Identification of Broadband Alternatives and Recommendations

Campbell County, VA

April 2014

RCC Consultants, Inc.

4900 Cox Rd.
Suite 235
Glen Allen, Virginia 23060
Tel: (804) 353-0300

Table of Contents

1.0 INTRODUCTION

1.1 REPORT SCOPE

Campbell County is interested in exploring a wide variety of broadband and wireless data system alternatives. RCC Consultants, Inc. (RCC) has been requested to analyze, evaluate and recommend a data solution initially for public safety users, with the potential to add non-public safety users to the system in the future.

The objective of the project is to pursue a Broadband initiative to determine the ideal coverage areas for our Public Safety providers. The goal is to develop a plan that incorporates the best or top three options for providing broadband access in the field for access by Public Safety and Sheriff’s Office employees. The main components of the plan would incorporate the following:

- Interviews with Key Administrative Staff, Information Technology, Public Safety and Sheriff’s Office Staff;
- Identification of potential options, costs, access speeds and vendors for implementation of the following possibilities:
  - Utilization of current cellular tower technology with access purchased on a per user basis;
  - Development of a County maintained system instead of utilizing a commercially maintained system;
  - Utilization of existing County and School facilities;
  - Utilization of the existing County communication system;
  - Any other options recommended.

This report includes an overview of the various technologies that are available, as well as an assessment of the pros and cons associated with each of the technologies. RCC has experience in the implementation of all of these various technologies including:

- Private licensed data systems (VHF/UHF/800 MHz and 4.9 GHz)
- Private unlicensed data systems (900 MHz/2.4 GHz)
- Trunked (voice and data) as well as dedicated mobile data systems
- Leased cellular (AT&T/Sprint/Verizon/nTelos/U.S. Cellular)
- Licensed and unlicensed point-to-point microwave systems
- Satellite data networks
- Hybrid Systems combining multiple networks

RCC is also at the forefront of the 700 MHz D Block licensing issues, having been selected as part of the Public Safety Systems Trust team to provide technical support during the definition and implementation of the Public/Private shared spectrum concept.

1.2 PROJECT ACTIVITIES

The scope of the project is summarized by the following tasks.

Task 1 - Project Initiation/Initial Program Review

Task 1.1 – Initial Project Coordination

Task 1.2 Develop Information Collection Document

Task 1.3 Data Gathering/Interviews

Task 2 – Requirements Development

Task 2.1 - Formulation of Concepts

Task 3 – Initial Projects Definition

Task 3.1 – Implementation Study

Task 3.2 – Project Recommendations

The on-site project kickoff took place on August 27, with interviews and site visits occurring over the next two days. Questionnaires and surveys were provided in advance of the meetings to gather insight into existing operations as well as agency needs.

The results of our review and findings are provided in the sections that follow.

2.0 MOBILE DATA SYSTEMS

RCC's Public Safety Information Systems group works with mobile data vendors across the country. Our team's knowledge of these systems allows us to assess the current systems as well as to match an agency's needs against existing systems and other vendor products.

RCC performed an assessment of the current applications and mobile data systems in use at Campbell County. In addition to standard mobile data computing from the field (digital dispatching to/from CAD, messaging, status updates), Automatic Vehicle Location is a desired capability that is supported by the DaProSystems Computer Aided Dispatch (CAD).

While the current focus is on public safety, a number of agencies were interviewed including the Sheriff's Office, Public Safety Department, which included Dispatch and Emergency Management Services (EMS) personnel, Volunteers, County Administration, Information Technology and GIS. Based on the information provided, the following number of current and future mobile data users was developed.

Mobile Data Users

Campbell County

27 patrol (take home vehicles)

10 investigators (take home vehicles)

0 current, 5 future command (chief, captain)

0 current, 4 future processing (warrants, serve papers)

0 current, 9 future School Resource Officers

4 Animal Control

7 current, 9 future Utilities

Altavista Police Department (PD) – 10 vehicles

Brookneal Police Department (PD) – 3 vehicles

8 Volunteer Fire Department Stations (Altavista, Brookneal, Timberlake, Concord, Gladys, Lynch Station, Rustburg, Evington) – 0 current, est. 3 vehicles per station, 24 vehicles total future

EMS/Volunteer Rescue Squad Stations – 27 vehicles

Career Medics – 2 vehicles

Supervisor- 1 vehicle

Career staff -1 vehicle

Fire inspections – 2 vehicles (1 staff, 1 Fire Chief)

Total current/future users – 94/138 vehicles

Typical Concurrent Use (including future):

Campbell County

7 patrol

10 investigators

5 command

4 serving warrants/papers

9 SRO

4 Animal Control

8 Utilities

Altavista PD – 3 vehicles

Brookneal PD – 2 vehicles

Volunteer Fire Department Stations – 0/8 vehicles (est. 25% response based on size/location)

EMS/Rescue Squad Stations – 7 vehicles (est. 25% response based on size/location)

Career Medic - 2 vehicles

Supervisor- 1 vehicle

Career staff -1 vehicle

Fire inspections – 2 vehicles (1 staff, 1 Fire Chief)

Total concurrent/future use – 65/73 users

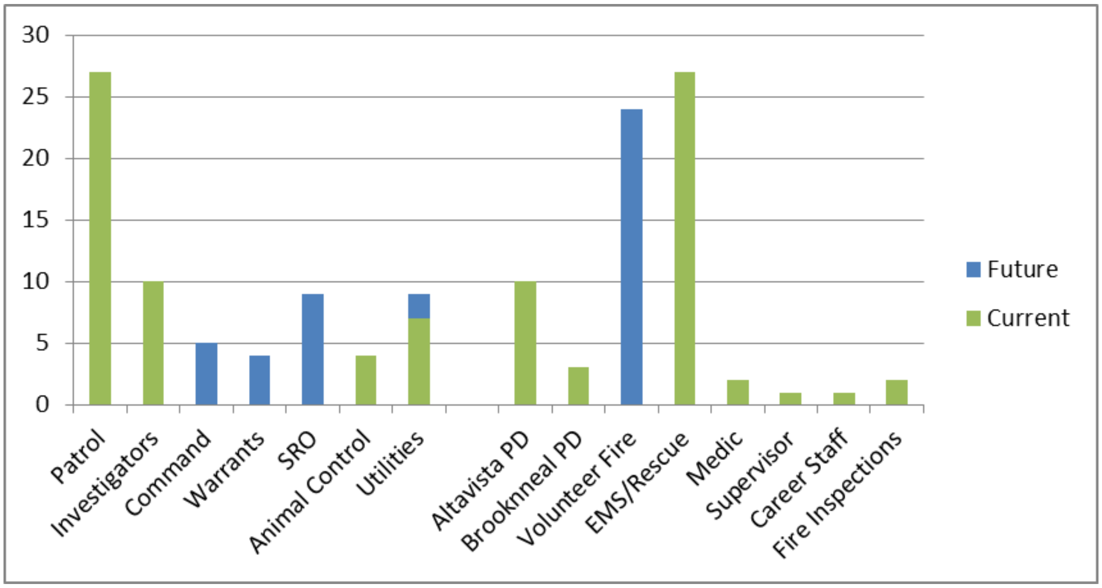

Figure 1 – Current and Future Mobile Data Users

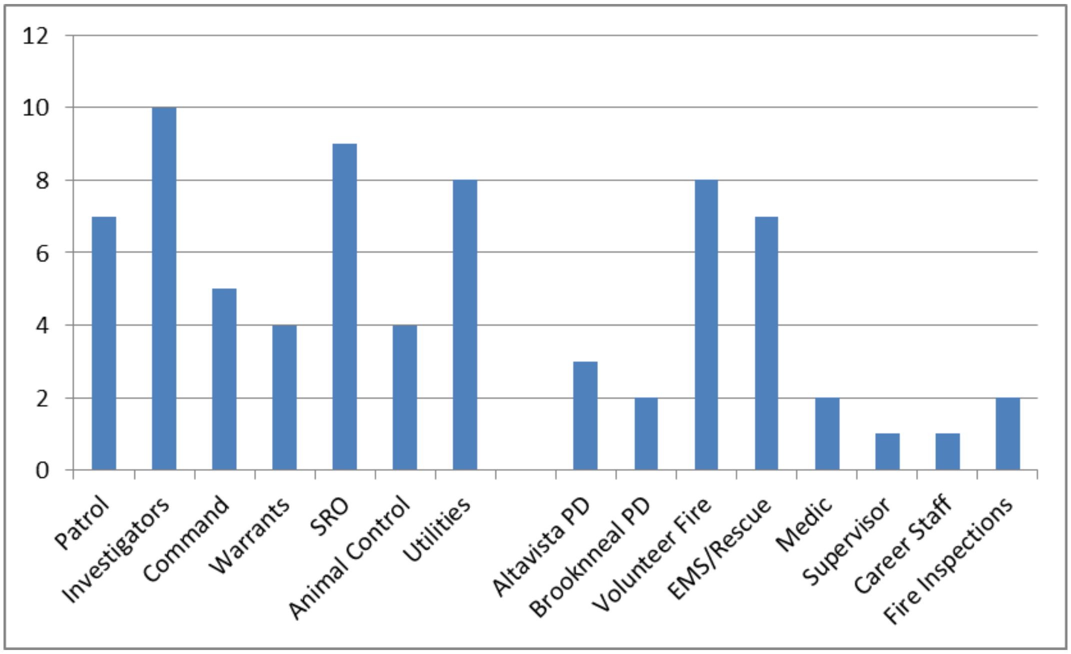

Figure 2 – Projected Number of Concurrent Users

The number of users is utilized later in the report for developing budgetary pricing estimates. The total number of users includes all vehicles that will be outfitted with mobile computers and associated wireless network devices as well as ancillary equipment such as mounts and antennas. The number of concurrent users can influence the design of the network if a large number of users are concentrated in a particular area, such as the County complex with Law Enforcement, Fire and communications personnel performing large amounts of data transmissions, because additional sites may be needed to handle the capacity of data. This can also be addressed with “hot spots” using local area access points to provide additional capacity. Given the relatively small number of users and the capability for hot spots to be added locally, no additional costs have been added to the network and costs are based on uniform usage throughout the County.

3.0 MOBILE DATA NETWORK OVERVIEW

Most of the users that have wireless connectivity currently use the Verizon Wireless network for mobile data operations. Verizon provides good coverage and throughput for users, but there are a number of wireless network alternatives available, and each solution carries with it risks and benefits. At a high level, the options can be sub-divided into either public or private networks. The following sections provide an overview of the various types of networks available for use. All of these are used by public safety personnel throughout the country.

3.1 MOBILE DATA SYSTEM OBJECTIVES

The following system objectives were considered in the analysis of mobile data system alternatives:

A. Campbell County coverage (approx. 500 sq. miles)

B. Wide Area coverage (including surrounding metropolitan areas)

C. Messages prioritized for Public Safety

D. Solution Expandable and capable of handling future needs/growth

E. Primary function is data (not voice)

F. Support for the following applications:

1. Dispatch, status updates
2. Field Reporting
3. Emergency notification
4. Messaging (e-mail/chat)
5. Queries to databases
6. Automatic Vehicle Location (AVL) - GPS
7. Internet/Intranet
8. Pictures, Video
9. Fingerprints, mugshots
10. Floor plans
11. GIS mapping

3.2 COMMERCIAL (LEASED SERVICE) WIRELESS DATA NETWORKS

Public networks are considered, for the purposes of this report, to be networks that are not privately purchased by an agency for that agency's exclusive use, but rather end user service that is leased on the network.

Public networks will have other users on the network, and the users could be other public sector agencies, commercial businesses or the general public. Public networks have the advantage of a significantly reduced up-front start up cost, with on-going maintenance and technology upgrades of the backend infrastructure provided as a part of the monthly service. These service providers are in business to provide the wireless service for a cost effective monthly fee. In order to be effective, the network provider needs to maintain a high availability and high reliability for the system. This means that they must continuously monitor the system for problems, upgrade the system as capacity approaches a predetermined limit, and react quickly if an outage is either reported or detected.

One advantage of public networks is that they allow seamless roaming throughout the United States (assuming you have coverage on the respective network, or roaming agreements in place with the associated partners in the various regions). The ability to roam outside of your immediate area and remain connected has many benefits for end users, administrators, and management personnel. End users may periodically be assigned short-term duties that require travel outside of the normal coverage area. Occasionally personnel are involved in conferences, training, or seminars that require extended travel. The ability to connect to, and remain in communication with systems and personnel, allows you to remain productive even while you travel. This is especially important for extended travel, as it allows you to keep up with work while you are away, rather than spending a significant amount of time just “catching up” when you first return.

The only up-front costs associated with a public network are the modem and the activation fee. Modems for a public network can vary from near zero to hundreds of dollars if purchased from the carrier. Rugged vehicle mounted modems can cost up to one thousand dollars and are typically available from third party vendors. The activation fee is typically less than $50 per unit. Some of these fees can be reduced or waived for public safety users, depending on the number of users and the duration of the contract. Modem selection must be matched to the wireless network, but most offer a variety of modem options, including external vehicle mounted modems, PC Card (PCMCIA) type modems, and internally mounted modems installed in the mobile computer. Vehicular modems limit the user’s ability to be on-line only while in the vehicle, while PC Card and internal modems allow the user to be on-line when the laptop is removed from the vehicle (assuming the Mobile Data Computer (MDC) is a removable laptop).

One of the risks associated with public networks is their survivability during times of disaster. Most cell sites have limited battery backup, typically in the range of several hours, without the ability for continuous operation through the use of generators and other long-term power alternatives. While some critical sites such as the Central Office may have these capabilities, much of the network will be limited to a short term battery backup. After that timeframe network coverage and capacity will be significantly reduced. Even when power is not affected, such as a critical incident that is localized to a particular area, high demand for system use can result in congestion, with limited or no communications. Currently these cellular data systems do not provide the ability to prioritize public safety users over other users, so all users are competing for limited system resources.

If a contract with a public carrier is considered, a number of contractual objectives should be discussed with the vendor. The following items need to be confirmed in writing and included in the contract, or negotiated prior to signing an agreement with a specific vendor. Some items may be rejected by the vendor, but the requests should at least be discussed and understood before signing a contract:

- Service Level Agreement – Guaranteed network reliability (less Acts of God) specific to the towers in Campbell County, along with associated penalty for failure to perform.
- Response Time guarantees and associated escalation procedures for problem resolution when a problem is identified in the network

- Coverage level throughout County (and associated test methodology)
- In-building coverage of specific locations may be able to be accommodated through network tuning (i.e. jail)
- Downward price reductions if publicly available during the term of the contract

While these issues alone are not likely to change the vendor selected, they can be used to help ensure the procedures are established for what to do when there is a network problem. While it is in the best interest of the vendor to maintain a reliable network, a group of 75 public safety users spread throughout the County and operating 24x7 are likely to be the first to identify a network problem. The process to quickly correct the problem should be established before signing a contract, in order to ensure problems are quickly identified and reported to the appropriate personnel.

3.2.1 COMMERCIAL SYSTEM ADVANTAGES

A. Low initial cost (w/competition among vendors)

B. Good data throughput (Able to achieve multiple Mbps but dependent on other users)

C. Field users can access the system anywhere the service provider has mobile service or provides service through an agreement with other providers; this means mobile data service when they roam outside of the region, even throughout the Continental United States (exception: unpopulated areas where no mobile telephone service is available).

D. The commercial provider is responsible for backend system maintenance and upgrades

3.2.2 COMMERCIAL SYSTEM DISADVANTAGES

A. **No system priority afforded to public safety traffic**. Possible system contention delays during high data traffic periods (i.e., during emergency situations).

B. System coverage design is based on the vendor’s revenue requirements.

C. High on-going cost (subscription cost)

D. Service provider could decommission the network as new technologies become available.

E. No flexibility in adding users – every additional unit on the system requires an additional service subscription

Figure 3-1 below is Verizon’s mobile data service coverage prediction for the Campbell County area. This map predicts generally good data service coverage.

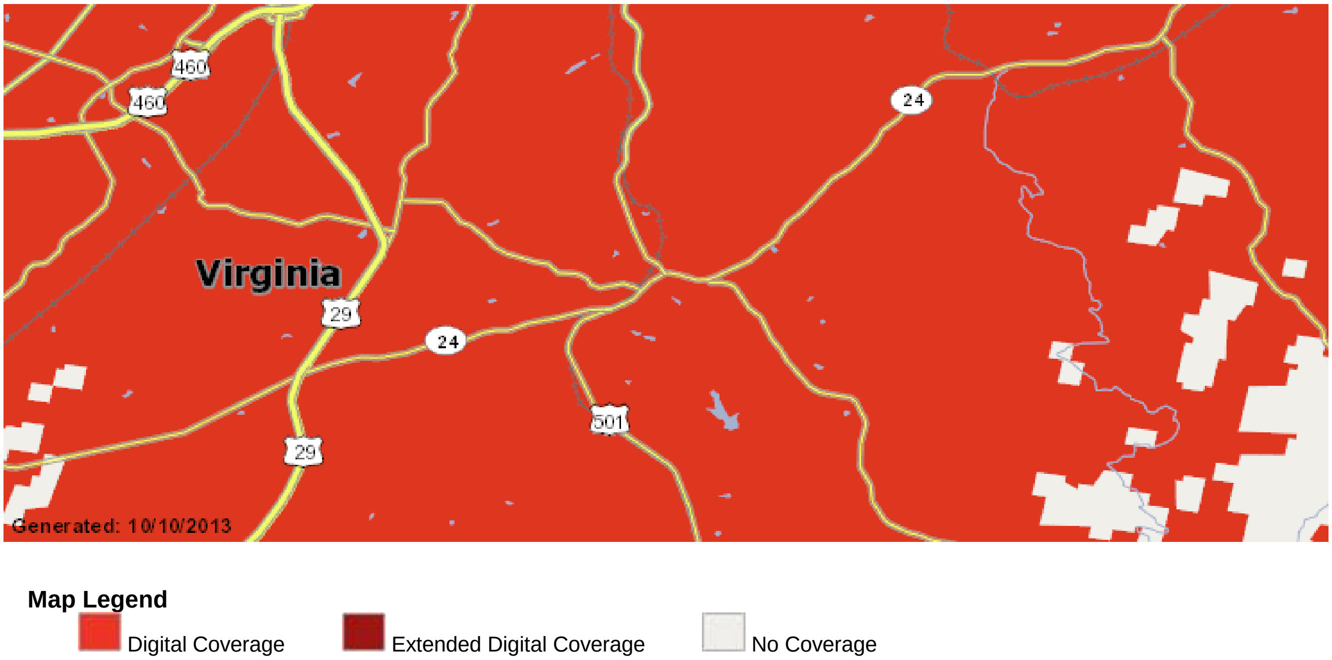

Figure 3-1 Verizon Data Coverage in Newark Area[1]

3.3 PRIVATE MOBILE DATA SYSTEMS

Private networks are purchased for the exclusive use of the procuring agency or agencies. The agency purchases system equipment and the infrastructure for the entire communications network. Private systems allow the agency total control over the network, so you never have contention with outside users, and there is no monthly usage fee. There is, however, a high initial cost for setting up a private data network associated with the procurement and installation of system equipment.

The current state-of-the-art private conventional (licensed) radio mobile data systems operate with a raw transmission speed of between 64 and 96 kilobits per second (kbps) over 25 kHz radio channels. This technology is available from several vendors in the market, including Motorola and CalAmp (formerly Data Radio), with extensive experience in public safety and government agency applications. A private mobile data system can make use of the voice radio system towers and infrastructure to minimize costs. Currently RCC is providing assistance in radio system upgrades in conjunction with the possibility of joining the Region2000 network.

Another alternative is a “non-exclusive” public safety use license which can also be obtained for 4.9 GHz systems. These systems share the general features of wireless Local Area Network (LAN) systems using 802.11a protocols, with up to 54 Mbps of raw data throughput. However, they require a significant number of sites and infrastructure to provide wide area coverage.

Many of the public safety voice radio systems include an option for providing data communications utilizing the voice radio system infrastructure. The data capability is usually very small (9.6 to 19.2 Kbps), but this can be used as an effective backup to the primary data

[1] Coverage map from www.verizonwireless.com.

communications network. The region is currently upgrading their Motorola 800 MHz voice radio system to improve coverage. The system, referred to as Region 2000, has the capability to include Integrated Voice and Data (IV&D), but it is not being utilized by the region and thus would not be a cost effective backup solution.

A relatively new option for data communications is TETRA, which is an open standard for digital trunked radio systems. TETRA stands for TErrestrial TRunked RAdio. TETRA had previously only been available outside of the United States, but has recently been approved for use in the US. It is a set of open standards developed by the European Telecommunications Standards Institute (ETSI). TETRA uses Time Division Multiple Access (TDMA) with four user channels on one radio carrier and 25 kHz spacing between carriers. Both point-to-point and point-to-multipoint transfer can be used. Digital data transmission is also included in the standard, though at a low data rate. In addition to voice and dispatch services, the TETRA system supports several types of data communication. Status messages and short data services (SDS) are provided over the system's main control channel, while packet-switched data or circuit-switched data communication uses specifically assigned channels. Data speeds are typically 12-15 Kbps, with up to 28 Kbps for the TETRA standard.

ETSI Technical Committee TC TETRA has released a new version of the TETRA standard which incorporates the next development step in the TETRA Enhanced Data Service, (TEDS). TEDS is a wideband service based on dedicated carriers. It can support 50kHz, 100kHz, and 150kHz channel widths, to deliver user bit-rates of 100 to 500kbit/s. TEDS uses the same air-interface techniques as wireless standards such as WiMax and Long Term Evolution (LTE) (3GPP Long-Term Evolution) with the same modulation scheme (quadrature amplitude modulation) and multiple subcarriers. TEDS has very narrow channels in comparison [LTE channels, for example, are 10 to 20MHz], which means users can deploy high data rates in small amounts of the spectrum.

If the TETRA system were planned for use by the County, it would provide a reasonable backup solution to the cellular mobile data network. However, since the County is not planning on obtaining this system, this alternative is effectively eliminated from consideration.

3.3.1 PRIVATE RADIO SYSTEM - ADVANTAGES

A. Dedicated System Access – Mobile data radio channels are dedicated to the Agency's mobile data access; the Agency prioritizes system data access. For example, the Agency could prioritize system access to Police/Fire transmissions. Non-mission critical transmissions (meter readings, software updates) could be scheduled for low-traffic periods.

B. System coverage design is optimized based on the Agency's requirements.

C. Public Safety-Rated System Components – System components rated for public safety users (or military) could be utilized to maintain system function during severe weather conditions. Redundant system components could be implemented to ensure maximum system uptime.

D. Agency-Controlled System Maintenance – The Agency would control system maintenance procedures. This would include scheduling system downtime for routine maintenance based on the Agency's needs.

E. Licensed frequencies reduce the risk of interference and degraded performance from other users or devices.

3.3.2 PRIVATE RADIO SYSTEM - DISADVANTAGES

A. High initial system cost (tower construction, frequency licensing/coordination, mobile receiver/modems, etc.)

B. Technology obsolescence – once purchased, technology can become obsolete in several years.

C. Data Rate (typical maximum of 96 kbps) – System data rate is low (as compared to the other alternatives), resulting in minimal Internet browsing and no real time video signal transmission.

D. Campbell County would be responsible for system maintenance.

3.4 WIRELESS LAN SYSTEMS

Wireless LAN (WLAN) uses low power spread spectrum radio transmission technology that is commonly used for high-speed broadband connectivity. This technology is rather limited in its coverage area. Therefore it is recommended to provide additional coverage or increased capacity, but would not be utilized as a Countywide solution. The technology offers very high data transmission rates when the user is within coverage. WLAN implementations use Direct Sequence Spread Spectrum (DSSS), Frequency Hopping Spread Spectrum (FHSS), or Orthogonal Frequency Division Multiplexing (OFDM) techniques. WLAN technology can be provided in the 900 MHz, 2.4 GHz, and 5 GHz bands, and usually uses an unlicensed portion of the spectrum. This means that anyone can deploy certified WLAN equipment without obtaining an FCC license. This can be both an advantage and a disadvantage of this technology, as further described below. Data transmission speeds of 1 to 600 Megabits per second (Mbps) are currently available, but transmission speeds drop off rapidly as distance from the access point increases. Achievable user data performance can be expected to be approximately 50% or less of this raw wireless transmission rate due to system overhead and signal strength. Much like a wired LAN network, the channel allows multiple users to share the available bandwidth. Typically, most vendors can support 5-10 simultaneous connections on a single access point, but the number of users is dependent on the amount of data that is being sent.

Some of the risk associated with using unlicensed frequencies is minimized by the underlying technology. The immunity to interference for WLAN technology is inherent due to the nature of spread spectrum technology, and coverage is predictable in known environments. However, proximity to noise generating sources in the same band such as a microwave oven or some portable telephones will have a negative impact upon the 2.4 GHz coverage patterns. Other nearby WLAN or spread spectrum systems can also interfere, reducing the number of available channels and thus the capacity and throughput of the system. The Federal Communications Commission (FCC) has allocated spectrum in the 4.9 GHz band for public safety and government wireless broadband use, including WLAN technology. Products are available for 4.9 GHz operations that are similar to WLAN technology products currently available in the previously mentioned frequency bands.

3.4.1 WLAN STANDARDS

In 1997, the IEEE released 802.11 as the first internationally sanctioned standard for wireless LAN technology, defining 1 and 2 Mbps speeds. Today 802.11 has grown into a family of specifications developed by the IEEE for Wireless LAN. These specifications are wireless standards that specify an “over-the-air” interface between a wireless client and a base station or access point, as well as among wireless clients. The 802.11 standards can be compared to the IEEE 802.3™ standard for Ethernet for wired LANs. The IEEE 802.11 specifications address both the Physical (PHY) and Media Access Control (MAC) layers and are tailored to resolve compatibility issues between manufacturers of Wireless LAN equipment.

The following sections describe a few of the wireless standards available today:

802.11a

The 802.11a standard, also an extension of 802.11, operates on a new, wider band of the frequency spectrum – between 5.15 - 5.35 GHz or 5.725 - 5.825 GHz – that experiences considerably less contention than the 2.4 GHz band. This technology is not compatible with either 802.11b or 802.11g; however devices commonly provide 802.11a, b and g in a single package.

802.11b

IEEE 802.11b is an extension to the 802.11 standard for wireless LANs and provides 11 Mbps transmission (with a fallback to 8, 5.5, 2 and 1 Mbps) in the 2.4GHz band using either frequency hopping spread spectrum (FHSS) or direct sequence spread spectrum. 802.11b is also sometimes referred to as Wi-Fi.

802.11g

IEEE 802.11g is an extension to the 802.11 standard for wireless LANs and provides 54 Mbps transmission in the 2.4 GHz band using either frequency hopping spread spectrum (FHSS) or direct sequence spread spectrum. 802.11g is also backward compatible with 802.11b; however, in a mixed environment the throughput bandwidth is lower.

802.11n

The 802.11n standard improves wireless network throughput over the previous standards (802.11a, 802.11b and 802.11g) with an increase in raw data rate from 54 - 600 Mbps (theoretical) with a required channel width of 40 MHz. 802.11n uses Multiple-Input Multiple-Output (MIMO) technology (multiple data streams) and frame aggregation to provide increased raw data rates.

802.11ac

The latest draft standard, which is now becoming available in the commercial marketplace, operates in the 5 GHz band and provides up to 1 Gbps of throughput (3 times faster than 802.11n) by expanding on 802.11n technologies. The new standard is backward compatible with 802.11n (in the 5 GHz band), but utilizes a wider (up to 160 MHz) bandwidth, up to 8 parallel (MIMO) streams, and a higher density modulation stream (256 QAM). Data connections of 450/900/1300 Mbps are achieved using 1 to 3 data streams respectively. Beamforming antennas in conjunction with the wider bandwidth and multiple data streams are also expected to increase the coverage as compared to 802.11n.

3.5 MESH NETWORKS

Mesh networks are essentially radio networks that dynamically adjust the communications path, using any available path including subscribers and access points for connectivity. Mesh technology was initially developed for military use, allowing users in challenging and dynamic environments to communicate. It actually takes the concepts developed and applied to the early stages of the Internet as the cornerstone of the design. In other words, a message can travel through the network in a number of different ways to be successfully delivered to the intended destination. The real difference is that the paths are not fixed. This technology has now evolved to public safety systems where a number of access points are located throughout the coverage area and the network is responsible for finding the closest and most effective path to deliver the message. Similar to Wireless LAN technology, this solution is good for filling in coverage holes or providing additional capacity, but is not recommended for a Countywide solution.

This configuration would employ outdoor-rated WiFi routers (Intelligent Access Points) installed throughout the service area on utility poles, street lamps, buildings, etc. These routers must be rated for extreme temperatures, high wind, and lightning strike survivability. As necessary, routers would interconnect with an embedded wireless backhaul capability, and be directly connected to a backhaul network typically comprised of fiber optic infrastructure. The number of wireless hops is generally designed to be limited to three.

The fiber backhaul infrastructure may be privately owned and operated by the County, or leased from the Local Exchange Carrier (LEC), the Mid-Atlantic Broadband Communities Corporation, or other service provider. If privately owned, RCC assumes that the County would build it using its own contractors. Costs would be dependent on terrain, distance and whether the fiber was installed aerially or underground, with minimum costs of approximately $50,000 per mile. Leasing fiber from a carrier or broadband network operator is feasible, but it is likely that exiting fiber assets are not in place at the specific locations that would be required to provide backhaul for a mesh network. Additionally, many carriers/providers with fiber assets prefer to lease bandwidth rather than dark fiber, which would probably not meet the County's requirements. Under normal circumstances, RCC would envision that the County would not install fiber solely to support this backhaul. Rather, we would envision such a fiber deployment to be completed in support of many applications, including networking among County facilities and schools, traffic signal control systems, Supervisory Control and Data Acquisition (SCADA) and other utility monitoring/control systems, video surveillance systems and others.

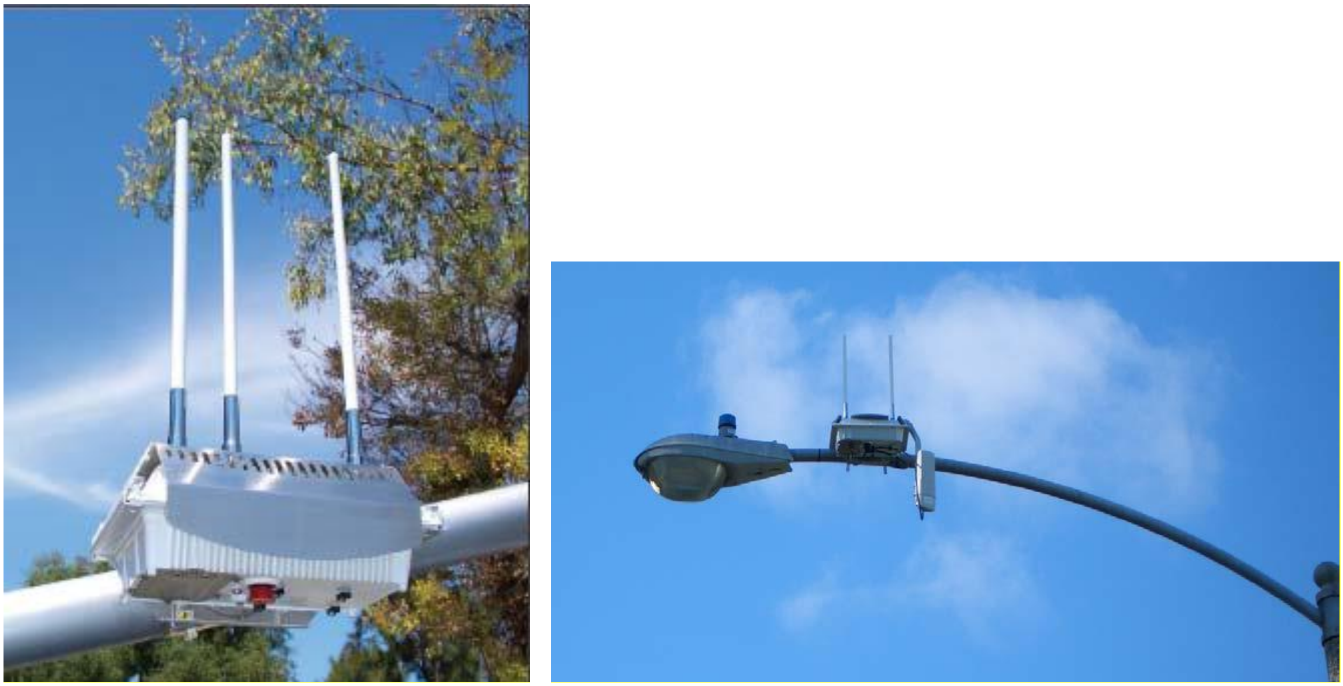

Figure 3-2 Outdoor Routers

Figure 3-3 below illustrates how the mesh routers transmit backhaul data back to the routers on the fiber link. The large router on the right represents the routers that would be on the fiber link. The backhaul data transmits wirelessly between the mesh routers throughout the network.

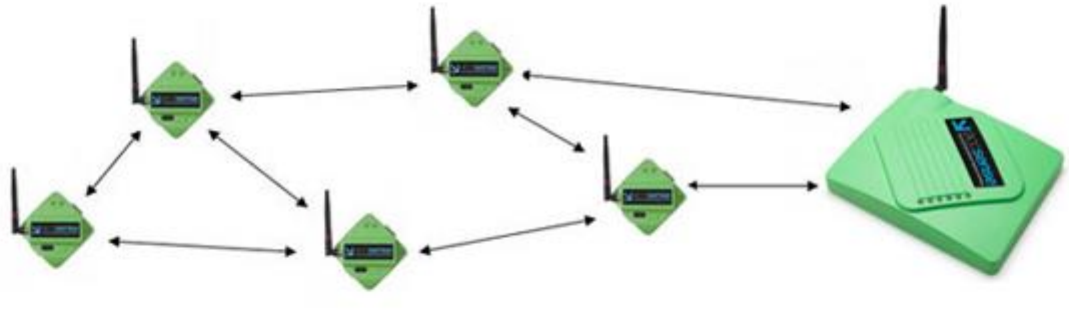

Figure 3-3 Mesh Routers

Wireless mesh routers fitted with omni-directional antenna systems are installed to communicate with field units equipped with mobile data modems. Each router should also be fitted with a battery backup system (the reserve battery time should be specified based on the number of hours to operate without external power). Thousands of wireless mesh routers would be required to completely cover the County (500 mi^2). *Depending on the technology deployed, terrain conditions, and area obstructions; 25 – 35 evenly spaced mesh routers will typically cover one square mile.*

3.5.1 MESH NETWORK – ADVANTAGES[2]

A. Low Cost - When compared to that of comparable, centralized, tower-based systems, the simplified easement, construction, and maintenance considerations of a mesh network leads to a lower deployment cost. This does not include the costs that may be associated with the deployment of fiber optic infrastructure for backhaul, as noted earlier.

B. Self Configuring - New nodes are automatically discovered and integrated into the mesh. Further, more access points can be added to a mesh network to increase capacity in high usage areas of the wireless network.

C. Self Tuning - Payload can be automatically balanced across the network via hopping and route optimization. Bandwidth and capital investment is optimized.

D. Self Healing – If a failure or congestion occurs in the mesh network, it can be isolated and traffic will be automatically routed around the issue.

E. Self Monitoring - The network, by virtue of the features, detects and reports on itself.

F. Non-line of sight connectivity – Unlike point-to-point or point-to-multipoint networks, mesh networks can route (i.e. hop) around obstructions and interference.

G. Interoperability - Modern mesh networks typically support industry standard Internet Protocol (IP). This means that existing Internet ready applications, devices, and wired networks will seamlessly integrate and operate with a mesh solution.

3.5.2 MESH NETWORK – DISADVANTAGES

A. A percentage of the available network throughput is consumed by the messaging overhead associated with identifying, configuring, and routing to other nodes.

B. Interference - Some unlicensed wireless frequencies such as 2.4 GHz can suffer from interference generated by consumer wireless devices. Other frequencies can be used such as 700 MHz or the newly licensed 4.9 GHz public safety spectrum to minimize or eliminate these problems. There are tradeoffs in using these frequencies in terms of spectrum and equipment availability. These issues should be resolved as soon as the market and users gain more experience and visibility with these new wireless solutions.

C. Training - Technicians need to acquire new skills for deploying, optimizing, and troubleshooting this new technology. Additional training is required to support and maintain fiber optic backhaul, if implemented.

3.6 SATELLITE

Satellite systems have been available to the public safety sector for some time and also undergone significant evolutionary changes. Virtually all systems used by public safety are commercial in nature due to the cost of the orbiting and terrestrial terminal based equipment. Satellite systems support many different operational platforms ranging from fixed location connectivity, to deployable fixed operations, to fully mobile operations including handheld

[2] Wireless Mesh Technology, IJIS Institute, Emerging Technologies Committee

devices. The first prerequisite for all satellite-based service is direct sky access with line of site to the satellite's position.

Satellites are often used as a backup to disasters where local communications infrastructure is temporarily unavailable, but can also be an effective tool for daily operations connecting rural and remote fixed locations and facilities. The capabilities provided by satellite systems are improving from historically low bandwidth solutions, and can now provide broadband data capabilities; however, the issues of high latency and high cost per megabyte still persist. Satellite systems also require a larger antenna than comparable mobile data systems. In order to obtain higher bandwidth, larger dish antennas are required. In order to maintain connectivity in a moving (mobile) environment and to maintain direct line of sight with the satellite, a more complex vehicle antenna solution is required.

Cost for satellite operation varies greatly with the bandwidth required and type capabilities of individual satellite systems. Satellite systems come in three basic space configurations, Low earth orbit where the satellite (or satellites) travel around the globe, often in a network of satellites at 100 to 1,200 miles above earth; medium earth orbit at about 1,240 miles above earth; or high earth orbit where they are located in a geostationary location which does not vary with the rotation of the earth. The later tend to have a detectable transmission delay due to their distant location of 22,000 miles above the earth.

3.7 HYBRID MOBILE DATA SYSTEMS

Hybrid mobile data systems involve using more than one wireless system for a solution. A hybrid alternative allows for implementation of multiple technologies in order to optimize the benefits of each solution, while at the same time mitigating the shortcomings of each individual network. It is also possible to implement a hybrid solution over time so as to reduce initial costs and approach the system(s) in phases. The technology allows for multiple solutions to work together by providing, as an example, a wide area coverage with limited bandwidth using one technology, and high data rates in selected areas (via hot spots). These hot spots or access points can be located at the Sheriff's Department, Fire stations, Rescue Squad stations, County complex, at certain buildings, street corners etc.

Hybrid solutions require multiple modems and antennas with multiple interfaces to the mobile computer. Middleware from a software provider must also be implemented in order to select the appropriate network when a device is moving between networks, and to maintain connectivity during these transitions. This middleware can automatically allow for the transfer of large amounts of data over hot spots when they become available, and default back to wide-area networks to ensure basic communications exist when not in range of a hot spot. This allows cellular networks to be the primary communications methodology used, with hot spots supplementing the network to provide additional coverage and capacity for users when they are in range of a hot spot.

Switching between the two networks can occur automatically using a middleware application such as Net Motion. The middleware application can also manage the types of communications to take place on each network. For example, if normal communications take place over a 4G cellular network and the user comes in range of a County hot spot, it may be preferable to switch over to the County network in order to take advantage of a higher transfer rate to handle a large file upload or download, thus saving potential additional costs that could be incurred on the cellular network. These transitions can be set up to occur automatically. Network management, file transfer initiation and resumption, as well as network passwords and session persistence (maintaining the user session as the user roams in and out of coverage), are all handled by network middleware applications on the system.

To the extent that the hotspots provide coverage throughout the County, they could also be utilized for backup purposes should there be a problem with cellular communications network. It is common to establish hot spots at key facilities such as the County complex where the Sheriff's Office and key County facilities are located, as well as Fire Stations, gas stations, repair depots or other facilities where users would likely be. Schools are another common location, especially if they have access to fiber connections that allow for high speed data connectivity to the County network.

3.8 PUBLIC SAFETY BROADBAND NETWORK

A potential long-term solution to satisfy the need for a mobile data network is the recently enacted Public Safety Broadband Network. The Middle Class Tax Relief and Job Creation Act of 2012 (Public Law No. 112-96, enacted February 22, 2012, the "Act"), created a First Responder Network Authority ("FirstNet") within the National Telecommunications and Information Administration of the U.S. Department of Commerce. The Act requires FirstNet to "ensure the building, deployment, and operation of the nationwide public safety broadband network". The Act also requires each state to make a decision either to "(A) participate in the deployment of the nationwide, interoperable broadband network as proposed by the First Responder Network Authority; or (B) conduct its own deployment of a radio access network in such State."

As the result of the long-term efforts by the FCC to reallocate and more efficiently use the critical resource known as Radio Frequency (RF) spectrum, television channels 52-69 were reallocated for alternate uses. This action produced the original 700 MHz frequencies designated for Public Safety use: 764 through 776 and 794 through 806 MHz. These frequencies were originally segregated for "narrowband" voice communications (6.25 and 12.5 kHz channels) and "wideband" data communications (50 kHz and up to 150 kHz channels). However, in 2007, the FCC revised the public safety allocation to 763 through 775 and 793 through 805 MHz, eliminated the wideband designated channels and designated a total of 10 MHz for broadband data communications. In conjunction with the re-allocation of spectrum, the FCC created what has become known as the "D" block of 700 MHz spectrum, which is immediately adjacent to the current 700 MHz public safety block allocated for broadband data usage. In accordance with the Act, the D Block will in fact be allocated to public safety.

It is important to understand that all states will have a federally funded Nationwide Public Safety Broadband Network deployed within their state according to the new law. Each state however, will have to decide if it will accept the network proposed by FirstNet, or of it will "Opt Out" and choose to build and operate the Radio Access Network (RAN) portion of the network itself. Regardless of a state's decision, FirstNet will build the core network and charge fees to use the core and leasing fees to use the spectrum. If a state chooses to Opt Out, it must submit a plan for the RAN network within the state, which must be approved by the FCC. The requirements of this alternate plan are quite strict, in an apparent effort to discourage states from opting out.

Each state's decision process is initiated by FirstNet, which will notify the Governor of each state when a Request for Proposal (RFP) is completed for that state detailing the rollout plan and level of funding determined by National Telecommunications and Information

Administration (NTIA) for that state. The Governor will have 90 days to choose whether to accept the plan from FirstNet or opt out and propose an alternative plan to build their RAN network for that state.

If the Governor chooses to opt out, he or she must notify FirstNet, the NTIA and the FCC and develop an RFP for the construction, maintenance, and operation of the RAN and submit the alternative plan to the FCC within 180 days of opting out. The State will be required to demonstrate that they will maintain compliance with the standards developed by the Interoperability Board. If the FCC approves the alternative state plan, in order to be eligible to apply to NTIA for a grant and a spectrum lease (from FirstNet), the state will need to demonstrate several assertions. Specifically, the state must show that it has the technical capabilities to operate and maintain the network; the funding to support it; the ability to maintain ongoing interoperability with the nationwide public safety broadband network; the ability to complete the project within specified timelines; demonstrated cost-effectiveness relative to the national plan; and demonstrate comparable security, coverage, and quality of service to that of the nationwide public safety broadband network.

If the FCC disapproves the plan, the deployment of the network within that state will proceed according to the plan proposed by FirstNet.

3.8.1 LONG TERM EVOLUTION (LTE) TECHNOLOGY

LTE, which stands for Long Term Evolution or 3GPP[3] Long Term Evolution, is the standard which the major commercial carriers have chosen for their next migration from 3G technologies.

Based on the sheer scale of commercial commitments along with the known capabilities of the LTE standard, and discussions with commercial carriers, public safety has endorsed LTE as the platform of choice moving forward both as support for the commercial carriers as well as for future planned public safety broadband systems.

Theoretical LTE network performance specifications include:

Peak Data Rate Downlink	100 Mbps
Peak Data Rate Uplink	50 Mbps
Cell User Capacity	>200 (@ 5 MHz spectrum)
Cell Site Coverage	5 – 100 km with slight degradation beyond 30 km

Table 2-1 Theoretical LTE Performance Specifications

Fourth generation mobile data systems using LTE technology are becoming more widely deployed in the 700 MHz bands. These systems provide significantly increased throughput, low latency, prioritization, and security needed by public safety. Spectrum is also dedicated to public safety, thus mitigating many of the risks associated with a public system. As these systems are currently in the process of being deployed and tested by several agencies, this is clearly the technology of the future, providing the increased throughput needed for new applications, as well as wide area coverage, public safety priority, and security. These

[3] 3rd Generation Partnership Project – an international collaboration between groups of telecommunications associations. www.3gpp.org/lte

systems also provide the ability for roaming between agencies, providing the benefits of a nationwide system dedicated for public safety users.

While these systems are in the early stages of being deployed for public safety use, the technology is sound and the benefits are proven. What remains to be determined is how much spectrum will be assigned to public safety, and if current plans to share some of the bandwidth with commercial users will remain in place.

At this time a number of agencies have been granted waivers to develop test systems for deployment. These initial systems are primarily statewide agencies or large jurisdictions due to the cost and risk associated with deployment of these initial systems. Over the next few years, it is believed that the requirements will become more stable and well defined, with more vendors providing LTE solutions in a more cost effective manner.

LTE has been set as the standard for the National Public Safety Broadband Network, which is envisioned to support public safety agencies from all over the country both while in their home jurisdictions and while in other parts of the country providing mutual aid assistance.

The technologies have evolved through generations of commercial cellular/mobile systems. 3GPP was originally the standards partnership evolving cellular systems towards the 3rd generation. However, since the completion of the first LTE and the Evolved Packet Core specifications, 3GPP has also become the focal point for mobile systems beyond 3G.

The goal of LTE is to increase the capacity and speed of wireless data networks using new Digital Signal Processing techniques and modulations that were recently developed. Its wireless interface is incompatible with 2G and 3G networks, and so it must be operated on separate wireless spectrum.

The first version of LTE to be standardized was Release 8 of 3GPP, which was frozen in December 2008. These specifications have been the basis for the initial LTE deployments. Key features of LTE release 8 include:

- High spectral efficiency,
- Robust performance against multipath interference,
- Support for multiple antenna configurations,
- Very low latency,
- Support of variable bandwidths: 1.4, 3, 5, 10, 15 and 20 MHz,
- Compatibility and inter-working with earlier 3GPP Releases,
- Support of Self-Organizing Network (SON) operation

Release 9 was frozen in December 2009 and some manufacturers are beginning to provide infrastructure that is compliant with Release 9. One of the key features of LTE Release 9 is the inclusion of Multicast/Broadcast capability. This feature will provide the foundation for group communications using LTE.

Release 10 was frozen in March 2011, but has not yet been incorporated into any system deployments. Release 10 is also known as “LTE-Advanced” and will provide even further enhancements to LTE systems. However, due to the major advancements envisioned for LTE-Advanced, hardware modifications may be required.

In December, 2012, the 3GPP Technical Specifications Group identified three key functional capabilities desired for Release 12 which are critical to public safety. These features include proximity services (direct mode) and group communications (push to talk or PTT). The third capability, mission-critical voice, was not added to Release 12, but is also considered a long term requirement for the success of Public Safety Broadband Network. The timeline set for Release 12 has been broken up into three stages, with Stage 1 frozen in March 2013, Stage 2 frozen in December 2013, and Stage 3 set for June 2014.

3.8.2 BACKHAUL NETWORK CONSIDERATIONS

A key portion of any wireless communications system is the backhaul or backbone network that connects the wireless communications sites and receives/transmits the data from/to the user in the field to/from the appropriate data network or server. A microwave backbone is generally used to support public safety communications systems due to its high reliability and relative ease of implementation.

Fiber connectivity, where available, is also an option for some portion of the backbone network due to its potential for high-bandwidth capacity. As noted, fiber is expensive to deploy, and RCC would not recommend a fiber installation solely in support of backhaul for the wireless communications system. We would prefer to see a fiber implementation that can support multiple users/departments and applications, including networking among County facilities and schools, SCADA and other utility monitoring/control systems, video surveillance systems, and others.

While an LTE system can utilize microwave and fiber connectivity similar to a traditional voice radio system, much greater capacity is required due to the higher data capacity of LTE. Typically, a single LTE radio site will require at least 30 to 50 Mbps of backhaul capacity. This will be a minimum based on the number of sites in the network and the network configuration. Backhaul links that are required to support data transfer to/from multiple sites or those that support sites that serve as aggregation points will require even higher data capacity.

3.8.3 COVERAGE AND CAPACITY

Two of the most important considerations when designing a wireless communications network are coverage and capacity. This is especially true with an LTE system, since these two factors are closely linked. An LTE system uses adaptive modulation, where the modulation form varies across a cell based on the signal strength received from the user equipment. Therefore, users located close to a transmit/receive site will experience significantly higher data rates than those located near the cell edge.

The maximum data rates that can be supported by an LTE system for a user near the serving cell site are on the order of 18 Mbps in the downlink and 6 Mbps in the uplink on a per sector basis for a 5 MHz channel, which is the current 700 MHz public safety spectrum allocation (not including the “D-Block”). While some of the capacity is reserved for control and signaling information, the majority of the capacity is generally available to support user traffic. These maximum data rates would double in a 10 MHz channel allocation, once the D-block becomes available to public safety users.

LTE uses “resource blocks” to allocate data to users, with a single resource block being the minimum amount to be allocated. For a 5 MHz channel, an LTE system will have a total of 25 resource blocks available per sector. Therefore, while the maximum data rates described above represent the maximum cumulative data rate available within a sector, the data capability may be allocated to a single user or to multiple users within a sector. If multiple users are all requesting service in a single sector at the same time, the maximum available capacity will be divided between the users.

For a public safety 700 MHz broadband LTE network, the minimum coverage and capacity design to meet the FCC requirements for waiver systems has been a design that satisfies data rates of 256 Kbps uplink (UL) and 768 Kbps downlink (DL), for all types of devices, for a user at the cell edge. It is not known at this time if FirstNet will follow these same guidelines or establish others. While these data rates may be minimally acceptable for certain applications, there will likely be portions of any proposed coverage area where higher data rates are desired or required. These areas must be designed with a higher cell density in order to ensure higher signal levels, and therefore higher data rates, throughout the cell.

While LTE technology is currently being deployed by wireless carriers throughout the United States, the actual Public Safety Broadband Network is still primarily a conceptual network, with only a few pilot projects underway. As a result, it is expected that it will be at least several years before this becomes a viable solution.

3.9 TECHNICAL CONSIDERATIONS

There can be significant differences among high speed network solutions. One of the key factors is if the solution uses licensed or unlicensed frequencies. Many of the broadband networks being deployed do not use licensed frequencies that voice radio systems typically use. Common 802.11 Wireless LANs, similar to those frequently found in coffee shops, utilize unlicensed spectrum in the 2.4 or 5 GHz spectrum. That does not mean that the information cannot be secured, only that there is a risk of interference that can reduce the effectiveness of the solution. Other unlicensed systems operate on 900 MHz frequencies, where radio signals propagate over longer distances. Higher frequencies result in shorter propagation. These systems typically trade off propagation distance and throughput, such that the farther the signal propagates, the lower the throughput that will be realized. As a result, 900 MHz systems can propagate signals for several miles, but the maximum throughput is typically in the hundreds of kilobytes. As the distance between the user and the base station is reduced, throughputs can increase into the 1 Mbps range. For systems operating in the 2.4 – 5 GHz range, raw throughput can be as great as 50 Mbps, but distances will be limited to several hundred feet. As a result, a large number of access points will be needed in order to provide coverage throughout the area.

Figure 3-4 Data Throughput of Available Systems illustrates the data throughput of available mobile data systems.

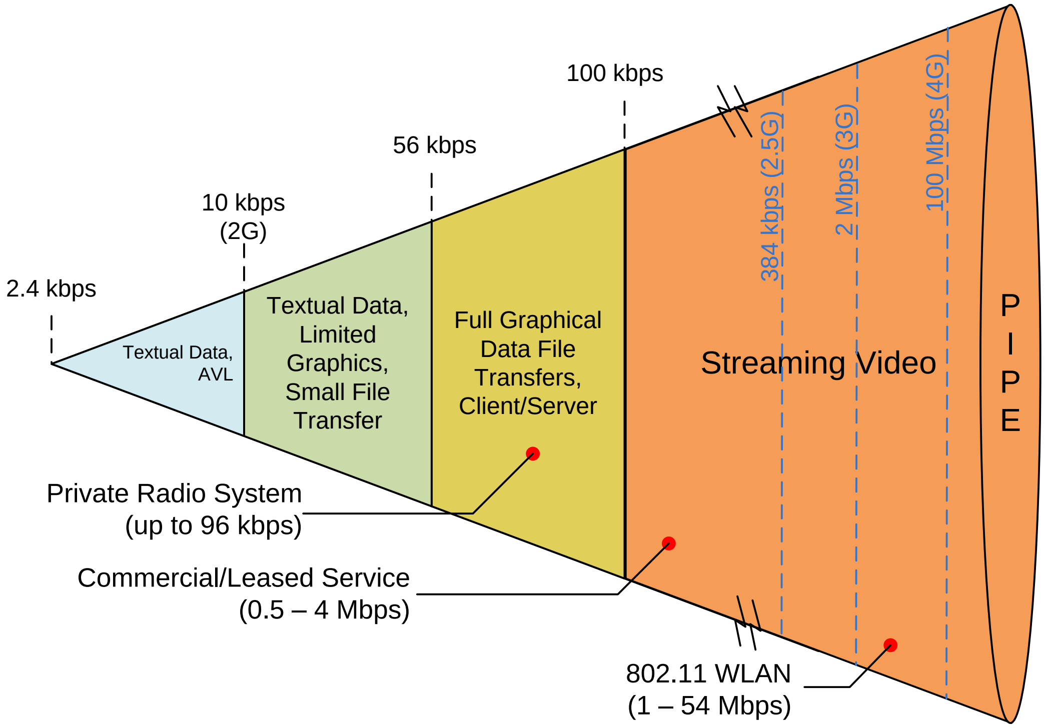
2.4 kbps
10 kbps (2G)
56 kbps
100 kbps
384 kbps (2.5G)
2 Mbps (3G)
100 Mbps (4G)
Textual Data, AVL
Textual Data, Limited Graphics, Small File Transfer
Full Graphical Data File Transfers, Client/Server
Streaming Video
P I P E
Private Radio System (up to 96 kbps)
Commercial/Leased Service (0.5 – 4 Mbps)
802.11 WLAN (1 – 54 Mbps)

Figure 3-4 Data Throughput of Available Systems

3.10 DATA SECURITY

Data security is a critical component of a wireless solution, especially in a public safety environment. The inherent technology of wireless broadband, coupled with encryption and common security precautions, provides a reasonable level of security for the system. Depending on the type of broadband solution chosen, the modulation scheme can include Orthogonal Frequency Division Multiplexing (OFDM), Frequency Hopping Spread Spectrum (FHSS), or Direct Sequence Spread Spectrum (DSSS). Frequency hopping technology was developed for the military, and results in a continuous changing of the carrier wave of the signal, making it extremely difficult to intercept. In addition, some vendors allow the selection of proprietary frequency hopping patterns to be specified for their equipment.

Wireless access to law enforcement information such as NCIC requires that the data be encrypted with at least 128-bit encryption and secured from end to end. This requirement will be increased to 256-bit encryption in the near future.

As part of an overall network security strategy, most companies employ firewalls to control access to their networks. A firewall prevents unauthorized users from accessing data and applications. For remote access, in addition to setting up a firewall, a Virtual Private Network allows private communications over public networks by enabling you to establish secure, end-to-end encrypted tunnels between the user and the back-end system. A VPN is considered one of the most effective ways to secure a network connection. Most VPN solutions use the Point-To-Point Tunneling Protocol (PPTP), the IPSec protocol, or Layer 2 Tunneling Protocol (L2TP). The VPN solution must integrate with the network and other security measures that are in place. One of the disadvantages to a VPN is that a VPN Client is usually needed on each user platform, thus adding to the complexity of the solution for both system administrators and users. VPNs are commonly used to provide a secure path for wireless data communications. It is recommended that all products procured should support the capability to be used with a VPN solution.

3.11 FIBER OPTIC NETWORK RESOURCES

RCC spoke with Dr. Rob Arnold, Asst. Superintendent for Instruction, for the Campbell County School District (CCSD) to discuss any network resources that CCSD might have that could be used by the County. CCSD is migrating to a new wide area network (WAN) architecture at this time. Until now, CCSD utilized a leased microwave service from Conterra. To provide this service, Conterra placed towers or roof structures to support microwave antennas, with direct line of sight to the primary tower on Candlers Mountain.

As this report is being completed, CCSD is migrating to a fiber optic-based WAN from Conterra. Conterra is now installing new fiber optic cabling that will connect all school sites. When completed, CCSD will be supported by a managed service from Conterra with 500MBPS links to every school. This may provide options for a future fiber optic backhaul network should the County wish to migrate to a private or hybrid public safety broadband network, since the fiber will connect to 21 school sites throughout the County.

Further, Conterra will be removing the antennas that served the CCSD microwave system eventually, but the towers/roof structures will remain in place, and could support a wireless backhaul service for the County as well.

RCC suggests that the County enter into discussions with Conterra to determine (a) the feasibility of routing the fiber in ways that would benefit the County, and (b) the potential use of the towers/roof structures to support a microwave backhaul solution.

Note that the towers, rooftops and fiber optic cabling are the property of Conterra, and that CCSD has no resources of its own that would support the County’s effort.

4.0 CONCLUSIONS AND RECOMMENDATIONS

4.1 SYSTEM REQUIREMENTS ASSESSMENT

RCC performed an assessment of the mobile data requirements, including the identified needs and desires, for use by Campbell County public safety users, as well as other agencies and departments. RCC's Public Safety Information Systems group works with a wide variety of mobile data network solutions and vendors across the country. Our team's knowledge of these systems allows us to assess the current requirements, identify candidate solutions, and to match an agency's needs against existing systems and other vendor products. This includes an analysis of costs as well as performance requirements.

4.2 COMPARING PUBLIC AND PRIVATE NETWORKS

The following table discusses some of the issues typically considered when trying to make the determination between a leased wireless data network and a privately owned alternative. This study does not address the components that typically are identical between the systems, such as the computers for the vehicles, software applications and their interfaces. This study only attempts to capture the radio network components associated with transporting the data. The types of funds available need to be determined, specifically noting if the funds are for capital improvements or are available for recurring costs.

Issue	Leased 3G/4G System	Private Dedicated Data System
Availability Anticipatable concerns regarding the procurement of the system during the next one to two years.	There are a number of vendors providing 3G systems in the Campbell County area, and system upgrades from 3G to 4G are being implemented, but County-wide coverage is an issue.	The current voice radio system is in place and provides good coverage throughout the County, but does not provide a data component. Future data solutions depend upon spectrum availability and reuse of existing towers and sites in order to be cost effective.
Control - Operational What, if any, issues exist that would limit the ability for the agency to regulate the ongoing operation of the system?	Virtually all control is relegated to the network operator. While they are often aware of the users' needs, the needs of the operator are the major motivating factor when making any decisions regarding the network.	Since the existing system would be owned and operated by the County, there are no issues related to control of the system.
Control - Scheduled Outages Who determines outage times for routine maintenance?	Little to no control is typically offered to the agency. However, they are normally conducted during off peak hours. Ideally the agency will be notified in advance of planned down time. To ensure	The County would have control of scheduled maintenance and planned outages.

Issue	Leased 3G/4G System	Private Dedicated Data System
	this happens, the agency must ensure that this clause is in the contract when selecting the network provider.	
Control – Upgrades What happens when a major revision to the network takes place?	With the on-going transition from 3G to 4G, infrastructure upgrades occur in the background with minimal impact to the users. Existing 3G modems will continue to work, but in order to take advantage of 4G technology, new modems will be required. It is the responsibility of the agency to upgrade end-user modems.	With a private data system, an annual maintenance fee will be paid to the vendor. This maintenance fee will pay for software upgrades and fixes to the hardware for both base stations and end user devices. Upgrades are scheduled and coordinated with the concurrence of the County.
Cost – Initial What is the initial cost to deploy the system?	Leased networks have a low initial cost of ownership Typically only the modems to connect to the network and some form of connectivity to the network is required. Modems can range from $0 - $1,000 per user (depending on configuration with AVL or power boosters), and the network connectivity varies depending upon the method chosen, but the installation cost is usually less than $1000, with an on-going lease cost between $300-$3000 per month depending on the type of link.	The initial cost is estimated to be between $1M and $1.5M depending on the number of base stations required, number of users, and vendor selected. This excludes any costs associated with the construction of a fiber optic backhaul network, estimated at a minimum of $50,000 per mile.
Data Capacity What, if any, constraints exist to carrying the anticipated load?	3G solutions on average offer hundreds of kilobytes per second to be downloaded to the device. 4G solutions can offer megabytes of data to be downloaded, but in either case the throughput is a function of how many users are on the network and how much data is being uploaded or downloaded at a given time. Most networks have a number of base stations at each site and a number of sites in a given area.	The throughput of a private mobile data system using a 25 KHz channel is 64 - 96 Kbps raw data rate. Wireless LAN/MESH network solutions offer speeds approaching 1 Mbps, but require significantly more sites in order to provide adequate coverage and throughput.

Issue	Leased 3G/4G System	Private Dedicated Data System
	Frequently, the network has substantially more capacity for a given area than a private solution.	
Data Contention Risk What, if any, risks are associated with the timely delivery of the data messages?	The risk is related to the number of users and the load they are presenting. With external users, this is not within the control of the agency. If there is a large incident in a populated area, anyone who is using the service within the area will be competing for the available bandwidth. This could include news staff, general population drawn to the scene as well as users residing in the area. In the long term, a priority access for law enforcement personnel would be desired.	Data contention is a function of the number of users needing to the use the system. The total number of users is predictable and in some extreme cases, specific users could be told not to the use the system. Based on the analysis provided, the risk of excessive contention should be minimal.
Expandability What constraints exist to expanding the coverage or capacity of the system? This is especially important if other groups within the agency want to join the system at a later time.	The agency typically has little direct influence on the expansion of the system unless the vendor can make a business case based on the number of committed users to build out a specified area.	Coverage and capacity would be defined at the time of procurement. Expansion of either coverage or capacity is through the addition of sites or more channels, and is in the control of the agency.
Failures What happens when a general failure occurs?	Typically, an agency has no ability to control or influence the restoration of a failure or ensure that adequate staff and spare components are maintained locally (in this case locally being a critical factor). The agency should strive to obtain contractual up-time commitments with associated penalties for failure to comply.	The availability of staff and spare components is directly controllable (at a cost) by the agency. It is recommended that critical spare components be kept locally, either at the agency or the local service provider's service center.
Maintenance Cost - Over Time	Typically all on-going maintenance costs are incurred	The County would typically pay the selected vendor a

Issue	Leased 3G/4G System	Private Dedicated Data System
What are the ongoing costs to maintain the system?	by the service provider. As new technology is deployed, the user community may be forced to upgrade or replace modems in order to take advantage of the new enhancements.	maintenance cost for system upgrades and hardware warranty/maintenance. These costs will be known and should be budgeted for if the system is to be retained. As alternate, County personnel can be trained to maintain the system, either as first level or advanced support providers.
Operational Cost - Over Time What are the ongoing costs to operate the system?	This solution has a predictable cost over time assuming long term contracts are in place. This solution typically has a higher recurring cost than a private solution, and has less flexibility in alternative cost arrangements.	This solution usually has a lower operating cost, and has potential flexibility based upon the fact that support services may be purchased or brought in house. With appropriate training, many functions can be provided by County staff. Alternatively, a decision could be made to scale back on support for specific items and further reduce costs.
Performance What is the expected performance of the system, both initially and throughout the system's projected lifespan?	Due to the fact that there is no control on the quantity of users or the applications utilized, the agency is at the mercy of the network provider to be vigilant enough to detect long term trends and to correct deficiencies. For planned or moderate duration incidents, temporary solutions (Cell on Wheels[4]) can be brought in to alleviate short-term problems.	Assuming the applications and their usage rate is known, the ability to predict or control the performance is possible because the quantity of users on the network can be controlled.
Portable Device Support How would portable devices be integrated	Public networks support a variety of portable devices.	Depending on the solution selected, some WLAN vendors offer a portable or handheld device, but most

[4] A Cell on Wheels (COW) is a fully functional, generator-powered mobile cell site that enhances coverage and capacity when needed.

Issue	Leased 3G/4G System	Private Dedicated Data System
into the solution in the future if desired?		private mobile data solutions are based on vehicle modems mounted in the car.
Reliability What reliability concerns exist with the network design?	The most common failure cited is power. While the network control facilities typically are hardened to stringent industry standards, the transmitter sites are frequently reliant on commercial power or have minimal back-up capabilities. This needs to be addressed with the specific vendor to get more information for the cell sites throughout the County.	Private public safety data systems have been available for a number of years, and are deployed in many public safety agencies. These systems have proven to be very reliable. As the data network migrates to a more commercial solution such as wireless LAN from commercial vendors, the number of sites and associated maintenance increases geometrically.
Security What security risks exist with this design?	While a general comment often made about public networks is that they are inherently insecure, additional measures can be taken to make them secure. If an effective end-to-end application encryption is implemented it should be considered secure. New CJIS requirements call for 2 factor authentication of mobile devices, currently scheduled for September 2014.	Due to the fact that most private networks use a proprietary protocol, it is considered more secure than open standards. However, networks are moving towards open IP protocols. Therefore, a minimum 128 bit end-to-end application encryption is recommended. New CJIS requirements call for 2 factor authentication of mobile devices, currently scheduled for September 2014.
Voice Contention Risk Can voice traffic interfere with the data traffic?	Since public safety does not have a priority for data, contention with the public is a critical concern. Small data packets and messages have proven to be more effective than voice for communications when an incident results in a high amount of voice traffic. The risk of data contention should be carefully explored before a decision is made.	If a dedicated data-only solution is procured, there is no concern for contention with voice traffic.

4.3 RECOMMENDATIONS

Each of the mobile data infrastructure alternatives identified in Section 3 are provided for information and comparison, though given the needs of users, coupled with geography and economic considerations, it appears that the continued use of leased cellular is the most effective solution for Campbell County. Verizon provides reasonably good coverage and throughput throughout the area. The most significant problem associated with Public Safety use of leased cellular services is that there is no ability for public safety users to have priority access for their data needs. It has been demonstrated that even when the cellular network is congested, small data messages such as text are more likely to be successfully transmitted than voice calls, which are likely to be blocked. As a result, some messaging capabilities may continue to be provided unless the network is physically knocked out from a storm or other physical disaster. Given the low startup cost for cellular, the relatively small number of users, and the competitive pricing available for public safety use, it is hard to justify the cost for development of a private network dedicated to public safety even with the addition of other agency users on the network.

In the longer term, the Public Safety Broadband Network will provide a wide area solution with good data throughput; however, but this is not likely to be a viable solution for 5 to 7 years. In the meantime, it is recommended that Campbell County continue the use of a leased cellular data network provider such as Verizon. This appears to be the most cost-effective solution, with minimal startup costs and low recurring costs based on the projected number of users. In conjunction with the cellular network, the use of wireless “hotspots” to enhance coverage and throughput at various locations such as the buildings at the County complex and facilities which include schools, libraries, fire stations, rescue squad stations, utility authority and other available structures will allow coverage and high speed data transfer for first responders.

A hybrid mobile data system solution with wide area coverage would be desired, but the voice radio system, as well as the Region2000 system, does not include a data capability.

4.4 BUDGETARY ESTIMATES

Budgetary estimates of the costs for a public and private mobile data system are provided below. The table includes costs for continued use of a cellular network, followed by costs for a new private mobile data system. Due to the excessive cost and high maintenance, a Countywide mesh network, this is not recommended as a wide area solution, but the costs for additional hotspots are provided with the costs identified per square mile of coverage. As can be seen from the table below, the estimated costs for a private system are quite high as compared to a leased cellular system. For comparison purposes, a total of 75 users have been included.

Cellular		**Initial Cost**	**Annual Cost**	**Total Cost (5 Years)**
# Users	75			
Modem (1 Time) [1, 2, 3]	$ 250	$ 18,750		$ 18,750
Service (Monthly)	$ 40		$ 36,000	$ 180,000
Replacement modems (5%)	$ 250		$ 938	$ 4,688
Total Cost				**$ 203,438**

[1] Modems are a one-time cost with the exception of lost or damaged modems. A 5% replacement cost has been included in the 5 year total cost.

[2] Modems vary in price depending on the need. Ruggedized vehicle mounted modems can be $1000 per vehicle, but non-ruggedized portable modems can be negotiated at little or no cost depending on the length of the contract with the carrier. Modems can also be imbedded in the mobile computer for several hundred dollars. For comparison purposes, a $250 modem cost was used.

[3] Activation Fees can be negotiated and have not been included in this estimate.

Private		**Initial Cost**	**Annual Cost**	**Total Cost (5 Years)**
# Users	75			
Modem (1 Time)	$ 2,500	$ 187,500		$ 187,500
Base Stations (5 sites)	$ 35,000	$ 175,000		$ 175,000
Infrastructure	$ 250,000	$ 250,000		$ 250,000
Install/Test/Tng/PM Services	$ 175,000	$ 175,000		$ 175,000
Maintenance (Annual)	20%		$ 72,500	$ 362,500
Total Cost				**$ 1,150,000**

MESH Network

As indicated in the recommendations, a Countywide wireless mesh network is not seen as a cost effective solution. The following costs are estimated for coverage with a MESH network, utilizing a total of 25 hotspots per square mile. A Countywide solution would be more cost effective due to economies of scale. These hotspots could also be installed in isolated locations to enhance specific area coverage:

System Component	**Quantity**	**Unit Price**	**Total**
Outdoor Wireless Access Points (and install H/W)	25	$4,500	$112,500
Battery Backup for Access Points	25	$250	$6,250
Hardware/Software Subtotal			$118,750
Services			
Installation/Setup	20%	$23,750	$23,750
Project Management	10%	$11,875	$11,875
Warranty/Maintenance	15%	$17,813	$17,813
Services Subtotal			$53,438
Contingency	15%	$25,828	$25,828
Grand Total			**$198,016**
		$/sq mi of coverage	**$198,016**

The above cost estimate does not include costs for fiber backhaul (minimum of $50,000 per mile), network management servers, or additional costs for mounting equipment in areas where a readily available mount such as a light pole or street light is not available.

Mobile user component pricing is estimated as shown below:

System Component	**Quantity**	**Unit Price**	**Total**
Mobile Receiver/Antenna/Cable Kit	75	$600	$45,000
Mobile Hardware Subtotal			$45,000
Services			
Installation/Setup	20%	$120	$9,000
Warranty/Maintenance	15%	$90	$6,750
Services Subtotal			$15,750
Mobile Unit Total			**$60,750**

In order to implement a multi-network solution and roam between multiple networks such as Verizon and fixed hotspots, a VPN middleware product such as NetMotion or RadioIP would be required. This would allow primary communications to take place over the faster Verizon cellular network, but in the case of failure it would automatically transfer selected communication message types (i.e. CAD dispatch messages) to be routed to the data network. This software also provides additional features such as network persistence, roaming, IP address management and data compression. The VPN solution for 100 users is estimated to cost between $25K and $50K depending on the modules that are selected.

4.5 THE NEXT STEPS

The County should decide which of the alternatives identified above would best suit its needs. If a private system or system components are to be purchased, procurement documentation should be developed to acquire the desired system(s).

Leased cellular services from carriers such as Verizon or AT&T generally provide “as is” coverage and availability. If coverage was needed in a particular area, it may be possible to negotiate an additional site based on the number of users and length of contract, but this is essentially a business case for the vendor to determine. The actual implementation of a new site can be lengthy, based on zoning requirements, approvals, procurement lead times and implementation timeframes. Fortunately, leased cellular carriers have become much more aware of the requirements of public safety users, and are more responsive to their needs. That being said, the concerns identified with leased services for public safety use as previously identified in this report need to be recognized.

In the case of a private/mesh type of solution, the County should specify (in procurement documentation/contract) that public safety agencies will be using the resulting mobile data system and the following system provisions should be included:

A. System Coverage: Typically public safety wireless systems are required to cover at least 95% of the geographic area of the jurisdiction.

B. System Availability: 99.9% or higher. This means the system can have up to 8.76 hours of downtime per year (43.2 minutes per month). Obviously, 99.99% (“four nines”) would be better; allowing 52.6 minutes of downtime per year (4.32 minutes per month).

C. System Component Redundancy. Single-Points-of-Failure in the system should be minimized.

D. Minimize Failed System Recovery Time. Whoever is maintaining the system (County or contractor) should have adequate training and system spares so that a system failure can be repaired quickly. In a contractor-maintained system arrangement, the contract could include provisions for liquidated damages for excessive system recovery times.

E. Scheduled Downtimes. System downtime scheduling should avoid public safety high traffic periods.

F. Rugged Mobile Field Components. Mobile field components (modems, antennas, power supplies, etc.) should be rated for public safety (or military) use.

Since RCC has negotiated and implemented these systems for numerous agencies, we will be happy to provide assistance in the decision making process, development of procurement documents, as well as the implementation, testing and acceptance phases of the project.

4.6 RECOMMENDATION

Based upon current technology and costs, RCC and County staff recommends use of cellular air cards as the most reliable mechanism for the foreseeable future with the development of County wireless hot spots at facilities, which include libraries, schools, fire stations, rescue squad stations, utility and other structures. One of the values of a hybrid network is that it allows for easy expansion as the needs increase. Monitoring usage of the system can help justify the costs, as well as identify when system expansion is warranted. Third party applications such as NetMotion provide the ability to roam between the various networks, as well as maintain session persistence when coverage is poor or intermittent. They also offer tools for analytics, as well as tools to monitor coverage throughout the County in order to identify areas where coverage is poor. This can also be used to identify high traffic areas where coverage is needed most. Cellular carriers will be able to provide reports on the amount of data used for each air card, and third party tools such as Solarwinds (www.solarwinds.com), CommView (http://commview-for-wifi.software.informer.com/) and Wapmon (http://wireless-access-point-monitor.soft112.com/) are available to monitor network traffic and activity. The County will continue to explore options as they unfold over the next five to ten years; however, the recommendation at this time is to utilize cellular technology along with wireless lans established at County locations for a relatively nominal cost. The County will continue to procure cellular air cards through an existing contract with Verizon with plans to assess other vendor offerings during FY15.