ITS@CAO - County of Los Angeles

Wireless Local Area Network Proposal

CAO - State Advocacy Office Location
Sacramento, CA

Prepared by:
CAO – ITS
June 27, 2002

Edwin Ro ero@cao.co.la.ca.us (213) 974-1336

Table of Contents

1. Executive Overview

The Chief Administrative Office (CAO) – Information Technology Service (ITS) Department of the County of Los Angeles is always searching for the latest technologies to increase productivity and reduce costs for its end users and related staff.

The CAO has a State Advocacy Office (SAC) located in Sacramento, CA which ITS exclusively supports either by telephone or on-site assistance. Currently, there is no local area network (LAN) or centralized Internet access at the SAC location. Each Windows 2000 workstation is stand-alone and connects to the Internet via dial-up provided by Earthlink. There are twelve end users at the SAC location and the need for a LAN and centralized Internet access is not an option, but a requirement. To contribute to the problem, the physical requirements for a wired LAN is not possible due to building complications and safety reasons. ITS investigated various possibilities to implement a LAN with the result being a wireless LAN also known as WLAN. Also, the installation of a single high-speed DSL line provided by the local telco would resolve the requirement for centralized Internet access with the use of appropriate hardware and Internet-sharing network protocols.

Several alternatives are possible for the WLAN implementation because of the wide range of products and services various vendors offer for a WLAN. The solutions that meet the various needs for ITS in implementing the WLAN would include hardware such as wireless access points, wireless network cards, firewalls, routers and gateways. Software essentials would include VPN, remote control and remote management. The proper combination and set-up of hardware and software components would result in a secure WLAN with the capability to remotely manage the WLAN from CAO headquarters in Los Angeles, CA.

The cost to have high-speed Internet access to the office environment has been reduced significantly with technologies such as DSL, cable and satellite. The demand for these Internet services is increasing on a daily basis and local telcos are constantly upgrading their infrastructure to offer reliable and consistent speeds up to 7.1 Mb/s. The implementation of DSL (Digital Subscriber Line) is the most popular implementation in the office environment for high-speed Internet access with speeds ranging from 128K to 7.1 Mb/s. DSL is provided to the office over a standard analog phone line which allows flexibility in terms of installation and set-up time constraints. With DSL at the SAC location would result in a reliable and centralized high-speed connection to the Internet.

The implementation of a WLAN is not something that can be implemented within a day or even a week, it involves careful planning and proper documentation. This proposal will layout the various options that ITS can implement at the SAC location as well as an overview of the WLAN technology. From this proposal, one will determine and realize that such an implementation of a WLAN and DSL will optimize cost, performance and productivity. The most realized benefit will be the cost savings when consolidating the twelve dial-up Internet access connections into one single high-speed DSL connection.

2. Wireless LAN Overview

2.1 Introduction

A wireless local area network (WLAN) is a flexible data communications system implemented as an extension to, or as an alternative for, a wired LAN. Using radio frequency (RF) technology, WLANs transmit and receive data over the air, minimizing the need for wired connections. Thus, WLANs combine data connectivity with user mobility.

2.2 Why Wireless?

The widespread reliance on networking in business and the meteoric growth of the Internet and online services are strong testimonies to the benefits of shared data and shared resources. With WLANs, users can access shared information without looking for

a place to plug in, and network managers can set up or augment networks without installing or moving wires. WLANs offer the following productivity, convenience, and cost advantages over traditional wired networks:

- Mobility: WLAN systems can provide LAN users with access to real-time information anywhere in their organization. This mobility supports productivity and service opportunities not possible with wired networks.
- Installation Speed and Simplicity: Installing a WLAN system can be fast and easy and can eliminate the need to pull cable through walls and ceilings.
- Installation Flexibility: Wireless technology allows the network to go where wire cannot go.
- Reduced Cost-of-Ownership: While the initial investment required for WLAN hardware can be higher than the cost of wired LAN hardware, overall installation expenses and life-cycle costs can be significantly lower. Long-term cost benefits are greatest in dynamic environments requiring frequent moves and changes.
- Scalability: WLAN systems can be configured in a variety of topologies to meet the needs of specific applications and installations. Configurations are easily changed and range from peer-to-peer networks suitable for a small number of users to full infrastructure networks of thousands of users that enable roaming over a broad area.

2.3 Range and coverage

The distance over which RF and IR waves can communicate is a function of product design (including transmitted power and receiver design) and the propagation path, especially in indoor environments. Interactions with typical building objects, including walls, metal, and even people, can affect how energy propagates, and thus what range and coverage a particular system achieves. Solid objects block infrared signals, which imposes additional limitations. Most WLAN systems use RF because radio waves can penetrate most indoor walls and obstacles. The range (or radius of coverage) for typical WLAN systems varies from under 100 feet to more than 300 feet. Coverage can be extended, and true freedom of mobility via roaming, provided through microcells.

2.4 Throughput

As with WLAN systems, actual throughput in WLANs is product- and set-up-dependent. Factors that affect throughput include the number of users, propagation factors such as range and multipath, the type of WLAN system used, as well as the latency and bottlenecks on the wired portions of the LAN. Data rates for the most widespread commercial WLANs are in the 1.6 Mbps range. Users of traditional Ethernet or Token Ring LANs generally experience little difference in performance when using a wireless LAN. WLANs provide throughput sufficient for the most common LAN-based office applications, including electronic mail exchange, access to shared peripherals, Internet access, and access to multi-user databases and applications.

As a point of comparison, it is worth noting that state-of-the-art V.90 modems transmit and receive at optimal data rates of 56.6 Kbps. In terms of throughput, a WLAN operating at 1.6 Mbps is almost thirty times faster.

2.5 Integrity and Reliability

Wireless data technologies have been proven through more than fifty years of wireless application in both commercial and military systems. While radio interference can cause degradation in throughput, such interference is rare in the workplace. Robust designs of proven WLAN technology and the limited distance over which signals travel result in

connections that are far more robust than cellular phone connections and provide data integrity performance equal to or better than wired networking.

2.6 Compatibility with the Existing Network

Most WLANs provide for industry-standard interconnection with wired networks such as Ethernet or Token Ring. WiLAN nodes are supported by network operating systems in the same fashion as any other LAN node: thought the use of the appropriate drivers. Once installed, the network treats wireless nodes like any other network component.

2.7 Interference and Coexistence

The unlicensed nature of radio-based WLANs means that other products that transmit energy in the same frequency spectrum can potentially provide some measure of interference to a WLAN system. Microwave ovens are a potential concern, but most WLAN manufacturers design their products to account for microwave interference. Another concern is the co-location of multiple WLANs. While WLANs from some manufacturers interfere with WLANs, others coexist without interference. This issue is best addressed directly with the appropriate vendors.

2.8 Licensing Issues

In the United States, the Federal Communications Commission (FCC) governs radio transmissions, including those employed in WLANs. Other nations have corresponding regulatory agencies. WLANs are typically designed to operate in portions of the radio spectrum where the FCC does not require the end-user to purchase license to use the airwaves. In the U.S. most WLANs broadcast over one of the ISM (Instrumentation, Scientific, and Medical) bands. These include 902-928 MHz, 2.4-2.483 GHz, 5.15-5.35 GHz, and 5.725-5.875 GHz. For WLANs to be sold in a particular country, the manufacturer of the WLAN must ensure its certification by the appropriate agency in that country.

2.9 Simplicity/Ease of Use

Users need very little new information to take advantage of WLANs. Because the wireless nature of a WLAN is transparent to a user's NOS, applications work the same as they do on wired LANs. WLAN products incorporate a variety of diagnostic tools to address issues associated with the wireless elements of the system; however, products are designed so that most users rarely need these tools.

WLANs simplify many of the installation and configuration issues that plague network managers. Since only the access points of WLANs require cabling, network managers are freed from pulling cables for WLAN end users. Lack of cabling also makes moves, adds, and changes trivial operations on WLANs. Finally, the portable nature of WLANs lets network managers pre-configure and troubleshoot entire networks before installing them at remote locations. Once configured, WLANs can be moved from place to place with little or no modification.

2.10 Security

Because wireless technology has roots in military applications, security has long been a design criterion for wireless devices. Security provisions are typically built into WLANs, making them more secure than most wired LANs. It is extremely difficult for unintended

receivers (eavesdroppers) to listen in on WLAN traffic. Complex encryption techniques make it impossible for all but the most sophisticated to gain unauthorized access to network traffic. In general, individual nodes must be security-enabled before they are allowed to participate in network traffic.

2.11 Scalability

Wireless networks can be designed to be extremely simple or quite complex. Wireless networks can support large numbers of nodes and/or large physical areas by adding access points to boost or extend coverage.

2.12 Safety

The output power of WLAN systems is very low, much less than that of a hand-held cellular phone. Since radio waves fade rapidly over distance, very little exposure to RF energy is provided to those in the area of a WLAN system. WLANs must meet stringent government and industry regulations for safety. No adverse health affects have ever been attributed to WLANs.

3.1 Wireless Local Area Network Diagram – Price Performance Solution

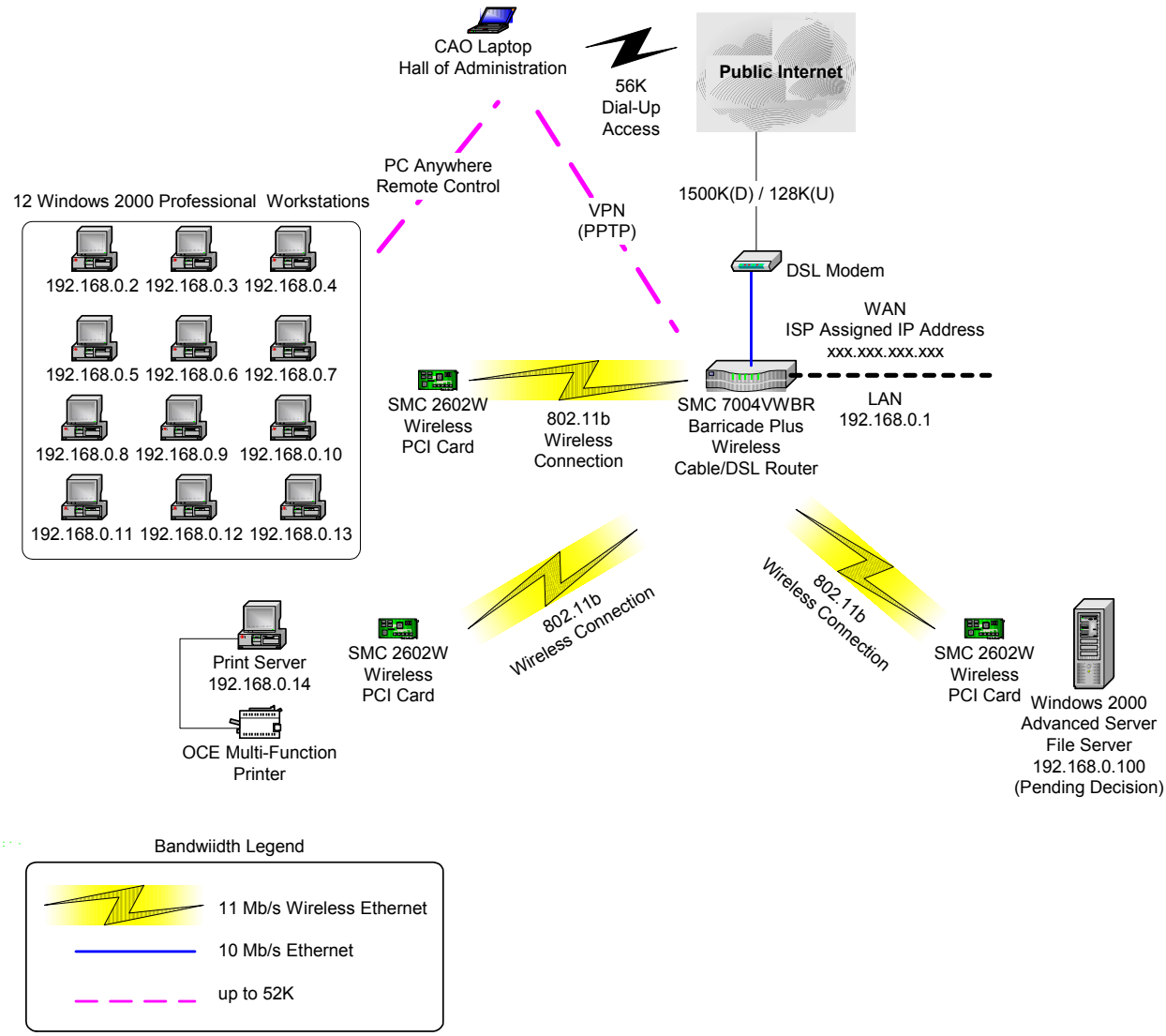

Figure 3.1a

3.2 Wireless Area Network Diagram – Management Security Solution

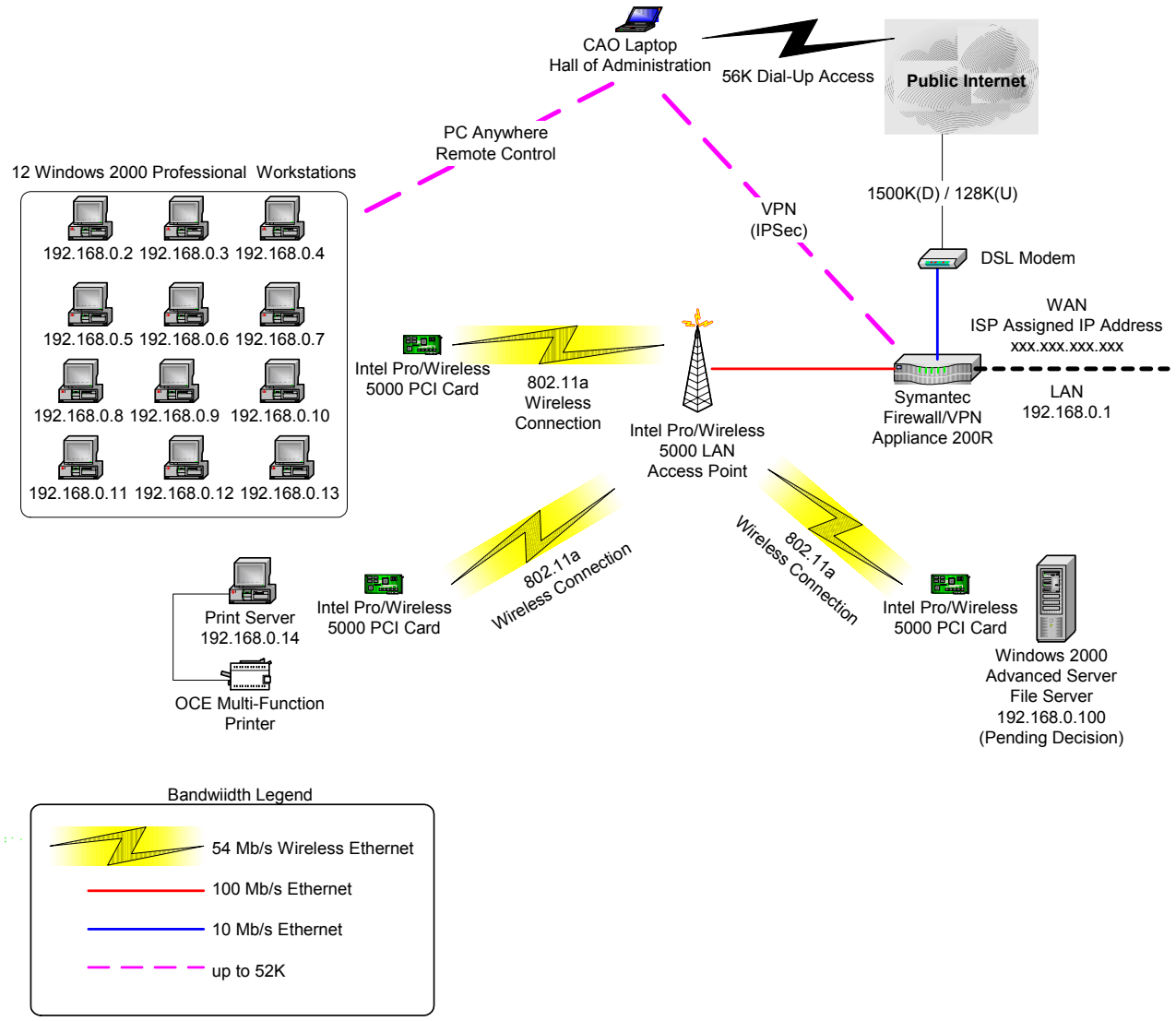

Figure 3.2a

4.1 Equipment Cost Summary Sheet - Price Performance Solution

Qty	Product Name and Features	Product Number	CDW Price	Extended Total
1	**SMC Barricade Plus Wireless Cable/DSL Router** Utilizes the 802.11b technology 11 Mb/s wireless LAN connectivity Robust Stateful Packet Inspection firewall IP address filtering and MAC address filtering Web site access control feature Hacker prevention and logging capability Built-in VPN tunnel 3-port 10/100 Mb/s switch built-in 1 10/100 Mb/s port for WAN connection	**SMC7004VWBR**	**$239.61**	**$239.61**
13	**SMC Wireless PCI Card** 11 Mb/s wireless LAN connectivity Up to 1,500 feet operating range 2.4 GHZ frequency band Direct Sequence Spread Spectrum (DSSS) Peer-to-peer or Access Point 64-bit or 128-bit encryption LEDs monitor network activity	**SMC2602W**	**$107.11**	**$1,392.43**
13	**Symantec pcAnywhere v10.5** Remote Access Perimeter Scanner Rebootless Host option allows for quick installs Remote access to servers File transfer utility Increases helpdesk productivity with remote control	**07-00-03411**	**$169.02**	**$2,197.26**
1	**DSL from Pacific Bell** DSL Modem ($99) Set-up Fee ($250) Activation Fee ($50) GSP/SBCIS Fee ($100) Note: There is an indefinite reoccurring fee of $64.95 each month for DSL access. Please refer to the cost summary portion of this proposal.	**n/a**	**$499.00**	**$499.00**

4.2 Equipment Cost Summary – Management Security Solution

Qty	Product Name and Features	Product Number	CDW Price	Extended Total
1	**Intel Pro/Wireless 5000 LAN Access Point** Speeds up to 54 Mb/s 13 times network capacity of 802.11b WLAN Operates on the 5 GHz UNII spectrum 8 non-overlapping channels 128-bit Wired Equivalent Privacy (WEP) Access Control List (ACL) Software configurable antenna	**WSAP5000AM**	**$365.96**	**$365.96**
13	**Intel Pro/Wireless 5000 LAN PCI Card** Speeds up to 54 Mb/s Up to 1,000 feet operating range Operates on the 5 GHz UNII spectrum 8 non-overlapping channels External antenna 128-bit Wired Equivalent Privacy (WEP) Site survey software	**WPCI5000AM**	**$207.10**	**$2,692.30**
1	**Symantec Firewall/VPN Appliance 200R** Integrated firewall Remote client to gateway VPN Gateway to gateway VPN 8-port 10/100 Mb/s built-in switch 2 10/100 Mb/s WAN ports Support Dynamic DNS Load balancing feature High availability with external backup modem	**16-00-00080**	**848.85**	**$848.85**
13	**Symantec pcAnywhere v10.5** Remote Access Perimeter Scanner Rebootless Host option allows for quick installs Remote access to servers File transfer utility Increases helpdesk productivity with remote control	**07-00-03411**	**$169.02**	**$2,197.26**
1	**DSL from Pacific Bell** DSL Modem ($99) Set-up Fee ($250) Activation Fee ($50) GSP/SBCIS Fee ($100) Note: There is an indefinite reoccurring fee of $64.95 each month for DSL access. Please refer to the cost summary portion of this proposal.	**n/a**	**$499.00**	**$499.00**

5. Bottom Line Cost Summary Analysis

Price Performance Solution				CDW Price
WLAN Equipment Cost Total				$ 4,328.30
	Qty	**Rate**	**Month**	**Year**
DSL Reoccurring Monthly Fee*	1	$ 64.95	$ 64.95	$ 779.40
Additional email accounts**	2	$ 2.00	$ 4.00	$ 48.00
Total			**$ 68.95**	**$ 827.40**
Current Analog Telephone Service***	12	$ 43.00	$ 516.00	$ 6,192.00
Current Dial-up ISP Fee (Earthlink)	13	$ 21.95	$ 285.35	$ 3,424.20
Total			**$ 801.35**	**$ 9,616.20**

Cost-Benefit Analysis	Year
Total Current Internet Access Fees	$ 9,616.20
Total DSL Access Fees	$ 827.40
Total Cost Savings Per Year	**$ 8,788.80**
Total One Time Equipment Costs	$ 4,328.30
First Year Cost Savings	**$ 4,460.50**

Management Security Solution				CDW Price
WLAN Equipment Cost Total				$ 6,603.37
	Qty	**Rate**	**Month**	**Year**
DSL Reoccurring Monthly Fee*	1	$ 64.95	$ 64.95	$ 779.40
Additional email accounts**	2	$ 2.00	$ 4.00	$ 48.00
Total			**$ 68.95**	**$ 827.40**
Current Analog Telephone Service***	12	$ 43.00	$ 516.00	$ 6,192.00
Current Dial-up ISP Fee (Earthlink)	13	$ 21.95	$ 285.35	$ 3,424.20
Total			**$ 801.35**	**$ 9,616.20**

Cost-Benefit Analysis	Year
Total Current Internet Access Fees	$ 9,616.20
Total DSL Access Fees	$ 827.40
Total Cost Savings Per Year	**$ 8,788.80**
Total One Time Equipment Costs	$ 6,603.37
First Year Cost Savings	**$ 2,185.43**

Notes:

* DSL Monthly Fee does not include applicable FCC surcharges and taxes

** 11 email accounts are included by default, however, 2 additional are required to satisfy user requirements

*** 1 analog phone would be kept to stabilize the DSL line

6. Technical Solution Description

The requirement for high-speed centralized Internet access as well as the ability to share printers and files has been crucial at the CAO State Advocacy Office (SAC) located in Sacramento, CA. The current use of individual dial-up accounts for twelve end users has been frustrating at times when researching on the Internet, sending large attachments and downloading research data. In addition, the sharing of files or printers involves physically walking to the intended user or printer with a floppy or ZIP disk to share or print information. This lack of productivity and inefficiency has instigated a proposal to implement a local area network with the use of wireless technology.

CAO – ITS recognizes such inadequacies and consistently provides and implements solutions toward any supported department to improve CAO work flow. ITS is determined to implement and support the SAC with a robust and productive solution that satisfies needs at the user, system and management levels.

6.1 Price Performance Wireless Area Network Solution

ITS proposes the Price Performance solution as depicted on Figure 3.1a to provide a cost-effective solution yet not sacrificing performance nor the requirements of the SAC. The core unit providing the centralized access will be the SMC 7004VWBR Barricade Plus Wireless Cable/DSL router. This router provides centralized Internet access with the use of NAT and DHCP technology. However, this solution institutes static IP addressing to alleviate any hackers from automatically receiving an IP address from the router. The router includes an integrated firewall that provides protection from external hackers with the use of Stateful Packet Inspection. The router includes an integrated 802.11b wireless access point to provide either 64-bit or 128-bit encryption with the use of Wireless Equivalent Privacy. Currently, speeds of up to 11Mb/s can be achieved with the 802.11b technology. Each user's workstation will be installed with an SMC 2602W Wireless PCI card to provide connectivity to the router. In terms of remote administration, the router allows VPN pass through to allow remote access utilizing the VPN protocol. The pcAnywhere software will be installed on each workstation that will allow CAO – ITS staff to remote control the desktop environment after authenticating to the VPN. The VPN security will be configured with Point-to-Point Tunneling Protocol (PPTP) that is the least secure of the VPN protocols yet the easiest to implement in terms of administration and set-up.

The drawbacks to the Price Performance solution are basically two reasons. First, the SMC 7004VWBR Barricade Plus Wireless Cable/DSL router provides all services to the network including VPN, wireless access, routing, security and firewall, which contribute to the central point of failure concept. In addition to the "central point of failure" concept, the SMC unit was originally designed for the SOHO environment, which contributes to less security features and lack of load balancing features during heavy usage. Second, the 802.11b technology will be used which operates in the 2.4GHz frequency. As one may know, the 2.4GHz frequency is congested with many types of cellular phones, cordless phones, and other types of wireless devices. This congestion may degrade network performance over a given period of time.

6.2 Management Security Wireless Area Network Solution

ITS proposes the Management Security solution as depicted on Figure 3.2a to provide the ultimate secure robust solution with no compromises in any subject area. There are multiple hardware components involved with this solution, which results in hardware that provides specialized features and performance specific to its purpose. The Symantec Firewall/VPN Appliance 200R will provide secure centralized Internet access for all users with the use of NAT and DHCP technology. However, this solution institutes static IP addressing to alleviate any hackers from automatically receiving an IP address from the appliance. The appliance includes an integrated firewall utilizing Stateful Packet Inspection that has been optimized for DSL Internet connections. The appliance includes a load-balancing feature that allows bandwidth to be adjusted accordingly to minimize performance degradation at the user level. The remote

administration and access feature utilizes the VPN protocol. The encryption used is IPSec, which is the most secure method of connecting to a VPN. The pcAnywhere software will be installed on each workstation allowing CAO – ITS to remote control at the desktop level to ease with helpdesk support. The appliance also has a high availability feature allowing an external modem to be attached to the appliance for back up Internet access.

The Intel Pro/Wireless 5000 Access Point will be attached to the Symantec appliance to provide secure wireless connections via the 802.11a technology. The 802.11a technology operates in the 5Ghz range, which is less congested and allows for consistent high speed wireless connections of up to 54 Mb/s. The access point includes 128-bit Wireless Equivalency Privacy with the option to authenticate users with VPN for extra security. Each user's workstation will be installed with an Intel Pro/Wireless 5000 PCI card to provide connectivity to the access point. The access point includes the Intel PROSet software that can used to monitor, diagnose, configure, and manage the wireless network. Once CAO – ITS is able to authenticate to the VPN and get on the SAC local area network, then the Intel PROSet becomes an invaluable tool to administer the wireless network.

The Management Security solution overcomes all the drawbacks of the Price Performance solution except for price. As depicted in section 5 of this proposal, the Management Security Solution costs $2275.07 more than the Price Performance Solution. However, the cost savings of $2185.43 still exist due to the consolidation of the dial-up accounts into a single DSL account. The solution overcomes the "central point of failure" concept with the existence of a dedicated wireless access point and dedicated firewall/VPN appliance. Furthermore, the wireless access point utilizes the 802.11a technology that avoids the congested 2.4GHz range. Lastly, the firewall/VPN appliance and wireless access point were designed for the enterprise environment which includes robust features such as load-balancing, high-availability features, IPSec encryption, wireless VPN authentication, and software configurable antenna.

7. Project Tasks

ID	Task Name	Duration	Start	Finish
1	Procure proposed equipment	5 days	Thu 6/27/02	Wed 7/3/02
2	Test wireless equipment to verify distance requirements	1 day	Thu 7/4/02	Thu 7/4/02
3	**Order and coordinate with PacBell to install DSL line at SAC**	**14 days**	**Thu 6/27/02**	**Tue 7/16/02**
4	PacBell to install and activate DSL line	12 days	Thu 6/27/02	Fri 7/12/02
5	Verify DSL account admin web page is online and active	3 days	Fri 7/12/02	Tue 7/16/02
6	**Day 1 at SAC location**	**1 day**	**Wed 7/17/02**	**Wed 7/17/02**
7	Fly to SAC	1 day	Wed 7/17/02	Wed 7/17/02
8	Verify that DSL connection at SAC with laptop connection	1 day	Wed 7/17/02	Wed 7/17/02
9	**Install, set-up, and configure firewall VPN equipment**	**1 day**	**Wed 7/17/02**	**Wed 7/17/02**
10	Configure DSL settings on firewall	1 day	Wed 7/17/02	Wed 7/17/02
11	Configure general local area network settings	1 day	Wed 7/17/02	Wed 7/17/02
12	Configure VPN settings	1 day	Wed 7/17/02	Wed 7/17/02
13	Configure high-availability with external modem	1 day	Wed 7/17/02	Wed 7/17/02
14	**Install, set-up, and configure wireless access point**	**1 day**	**Wed 7/17/02**	**Wed 7/17/02**
15	Configure antenna for optimal reception	1 day	Wed 7/17/02	Wed 7/17/02
16	Configure Wireless Equivalency Privacy	1 day	Wed 7/17/02	Wed 7/17/02
17	Configure wireless encryption keys	1 day	Wed 7/17/02	Wed 7/17/02
18	Configure VPN wireless authentication	1 day	Wed 7/17/02	Wed 7/17/02
19	**Day 2 at SAC location**	**1 day**	**Thu 7/18/02**	**Thu 7/18/02**
20	**Back-up data**	**1 day**	**Thu 7/18/02**	**Thu 7/18/02**
21	Back-up files, emails, address book, and any other requested data	1 day	Thu 7/18/02	Thu 7/18/02
22	**Configure workstation for wireless network**	**1 day**	**Thu 7/18/02**	**Thu 7/18/02**
23	Remove dial-up modem and software settings	1 day	Thu 7/18/02	Thu 7/18/02
24	Install wireless PCI card with latest drivers	1 day	Thu 7/18/02	Thu 7/18/02
25	Assign static IP address	1 day	Thu 7/18/02	Thu 7/18/02
26	Verify connectivity to wireless network	1 day	Thu 7/18/02	Thu 7/18/02
27	Configure Internet Explorer	1 day	Thu 7/18/02	Thu 7/18/02
28	Configure Outlook Express with new email account	1 day	Thu 7/18/02	Thu 7/18/02
29	Install Symantec pcAnywhere for remote control	1 day	Thu 7/18/02	Thu 7/18/02
30	**Configure OCE Multi-Function printer for network printing**	**1 day**	**Thu 7/18/02**	**Thu 7/18/02**
31	Install wireless PCI card with latest drivers	1 day	Thu 7/18/02	Thu 7/18/02
32	Share printer on the wireless network	1 day	Thu 7/18/02	Thu 7/18/02
33	Configure workstations with shared printer	1 day	Thu 7/18/02	Thu 7/18/02
34	**Day 3 at SAC location**	**1 day**	**Fri 7/19/02**	**Fri 7/19/02**
35	**Train users**	**1 day**	**Fri 7/19/02**	**Fri 7/19/02**
36	Explain the new set-up and benefits	1 day	Fri 7/19/02	Fri 7/19/02
37	Explain the use of pcAnywhere	1 day	Fri 7/19/02	Fri 7/19/02
38	Train on Internet Explorer and Outlook Express	1 day	Fri 7/19/02	Fri 7/19/02
39	**Verify functionality of wireless network**	**1 day**	**Fri 7/19/02**	**Fri 7/19/02**
40	Test pcAnywhere remote control with dial-up connection	1 day	Fri 7/19/02	Fri 7/19/02
41	Verify all network settings are secure as possible	1 day	Fri 7/19/02	Fri 7/19/02
42	Answer any last minute questions or concerns from users/staff	1 day	Fri 7/19/02	Fri 7/19/02
43	Fly to Los Angeles	1 day	Fri 7/19/02	Fri 7/19/02

Note: Steps 9 – 14 would be the same for either price performance or management security solution. Dates shown are not actual project dates, but to assist in interpreting the schedule.

8. Conclusion

From this proposal, one is able to determine that the implementation of DSL and wireless technology will significantly reduce yearly costs as well as increase Internet and network performance. Although one time equipment costs exist, the cost savings per year result in being more than one time equipment costs. This implementation is not only an excellent opportunity that further integrates the latest technologies at the County of Los Angeles, but also the allocation of yearly cost savings could be contributed toward researching and testing the latest technologies to further enhance productivity and the possibility to streamline inefficient processes.

The choice between the price performance solution and management security solution is one to be made by upper-level management. However, it is clear that the drawbacks of the price performance solution could result in possible security breaches and performance degrades. The management security solution not only alleviates the drawbacks, but its one-time costs are still below yearly cost savings. Again, the goal of CAO – ITS is to implement the most secure and robust solution to better enhance the end user experience while increasing productivity.

The project tasks depicted in section 7 clearly demonstrate that the implementation of this project will involve two CAO – ITS staff members to complete it in a professional and timely manner. Furthermore, knowledge transfer is brought upon two staff members to minimize the learning curve in the event CAO – ITS staff reduces in number or infrastructure support increases significantly.

The CAO – ITS department of the County of Los Angeles is always searching for the latest technologies to increase productivity and reduce costs for its end users and staff. This proposal clearly satisfies the requirements for implementing a network at the SAC location as well as centralizing Internet access while reducing costs.