White Paper

Improving Government Services and Constituency Satisfaction Using the Cisco Unified Wireless Network

This white paper describes how government entities can employ wireless LAN mobility services to improve efficiency and constituency satisfaction.

SUMMARY

State and local governments face an array of challenges—an aging population straining existing resources, continuing demands to improve security and disaster responsiveness, and a desire to improve government services. While information technology solutions alone cannot solve these complex problems, technology can improve efficiency and increase communication between government employees and their constituents. Wireless LANs in particular are uniquely positioned to help government agencies address many of these issues by becoming the platform for intelligent wireless LAN mobility services. This paper explains how the mobility services of the Cisco® Unified Wireless Network can improve the delivery of government services.

TRENDS DRIVING STATE AND LOCAL GOVERNMENT IT

Three trends point to the need for pervasive wireless LANs within government organizations. A 2005 Forrester Research study[1] of government IT executives found that the highest priorities remain improving security and business continuity. While shoring up security has been a major theme for several years, 71 percent of respondents reported that improving security is still the highest priority for IT spending; 66 percent rated business continuity as the highest priority. Another important concern expressed by IT managers in government was the need to replace existing employee computing equipment, including laptops, with over 66 percent of government respondents indicating that this was a priority. Because over 90 percent of laptops today come equipped with wireless LAN capability, it's not surprising that this trend is closely coupled with the desire to enable employee mobility.

Government workers are one of the most mobile of all workforces. From maintenance personnel to healthcare workers and transportation employees, thousands of government workers perform their jobs on the go every day. Like their private sector counterparts, government entities have discovered that wireless LANs are an important component of a mobility strategy to enable employees to be more productive. Not surprisingly, the Forrester Research study found that government has the highest percentage of employees who require mobility—a full 31 percent. This percentage is more than that for any private sector industry.

PERVASIVE WIRELESS LANS REINFORCE GOVERNMENT IT OBJECTIVES

A pervasive wireless LAN capability is the common element in all these trends. Pervasive wireless LANs and laptops significantly advance a government organization's business continuity plan. Employees can easily move to an unaffected area of a building or campus and instantly be connected to the network. If necessary, the WLAN itself can be easily removed and set up at a new location, allowing operations to start up much more quickly than in an all-wired network environment. Employees can even connect directly in ad hoc mode if the need arises.

Beyond business continuity, pervasive wireless LANs enable government organizations to improve productivity and reduce costs day-to-day. And government IT executives know this, with over 90 percent adopting wireless LANs, according to the Forrester Research study. As laptop prices have come down dramatically and embedded WLAN capability has become standard, it's become much easier to turn employee mobility into a net positive. New centralized wireless LAN architectures, such as the Cisco Unified Wireless Network, now make

[1] "*State and Local Government Data Center Spending Trends: 2005*," September 20, 2005, Forrester Research

deployment and ongoing operation of a pervasive wireless LAN simple. And with the deployment of a pervasive wireless LAN, four key mobility services are enabled: guest access services, location services, advanced security services, and voice services.

BENEFITS OF CISCO UNIFIED WIRELESS NETWORK MOBILITY SERVICES FOR STATE AND LOCAL GOVERNMENTS

In contrast to pockets of wireless LAN capability, a pervasive wireless LAN enables significant new capabilities for government organizations. Guest, voice, security, and location services can all have a substantial impact on productivity, efficiency, and security when enabled organization-wide. Here are some examples of how pervasive wireless LANs can create new services, or renovate existing government processes:

- **Improving logistics and maintenance**—Update transportation management systems with passengers served, fuel status, collected revenues, and video surveillance logs
- **Increasing responsiveness and control over telecommunications**—Track expenses, offer consistent in-building call quality, and integrate telecommunications into the existing voice PBX infrastructure through voice over wireless LAN
- **Enhancing decision making and increasing digital inclusion**—Use guest networks for constituents, system integrators, and vendors in public buildings
- **Tracking and securing assets**—Use location services to reduce the time and expense of locating or repurchasing assets
- **Improving patient services**—Deliver instant access to medical records, reach the closest caregiver, and track critical assets or at-risk patients through a pervasive wireless LAN
- **Engaging citizens**—Offer an online city services guide and Web portals both in public buildings and outdoors
- **Protecting the community**—Secure highly trafficked thoroughfares and business districts with wireless video surveillance

The rest of this paper will discuss potential applications and benefits for each mobility service, and provide a brief description of how the Cisco Unified Wireless Network implements these services.

Guest Services

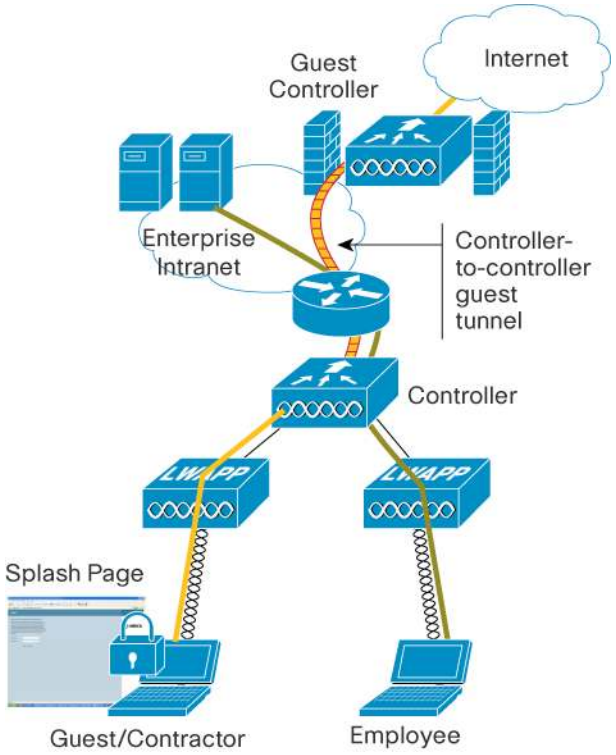
Most government organizations experience a daily flow of vendors, system integrators, visiting government employees, and constituents within the building. Enabling easy access to the Internet for all can enhance productivity and efficiency. Guest access for vendors and system integrators helps government entities speed decision making. Onsite access to company networks enables faster response times. Similarly, providing guest access for the public results in many tangible and intangible benefits. The increasing prevalence of Wi-Fi-enabled smart phones creates new possibilities, such as submitting forms online through Web portals or getting resource and service information while in government facilities. For people who need to wait for in-person assistance, the ability to use e-mail or access the company network creates good will: people appreciate being able to use their time productively.

Of course, a primary concern for any IT administrator is the ability to offer guest services in a secure way, ensuring that the government network and the information on it remain isolated from guest users. To allow multiple user groups to utilize the same infrastructure, the Cisco Unified Wireless Network enables up to 16 independent wireless LANs. A wireless LAN is defined by a unique network name (Service Set Identifier or SSID), security, and quality of service (QoS) setting. This allows the administrator to define separate SSIDs for different user groups. As an example, the SSID “guest” might be created for visitors who wish to have wireless Internet access. Another SSID “office” could be set up for employees, while a third named “shipping” might be established for business-specific devices such as bar code scanners.

Furthermore, each wireless LAN can be directed to a specific VLAN, ensuring that only the necessary resources are available to the users of that wireless LAN. Additionally, administrators can set the SSIDs to broadcast or not broadcast, at their discretion. This allows for an additional level of security. By broadcasting only the guest network SSID, fewer attempts will be made by unauthorized users to access the internal, private wireless LANs.

For some government entities, isolating the guest traffic even further is essential. In this case, the Cisco Unified Wireless Network can create a Layer 2 tunnel to direct all guest traffic outside the unsecured network area to a controller dedicated to guest services. Figure 1 shows an example of such a topology. Even remote and branch office guest users can be tunneled to a wireless LAN controller for guests, which then applies the appropriate policies before Internet access is granted. Employee wireless usage policies are managed by the wireless LAN controller(s) internal to the enterprise.

Figure 1. Directing Guest Traffic Outside the Unsecured Network Area Through a Layer 2 Tunnel



Users enter the guest network by opening their browser. A captive portal redirects the browser to a specific address where a customized login page can be presented. For tracking purposes, unique user names and passwords can be required. Administration is greatly simplified through the Cisco Guest Access Lobby Ambassador. Endpoint control—for both employees and guest users—to ensure that viruses, spyware, and worms are not introduced can be managed through Network Admission Control. For more detailed information about setting up a secure guest network, see *Achieving Business Goals and Enhancing Customer Relationships with a Secure Guest Access WLAN*.

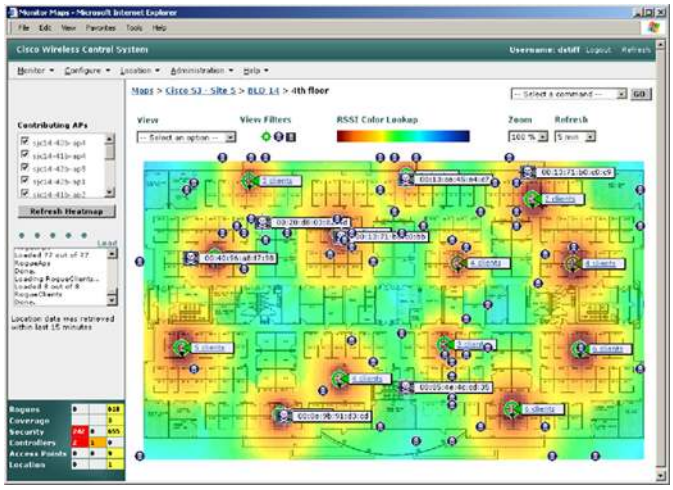
Security Services

When the most recent security standard, IEEE 802.11i is employed, wireless networks are as secure as many wired networks (and in some cases, more secure). However, because wireless LANs can penetrate beyond the physical boundaries of a building, wireless threats from unauthorized infrastructure and clients are a problem. The good news for government IT managers is that these threats can be detected and prevented using the Cisco Unified Wireless Network while it simultaneously provides service to wireless clients.

The most common threat is the rogue access point. Rogue access points are typically consumer-grade access points that are brought in by employees anxious to bring wireless service to their general surroundings. Unfortunately, because the default mode for most of these access points is to have security disabled, they become an unsecured portal to the enterprise network for anyone within range of the signal. And because wireless LAN signals can pass outside the building, unauthorized personnel may gain access to the network.

To address this security risk, the Cisco Unified Wireless Network provides advanced security services that continuously monitor, identify, and prevent wireless threats. Cisco Unified Wireless Network lightweight access points, whether servicing clients or configured as air monitors, scan for all Wi-Fi activity. If a managed access point detects another access point over the air, and it is not managed by a Cisco Unified Wireless Network controller, it is classified as a rogue. As Figure 2 shows, the location of the rogue will be immediately plotted on the floor plan map in the Cisco Wireless Control System (WCS). This technique ensures quick physical removal without time- consuming inspections using a handheld analyzer. Similar techniques are used for ad hoc networks, client misassociation, denial or service attacks, and penetration attempts.

Figure 2. Plotting a Rogue Access Point on a Floor Map



In addition, only Cisco offers the ability to integrate wireless intrusion detection system/intrusion prevention system (IDS/IPS) services with wired network IDS capability, endpoint compliance, and offsite endpoint protection, delivering a truly unified IDS/IPS solution.

Location Services

State and local governments invariably own significant numbers of assets with great value, whether the value is simply the capital cost of the item or the value of the information on a mobile device. Parks and recreation departments, transportation maintenance depots and utility yards all contain parts, tools, and vehicles. Government offices have expensive IT assets, including mobile devices, printers and other items, that should not leave the premises. County hospitals contain an array of items from medical emergency carts to monitoring equipment to utilitarian items such as gurneys and wheelchairs. And at-risk patients, including infants or the elderly, may also need to be tracked for their safety.

Knowing exactly where an asset is can enhance productivity, improve customer satisfaction, reduce cost overruns, and increase security. Instead of spending resources looking for an asset or wasting capital by purchasing it again, location tracking immediately identifies the location of the asset. Devices or people that should not leave a specific site, building or floor can be monitored so that alarms are triggered if the device or person leaves its designated area. And precise location tracking enables quick physical removal of wireless threats such as rogue access points. Furthermore, location tracking can facilitate process improvements leading to long-term permanent efficiency gains. As a history of asset utilization is developed, new procedures can be put in place to more effectively utilize the asset.

Cisco Unified Wireless Network Location Services create the ability to quickly locate any Wi-Fi device to support enhanced network security, management, and troubleshooting as well as enable location-based applications. Using Cisco Aironet® access points, Wi-Fi clients, and active RFID tag signals, the Cisco Location Appliance calculates device locations, which are then displayed in real time through the Cisco WCS on site-specific floor plans. A standards-based application programming interface (API) allows integration of the location information into business-specific security, enterprise resource planning (ERP), or workflow applications. Additionally, the

appliance provides location-based alerts for business policy enforcement, and it records rich historical location information that can be used for location trending, audit trails and regulatory compliance, rapid problem resolution, and RF capacity management. For government organizations, this means improved asset utilization, and improved protection against theft and inadvertent release of sensitive government or constituent data, as well as reduced inventory costs.

Location tracking also enables fine-grained user authentication. Instead of simply requiring a username and password to authenticate access to the network, the network can also use the precise physical location of the person requesting access. As an example, to protect privacy, a hospital could require that sensitive medical data be accessed only from within the hospital, or a city agency could require that tax records be accessed only from within a specific city building. In this way, medical records would not be accessible from the payroll department and tax records would not be accessible from the parks and recreation department. Individuals outside the building, or even outside a specific portion of a building, would be refused access, further enhancing security of the network and information.

VOICE SERVICES

Voice over IP is rapidly gaining ground as the preferred method to deliver voice communications within enterprises and government organizations alike. By delivering voice and data over a single converged IP network, acquisition and operational costs are significantly decreased. Additional benefits include lower costs for moves, adds and changes and increased productivity through presence technology that enables employees to reach each other on the first try. When voice over IP is deployed over wireless LANs, these same benefits are multiplied by making mobile workers reachable when they are away from their desks. Unlike cellular phone, service which may be spotty or nonexistent within a campus, voice over wireless LAN (VoWLAN) provides continuous, high-quality service when a pervasive wireless LAN is deployed.

Government organizations can realize many benefits from deploying VoWLAN services. One of the most important benefits is integration with existing voice services within the organization. Many mobile workers have resorted to using cell phones as their primary work phones. However, relying on cell phones precludes integration with the enterprise PBX, which may provide unified messaging, including a single voice mailbox, directory services, multiparty conference calling, and collaboration. When employees use cell phones, IT managers also lose visibility into the phone service; this, in turn, hampers support and makes it more difficult to assess telecommunications costs. What's more, many people work in jobs in which it's important that they be instantly accessible, no matter what their physical location. Examples include forensic technicians who need to be easily reached anywhere within the lab by prosecutors and detectives; and judges, district attorneys, and other officers of the court, who need to be reached anywhere within the court buildings.

The Cisco Unified Wireless Network delivers voice services through unique enhancements that support demanding real-time communications capabilities, including the following:

- Industry-leading quality of service (QoS) and Call Admission Control (CAC) on the wireless voice network, enabling voice and data applications to coexist seamlessly
- Power saving for extended handset talk-time battery life
- Real-time RF scanning and monitoring of the RF environment, delivering a self-configuring, self-optimizing, and self-healing wireless network to ensure the quality and availability of voice services
- Fast secure roaming across the campus while maintaining Wi-Fi Protected Access 2 (WPA2) security
- Access points with MAC layer enhancements to intelligently handle voice and reduce voice packet delays caused by retries

The Cisco Unified Wireless Network supports the widest variety of voice clients in the industry. The Cisco Unified Wireless IP Phone 7920 is an easy-to-use IEEE 802.11b wireless IP phone that provides comprehensive voice communications in conjunction with Cisco Unified CallManager and the Cisco Unified Wireless Network. In addition, the Cisco Compatible Extensions program gives voice client manufacturers the ability to design current and future voice wireless innovations into a wide variety of devices.

The Cisco Unified Communications system provides a full-featured, scalable, distributable, and highly available IP telephony call-processing solution. The Cisco Unified Communications system and its application partners, combined with Cisco's voice-capable wireless infrastructure, together enable government workers to move freely within their campuses without loosing connectivity and access to IP communications applications.

CONCLUSION

A pervasive wireless LAN deployment enables new services that can significantly improve state and local government effectiveness both internally and externally. Deploying the Cisco Unified Wireless Network pervasively across a government organization enables comprehensive guest, security, location, and voice services. Through a pervasive guest network, vendors, system integrators and citizens can interact and make decisions on site, or simply make use of what was formerly unproductive time, imbuing government with a new sense of efficiency and service. Guest access also creates new ways for citizens to quickly request services or resources through Web portals and Wi-Fi-enabled devices, including smart phones.

Security services are a critical piece of any government IT security strategy to protect against wireless threats such as rogue access points. Immediate identification and prevention of such threats is critical in today's wireless age to maintain network and data integrity. As government organizations are likely holders of confidential citizen information, it is imperative that this potential vulnerability be fixed before the public's trust is violated as a result of a security breach.

Location services can be coupled with security services to provide fine-grained authentication of users based on their physical placement within a building, creating an even higher hurdle for would-be hackers. And tracking the many assets owned by government organizations —from vehicles, to parts, to critical hospital equipment, to patients—ensures that people and capital resources are used wisely, and security of valuable items or people is maintained.

Voice services complete the mobile capabilities of government organizations by reducing inefficiency and the public's dissatisfaction with having to play voicemail tag. Cellular coverage does not have to be relied on within buildings. Even more important, advanced capabilities, such as presence technology, ensure that the right communication reaches the right person the first time.

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the Cisco.com Website at www.cisco.com/go/offices.

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus • Czech Republic Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel • Italy Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Printed in USA C11-360474 07/06