,660*

9.3 Scenario 2, Phase B

This scenario presents an implementation strategy to implement public wireless coverage citywide or in defined areas using 802.11ac technology. This is a longer-term implementation scenario, utilizing a new fiber-optic-based backhaul network to link each access point to the core network, capable of supporting gigabit throughput to each access point.

In Palo Alto, the existing CPAU fiber-optic infrastructure does not have sufficient citywide area coverage, points of presence, or capacity to support citywide implementation of a public Wi-Fi network. A backhaul network to support this topology would be required to connect to wireless access points with a spacing between sites of 1,000 feet or less. This scenario is feasible only with the complementary deployment of a citywide fiber network, which has a projected cost of approximately $77.6 million.

9.3.1 Basic Assumptions

We assume a new backhaul infrastructure will be used to deploy this network to the maximum extent possible. Specifically, fiber-optic backbone cable will be connected to each access point. This cost estimate assumes that the fiber attachment (drop) cost will be the same as attaching a residential subscriber to an FTTP network.

As in the case of Phase A, all access points will be mounted on existing City-owned light poles, traffic signals, or other similar structures that permit mounting at a level of approximately 20 feet above ground and have existing AC power.[44]

The system will be constructed to meet performance specifications under IEEE 802.11 ac. The estimated useful life for this technology is five years.

[44] As we note in Section 5, mounting access points would require an evaluation of the impacts on City infrastructure—including potential complications related to mounting on traffic signals and the visual impact of new equipment on street lights and municipal buildings.

For the purpose of equipment replacement it is assumed that the useful life for any electronic equipment is seven years or less. Fiber-optic cabling, access points mounting equipment and hardware all have a useful life of 30 years.

For purposes of this estimate we assume the coverage area to be 11.5 square miles. This is our estimate of the area containing most of the City's contiguous residential neighborhoods and commercial business areas. It excludes park and preserve areas west of the City proper in the foothills and the large commercial corporate office parks. Coverage signal intensity is targeted to support smartphones, tablets, and laptops within the 11.5-square-mile service area. Due to the high density of large trees in residential areas, reliable in-building service may require users to install external receiving equipment with regeneration capability within the structure.

This network will support client equipment operating in the 2.4 GHz and 5 GHz unlicensed Wi-Fi bands.

9.3.2 Financial Summary

We estimate the capital cost to construct the infrastructure for this deployment to be approximately $3.3 million, and the yearly operating expenses to be $433,000 (assuming operation on a subscription basis at $20 per month, with a minimum of 1,880 customers). Full financial projections for this scenario are included in Appendix C. The table below provides a summary of projected capital costs for this scenario.

Table 7: Scenario 2-B Financial Summary (Capital Costs)

Item	Cost
Fiber Access drops	$1,495,000
Backup power	$345,000
Fiber Core Electronics	$155,500
Fiber drops	$287,500
Installation	$743,750
Engineering & Oversight	$272,410
Total	*$3,299,160*

9.4 Scenario 3

This scenario presents an implementation strategy to create high-capacity point-to-multipoint broadband wireless coverage citywide for Public Safety, Utilities, Public Works, and Traffic engineering users. This scenario would use a primary core site at City Hall and a new backup core site to support the most critical sites (redundantly) at a to-be-determined site in the Foothills preserve area.

9.4.1 Basic Assumptions

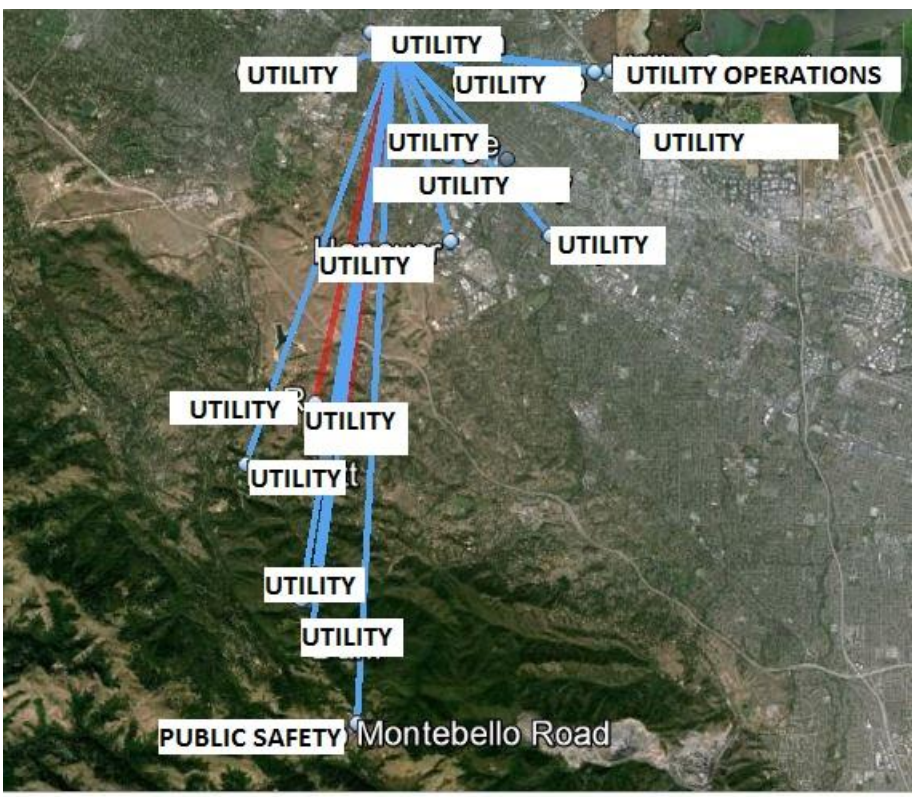
This model assumes that services will be obtained through a line-of-sight path between the core sites (City Hall and Foothills site). Multi-sector antennas will be installed all at all core sites with 90-degree sectors providing a minimum throughput of 100 Mbps/ sector.

Sites to be served include:

- Mobile public safety command vehicles
- All Police/Fire radio sites
- Utilities facilities
- Utilities facilities not connected to fiber-optic network
- Selected Traffic engineering sites
- Portable Public Works camera sites

Figure 28 shows the locations of some key fixed sites assumed for the network to prepare this estimate. The map will be expanded if the scenario is proposed for implementation and the backup site location is selected.

Figure 28: Point-to-Point Links (Scenario 3)



9.4.2 Financial Summary

Table 8 provides a summary of parameters and projected capital costs for this scenario. It is anticipated that the annual operational cost to support this scenario will be low. Staffing will be supported by Public Safety and Utilities as a minor add-on to their current operation of radio, fiber-optic, and other communications equipment. Hardware maintenance will likely be outsourced to equipment manufacturers/vendors. For this scenario we estimate a maximum annual expenditure of $10,000 with a useful equipment life of seven to 10 years.

Table 8: Scenario 3 Financial Summary (Capital Costs)

Parameters	
Core Sites	2
Client sites	30
Capital Costs	
Base Stations (2)	$190,000
Client Access Units	$45,000
Installation	$25,000
Engineering and Oversight	$25,000
Core Site Network Integration	$85,000
Total	*$370,000*

9.5 Scenario 4

This scenario presents an implementation strategy to create wireless coverage citywide for public safety vehicles at key City locations and along predefined routes. The initial deployment includes vehicle router equipment to interface with commercial cellular networks, 4.9 GHz equipment, and future FirstNet deployments. For planning purposes, a fleet deployment of 50 vehicles is assumed.

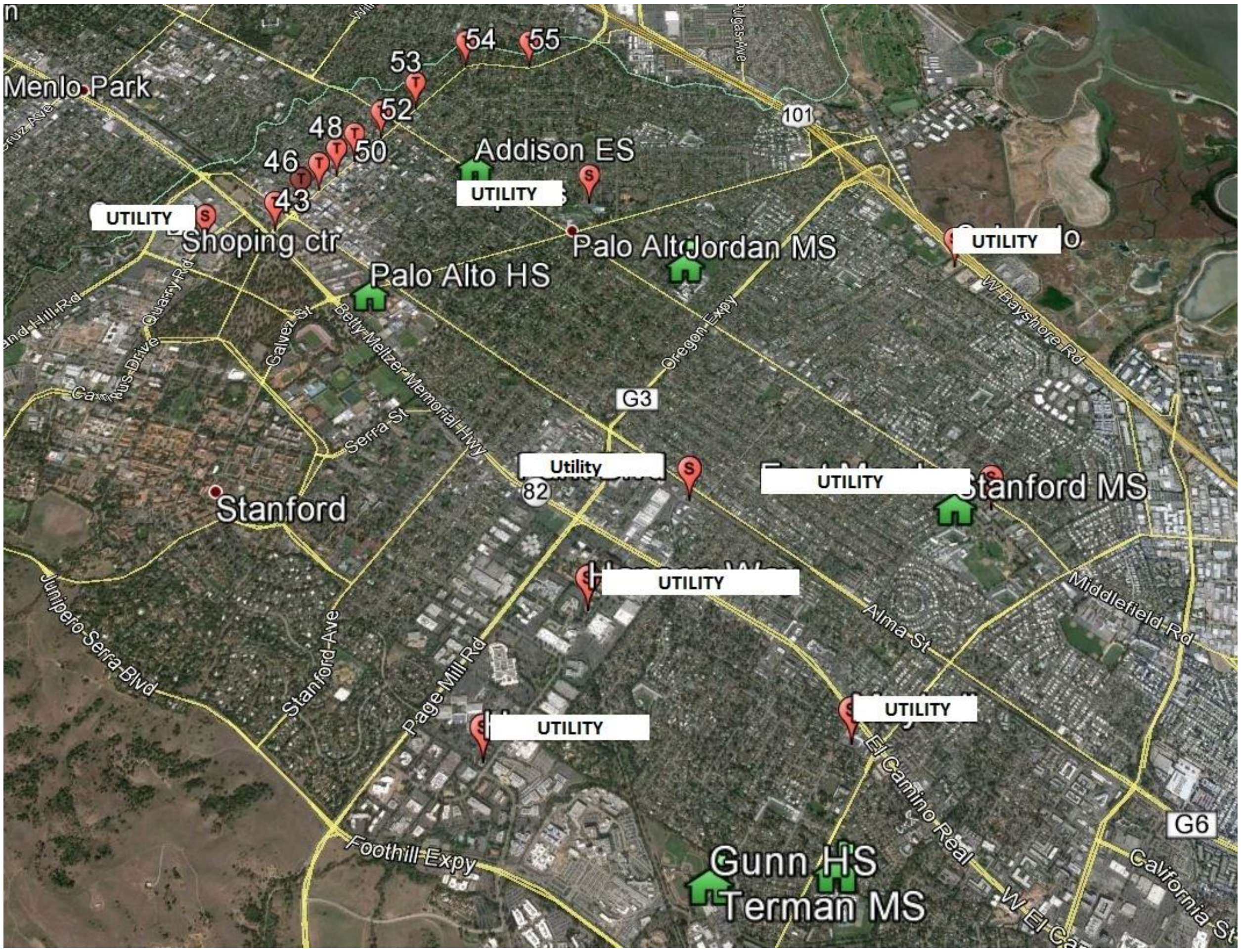
9.5.1 Basic Assumptions

This model assumes that all network backhaul infrastructure is in place and will be used to deploy this network to the maximum extent possible. Specifically, the access point will be located at traffic signals (9), public schools (5), and utility facilities (9). All selected facilities have IP network connectivity and all have available AC primary power.

The system will be constructed to meet performance specifications under IEEE 802.11a. The estimated useful life for this technology is five years. For purpose of equipment replacement, it is assumed that the useful life for any electronic equipment is seven years or less. Fiber-optic cabling, access points mounting equipment, and hardware all have a useful life of 30 years.

Figure 29 is a map showing the locations of traffic lights (T), public schools, and utility facilities that have been selected to establish this pricing model.

Figure 29: Map of Locations for Scenario 4 Deployment



9.5.2 Financial Summary

Table 9 provides the details for our projections, and assumes a six-month construction timeframe using existing IP fiber network connected backhaul.

It is anticipated that the annual operational cost to support this scenario will be low. Staffing will be supported primarily by Public Safety as an addition to its operation of land mobile radio and other existing communications equipment.

Hardware maintenance no doubt will be outsourced to equipment manufacturers/vendors. For this scenario we estimate a maximum annual expenditure of $30,000 with a useful equipment life of five to seven years.

Table 9: Scenario 4 Financial Summary (Capital Costs)

Parameters	
Access Points (En Route)	9
Hot Spot Access Points	23
Vehicle Routers	50
Capital Costs (Unit)	
Wireless AP Hardware	$2,100
Battery Backup	$600
Mobile Routers	$2,500
Installation Cost (Unit)[45]	
AP Router and Power	$1,250
Fiber Hub Integration	$25,000
Vehicle routers	$1,500
Capital Costs (Total)	
Access points	$67,200
Mobile Routers	$125,000
Fiber Core Electronics	$30,000
Installation	$87,500
Engineering & Oversight	$27,900
Total:	*$337,600*

[45] Per unit costs used to develop total capital cost for installation.

10 Business Case for Citywide Wireless

In our development of Scenario 2, we examined the advantages and disadvantages of the various business models used in other communities to deploy municipal wireless networks. Our analysis included a review of networks deployed in other cities. The business models examined included the following:

1. City-owned wholesale model: the wireless network is owned and operated by the City

2. Privately owned managed-services model: the wireless network is owned and operated by a service provider, but the City is an "anchor tenant" for the network

3. Hybrid model (public–private partnership): the City owns the network, but outsources operation and maintenance to a service provider

10.1 City-Owned Wholesale Model

We examined this option in the context of either the City's Information Technology department or the Utility providing this service. Currently the City does not have staff with the capability of supporting a major telecommunications deployment citywide. The recent deployment of wireless technology throughout major City facilities required the services of an outside contractor to support day-to-day operations. Moving from a platform of several dozen buildings to an entire citywide system consisting of more than 600 access points and possibly thousands of subscribers would represent a major departure from the way the City currently operates. Further, based on all of the available information, the revenue requirements to support such an operation greatly exceed service fees and costs for penetrations observed in other markets that do not have the wide variety of wireless availability that exists in Palo Alto.

10.2 Privately Owned Managed-Services Model

As part of our analysis we examined in detail the wireless requirements for City agencies. Scenarios 3 and 4 as defined in this report are targeted to address City government needs. (For reasons of security, network capacity, or availability, the use of a common citywide municipal wireless network was dismissed for supporting City government applications.)

It should be noted that most of the citywide government-related telecommunications applications are currently addressed by the existing fiber-optic network. Further, the broadband needs met by the existing network generally fall under the nature of supporting critical infrastructure and are more appropriately served by an independent wireless network with highly refined user requirements.

We did not uncover any significant need or revenues that might be directed to a partnership with a private operator whereby the operator would receive payment for City use. We note that in other communities where this approach has been used, the communities do not appear to have resources like the high-capacity fiber-optic network, as is the case in Palo Alto.

10.3 Hybrid Model (Public–Private Partnership)

As noted in this report, there is a significant opportunity for an outside vendor to partner with the City and the use much of the existing infrastructure to facilitate citywide deployment of a broadband wireless system. Scenario 2 examines the cost to construct and operate a citywide network leveraging a segment of the City's infrastructure.

The City could consider issuing an RFP to solicit the interest of prospective commercial organizations for such deployment. As discussed in the next section of this report, there are opportunities for integrating or blending Wi-Fi and wireless services in the urban environment. Wi-Fi deployment would increase capacity while also possibly making available to commercial wireless service providers additional sites citywide for their small-scale antenna deployment.

If the City were to move forward on this model, it would clearly need to examine the feasibility of obtaining sufficient revenue from the deployment to address the long-term cost of operation. Experience nationwide indicates that the public will use free Wi-Fi services where available; the issue here is obtaining revenue from the service.

Most consumers associate access to Wi-Fi with restaurants, coffee shops, and institutional waiting rooms. For the consumer on the move, network access is normally provided through smartphones. And while residential service is feasible for Wi-Fi, specific environmental issues in Palo Alto (such as foliage, restrictions on antenna placement for access equipment, and in many cases the need for an externally mounted access units for consumers) represent impediments not just to commercial deployment, but to the use of City Wi-Fi as a replacement for wired Internet service in many residents' homes.

11 Future Wireless Technology Innovations

This report presents a pragmatic examination of current requirements for broadband wireless services within the City of Palo Alto and alternatives for using existing infrastructure to address needs in the near-term. The recommendations contained herein focus on leveraging existing assets and using off-the-shelf technology available from major vendors. All of the scenarios presented in this document represents technologically and financially viable undertakings.

We note, however, that investments in physical infrastructure relating to wireless—such as mounting location for access devices, powering (either through commercial sources or renewable energy), and backhaul from access locations to network control centers over high-capacity fiber-optic technology links—represent a prudent investment to support long-term wireless deployment by either municipal entities or commercial wireless vendors. Much of the infrastructure has the potential for multiple uses—in the same way that operators often share cell towers, meaning that the same infrastructure supports competing commercial service providers.

11.1 Future 5G Technology Deployment

The Next Generation Mobile Networks (NGMN) Alliance,[46] an international consortium of wireless service providers and equipment manufacturers, is currently formulating the system-level requirements for "5G" next-generation public wireless networks targeted for deployment in 2020. The Alliance's white paper published in February 2015 set out the system-level performance specifications for this new technology.[47] It also addresses requirements for various categories of user access equipment such as smartphones and office technology, as well as new areas of focus such as the Internet of Things (telemetry and appliance devices) and broadcast services and emergency communications in times of natural disaster.

A few of the key points addressed in this comprehensive, visionary document include:

- Data transfer speed baselining at 1 Gbps. with a peak throughput up to 10 Gbps
- Several hundreds of thousands of simultaneous connections to be supported for massive sensor deployments (Internet of Things).
- Enhanced spectral efficiency (more throughput per segment of radio bandwidth)
- Improved coverage

[46] https://www.ngmn.org/home.html
[47] NGMN 5G White Paper, NGMA Alliance, Frankfurt, Germany Feb 2015

- Significantly reduced latency (i.e., ≤10 msec. for all applications and ≤ 1 msec. for critical applications)

The rapid growth of the Internet of Things ("IoT")[48] will require bits of information from sensors embedded in our devices; at the other end of the scale, the increase in enhanced high-definition video traffic, high-resolution photos, and terabit file transfers will require enormous amounts of bandwidth. Users will require portable equipment that can operate for long periods of time with very limited power sources. Other users' requirements are focused on rapid access anticipating network latency of 1 msec. or less.

The City of Palo Alto will need to take into account the sweeping upgrade in technology proposed by the move to 5G, because that new technology will set the benchmark for consumer expectations for any City services. Any deployment by the City of Palo Alto needs to be compatible with the community's expectations—and specifically with competitive services that will be offered by commercial wireless providers. (As a point of comparison, consider that wireless systems implemented by commercial organizations and municipal governments prior to the deployment of 4G technology by commercial operators were essentially obsolete once the new commercial technology was deployed.) That said, investment in core wireless infrastructure will provide a foundation for supporting the continual migration of wireless technology standards for access devices.

11.2 Integrating Wi-Fi and Cellular

One option for increasing the availability of wireless spectrum and increasing throughput to user devices is to bond or integrate Wi-Fi services with cellular service. Although Wi-Fi and LTE cellular technologies use different transmission, encoding, and radio spectrum, they can be linked by enhanced user access equipment that communicates simultaneously with both networks.

Generally, cellular technology provides the most robust means for communicating from the user to the wireless access point. Further, in most practical applications the communications traffic is heavily weighted toward downloads to user devices. Smartphones and other devices can be preprogrammed to take advantage of the presence of both Wi-Fi and cellular service so that upstream traffic from the user can be targeted toward the cellular link (which generally exhibits greater range and reliability that a similar link to a Wi-Fi access point).

---

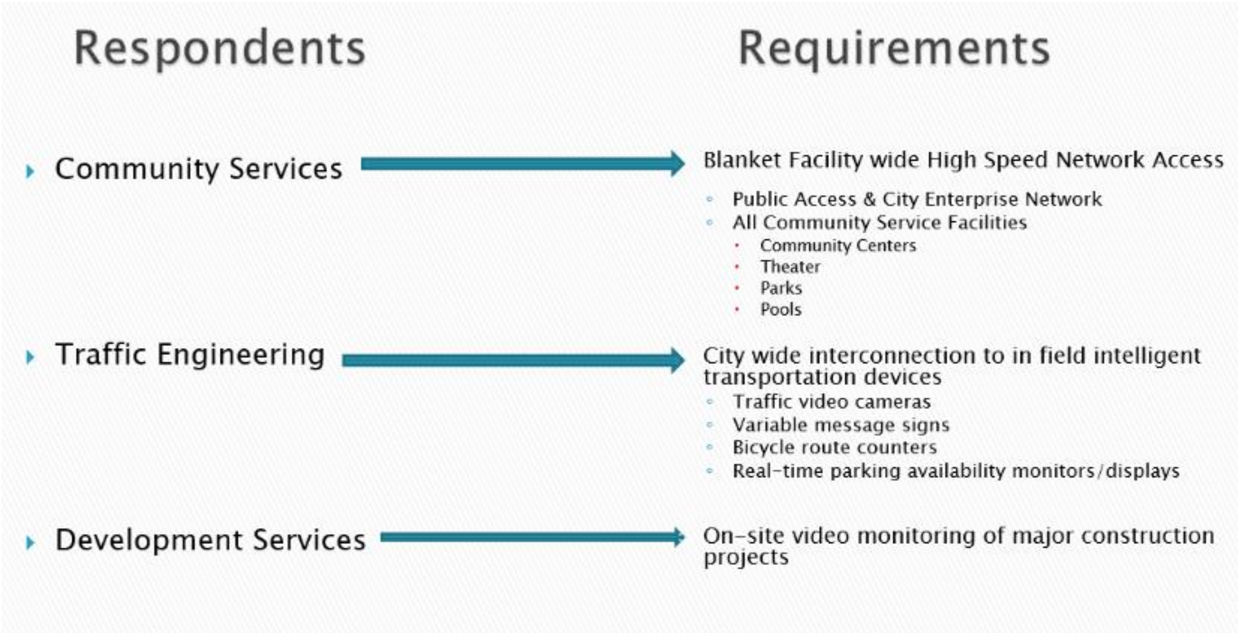
[48] The "Internet of Things" is the popular name for the growing number of consumer devices like appliances and thermostats that are "Web-enabled" and can be accessed and controlled by a user over an Internet connection. See, for example: http://www.wired.com/2015/04/google-says-internet-things-will-save-electricity/.

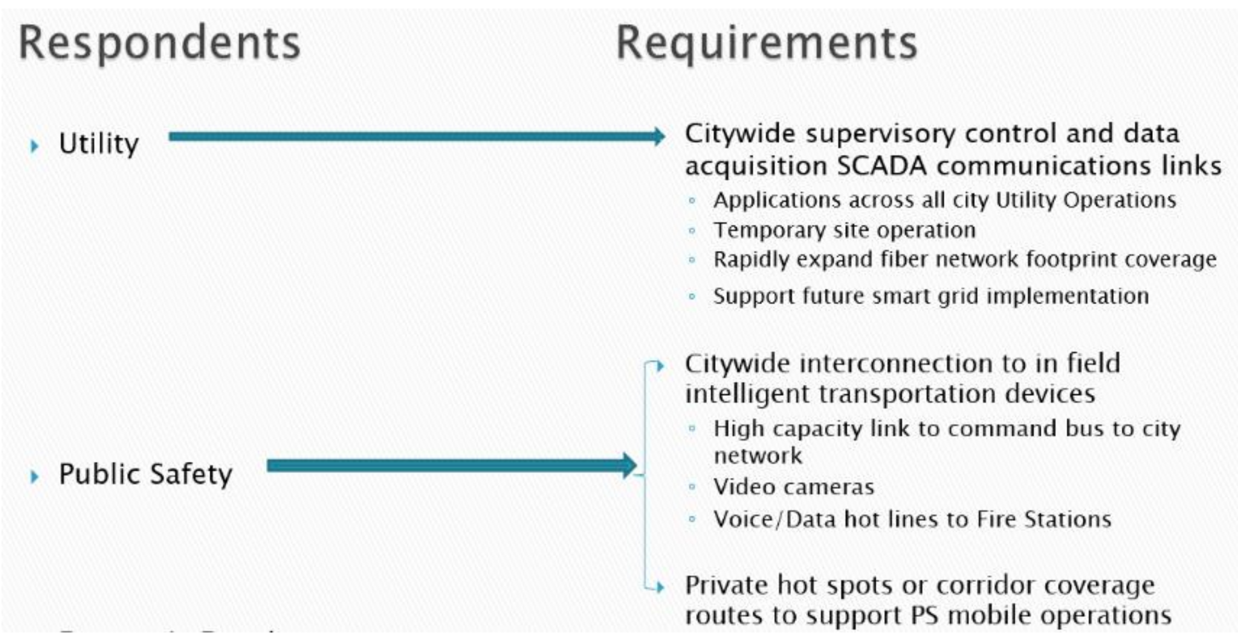
Alcatel-Lucent is one of the organizations examining this concept and looking into integrating Wi-Fi into the existing 4G cellular infrastructure.[49] This represents a stopgap measure to increase the overall download capability of existing cellular services.

We recommend that the City monitor this blending technology along with other approaches to integrating cellular and Wi-Fi technology. Assuming such technologies are successful, they may create a demand for a consistent level of high-quality Wi-Fi service throughout the community and possibly create an economic justification for deploying a citywide Wi-Fi blanket.

[49] Blending Wi-Fi and Cellular, Alcatel-Lucent Strategical White Paper, June 2015.

Appendix A: Summary of Potential Stakeholder Needs





Appendix B: Financial Projections for Scenario 2, Phase A

[This page intentionally left blank.]

Appendix C: Financial Projections for Scenario 2, Phase B

[This page intentionally left blank.]

Appendix D: City Survey Results

This survey was conducted by the City; the results (which are not statistically significant) represent an anecdotal snapshot of public opinion. We include it here at the City's request.

[This page intentionally left blank.]