White Paper

Success Strategies for Deploying a Citywide Outdoor Wireless LAN

This paper describes relevant standards and best practices for the Cisco Outdoor Wireless Solution in hotspots, hot zones, and pervasive outdoor wireless deployments.

CHALLENGE

Municipal governments must meet rising needs for city services on ever tightening budgets. For many cities with a reduced tax base and federal or state subsidies, the challenge is to maintain or improve basic services and public safety with fewer personnel. As in any enterprise, efficient access to data, network resources and the Internet is a necessity, not an option, for improving productivity with fewer resources. One significant difference between municipal governments and many enterprises, however, is that many city services are performed outdoors. Tasks such as the following are performed outside of a city government building, where access to a reliable network is not a given:

- Building and fire code inspections
- City parks and recreational facility upkeep
- Code enforcement
- City maintenance
- Traffic monitoring, community policing, and other public safety duties

Delivering reliable, high-speed network access outdoors is much more problematic than providing this kind of access inside a building. Adding to the challenge is the desire of many local governments to go beyond baseline services and do more for their citizens and community. Initiatives to stimulate economic development, making technology accessible to more constituents, or encourage tourism are widespread, based on the principle that a vibrant local economy and residential base will improve the financial health of the city.

One common theme of these initiatives is affordable broadband access—in downtown areas where economic revitalization is the goal, in residential neighborhoods where the current broadband offering may not be within the means of lower-income families, and in business districts that want to attract conferences, business travelers, and tourists. But delivering this access is another matter. Incumbent service providers may not provide affordable access to all areas. In some cases, broadband access may not be available at all, especially in lower-income or less populated areas.

Delivering network connectivity to mobile public safety and city personnel raises a whole new set of challenges. With no fixed location, users face two choices: either return to an office to gain network access or use wireless cellular wide area networks (WANs). Having to return to the office is not efficient—the time and travel required from the field to a building for network connectivity result in undue delays. The effectiveness of WANs depends upon the application and data needs. WAN download and upload speeds are typically much slower than LAN speeds. For tasks that require large files, pictures, and video, using a WAN connection may be more frustrating than returning to an office.

SOLUTION

An alternative method of providing cellular communication services is to deploy high-speed wireless networks based on the IEEE 802.11 standards, also known as wireless LANs (WLANs) or Wi-Fi. When multiple access points are used to cover outdoor areas, they are commonly referred to as wireless mesh networks. However, deployment of a wireless mesh network may raise questions about the ability to extend the city's network outdoors and keep it secure. While the wireless medium has specific unique characteristics, IT managers can take comfort in the fact that essential WLAN security measures are not very different from those required to build strong wired network security. Thus, by employing the proper

WLAN security measures, IT administrators can maintain corporate privacy. This paper discusses different users, applications, and deployment models for wireless technology for outdoor wireless network deployments

OUTDOOR WIRELESS NETWORK APPLICATIONS AND USER TYPES

Understanding the different users and the anticipated applications for a wireless network is an important first step in any discussion of security measures. As with an indoor enterprise network, different types of users and applications necessitate different security measures. In general, there are three basic usage models for outdoor wireless networks:

- Municipality and city agency applications
- Public safety applications
- Public use applications, including use by residents, businesses, and tourists

Municipality and City Employee Applications

For many cities, streamlining workflow in the field represents an enormous potential reduction in manpower and increase in productivity. A primary goal is enabling employees to remain in the field instead of having to return to a central office to receive the next job or modify their route as a result of changing conditions. Using wirelessly enabled PDAs or laptops allows city personnel to receive job assignments, plans, or research material or equipment databases while in the field. Bar-code scanners can be used for asset or service tracking and can provide instant updates to other team members. With wireless mobility, city personnel can become more responsive to ad-hoc assignment changes.

Another important application is automatic meter reading, which is currently a time-intensive task. A wireless network can aggregate data from automatic meter reading (AMR) solutions in areas of a city where a fiber network may not be available. This eliminates the need for manual reading, which is not only expensive, but may also be a safety risk for meter reading personnel. Even if meter reading is currently accomplished wirelessly by personnel in the field, significant time and money can be saved by eliminating this step. Another use of AMR is the real-time monitoring of water and electricity usage data, creating more visibility into consumption. With real-time monitoring, agencies can determine if a high usage of electricity or water at any given time could be a result of faults in the system, such as water leakage from broken pipes. A quick response can improve customer satisfaction with the agencies' performance in emergency situations.

Public Safety Applications

Public safety applications cover a broad spectrum of potential users: police, fire, emergency medical services, 911 centers, airports, and transit agencies. These users need levels of system coverage, capacity, security, and control that commercial carrier systems often cannot achieve. What's more, public safety agencies are often accustomed to deploying and managing their own private systems. Some examples of applications that improve the effectiveness of public safety agencies include the following:

- **Mobile data access**—Immediate full-text access to DMV records, warrants, mug shots, criminal records, and Amber Alerts (high-priority bulletins about missing children) to speed decision making and increase safety
- **Streaming video and digital images**—Video surveillance from government buildings and businesses to gauge the nature of the response needed
- **Building schematics and plans**—Immediate access to schematics and plans as critical aid to fire safety personnel in search and rescue operations
- **Ad-hoc wireless networks**—Critical for facilitating local communication among emergency responders

Mobile devices, such as laptops and PDAs, are most commonly used for these applications. The devices are generally used in response vehicles, or "ruggedized" for use outside the vehicle. Because of the highly sensitive nature of much of the information, security measures for these applications must be much more stringent than for municipal or public usage applications.

Public Use Applications

Public use applications represent the most widely discussed area of outdoor wireless networks based on Wi-Fi. The permutations range from free, pervasive outdoor deployment in city centers for use by anyone to daily fee-based systems to monthly subscriptions for businesses and residents in select areas. Applications using the network therefore will be broad, but in general, the primary goal is to provide a high-speed broadband connection with the security of that connection left up to the user. While the laptop is currently the primary device for connecting to the network, a wide range of devices that are designed to connect to public Wi-Fi networks are becoming available. Examples include mobile data devices such as the RIM Blackberry, phones that operate as Wi-Fi and even cameras that are enabled with embedded wireless LAN clients.

MULTIUSE NETWORKS ARE BECOMING STANDARD

An initial network deployment may begin with a single user and application type to prove out the design, but will likely quickly migrate to a multiuse scenario. Even if this is not specifically planned for, the impact Wi-Fi has on outdoors is much the same as indoors. Once awareness of an outdoor WLAN exists, there is an almost immediate desire by multiple constituencies to use it. The implication for those planning and designing the network is enormous: the infrastructure must be able to support multiple users with varying endpoint devices that will likely require different authentication and security methods.

OUTDOOR WIRELESS DEPLOYMENT ARCHITECTURES

A few highly publicized plans to cover entire cities with Wi-Fi have received significant attention; however, multiple deployment models exist. Outdoor wireless LAN deployments fall into one of three distinct categories: hotspots, hot zones, or a pervasive wireless deployment. Each type of deployment has distinct requirements that Cisco Systems® addresses through a range of Cisco Unified Wireless Network products and autonomous wireless solutions.

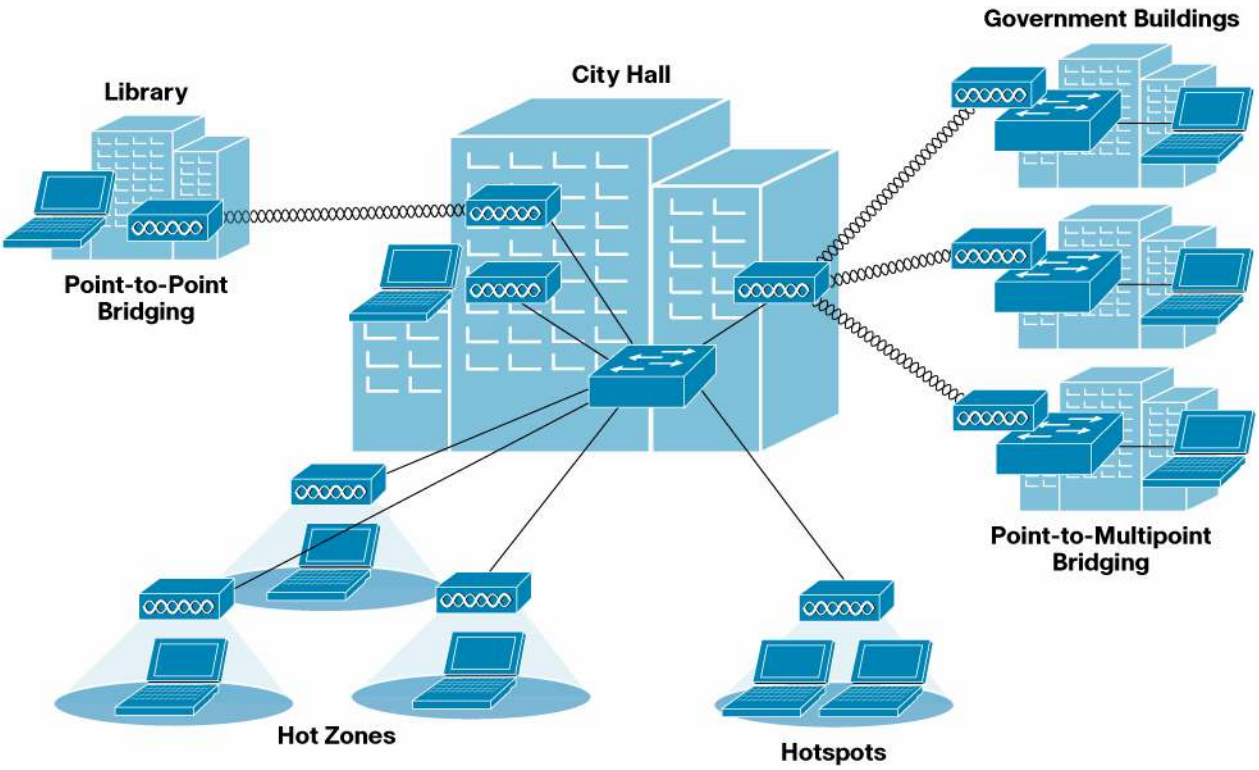
Hotspots

Hotspots are characterized by a deployment of a single access point. The term is commonly used to refer to a single wireless LAN access point within a café or restaurant, but it is also applicable when that access point is deployed outdoors. In fact, many cities find the simplest entry point into an outdoor wireless network is to create hotspots of coverage outdoors around government buildings—fire stations, police stations, courthouses, field service depots, and so on—allowing city personnel to gain high-speed connectivity at various locations around town without having to return to headquarters.

Cisco Wireless Network Solution for Hotspots: Cisco Aironet 1300 Series Outdoor Access Point

The Cisco Wireless Network solves the challenge of multiple hotspot deployments through the Cisco Aironet® 1300 Series Outdoor Access Point. Engineered specifically for harsh environments, the Cisco Aironet 1300 Series is ideal for outdoor hotspots (Figure 1). The Cisco Aironet 1300 Series supports the innovative features available with Cisco Aironet and Cisco Compatible client devices.

Figure 1. Cisco Aironet 1300 Series Outdoor Access Point Deployment



The Cisco Aironet 1300 Series supports the IEEE 802.11g standard providing 54 Mbps data rates with a proven, secure technology while maintaining full backward compatibility with legacy 802.11b devices. Two models are available—one with an integrated high-gain antenna, and a second with external antenna connectors.

The Cisco Aironet 1300 Series has an RP-TNC connector that allows the deployment of omni-directional, sector, or high-gain dish antennas to optimize and increase coverage for specific environments. In addition to supporting several antennas available from Cisco, the Cisco Aironet 1300 Series has different mounting options. These optional mounting kits are available for mounting to a roof, wall, or pole. The quick-hang mounting bracket allows for a simple, one-person installation.

Hot Zones and Pervasive Wireless Deployments

Deploying multiple access points to create a single contiguous coverage area creates a hot zone. Hot zones typically concentrate a wider coverage in dense areas with a higher capacity to support many users. Downtown business districts, city government campuses, recreational parks and venues, and harbors or marinas are all common locations for WLAN hot zones. Pervasive wireless deployments are simply extensions of hot zones across an entire municipality or a significant portion of it. Aside from the obvious increase in access points needed with a larger deployment, the main difference between a hot zone deployment and a pervasive wireless deployment is the requirement for more backhaul points of broadband connectivity to the edge access points, allowing data traffic to move more quickly to the Internet and reducing congestion at the access level.

Because hot zones and pervasive wireless deployments consist of multiple access points, these deployments must support two requirements:

- Uninterrupted roaming of mobile devices across multiple subnets
- Easy backhaul connectivity for the access points

Uninterrupted Roaming of Mobile Devices Across Multiple Subnets

Larger outdoor wireless deployments are likely to place access points across subnet boundaries. Similar to an indoor wireless LAN deployment, outdoor wireless deployments require the infrastructure to support uninterrupted connectivity as a mobile device roams across a subnet boundary. Cisco offers a Mobile VPN client for handheld devices to facilitate uninterrupted roaming between Wi-Fi subnets. The software client allows applications to stay active when a user travels between wireless (Wi-Fi or cellular) coverage areas. Police, fire, and emergency responders requiring real-time data or video feeds and transportation system telemetry are all examples of situations in which devices need to maintain mobile connectivity across large geographic distances.

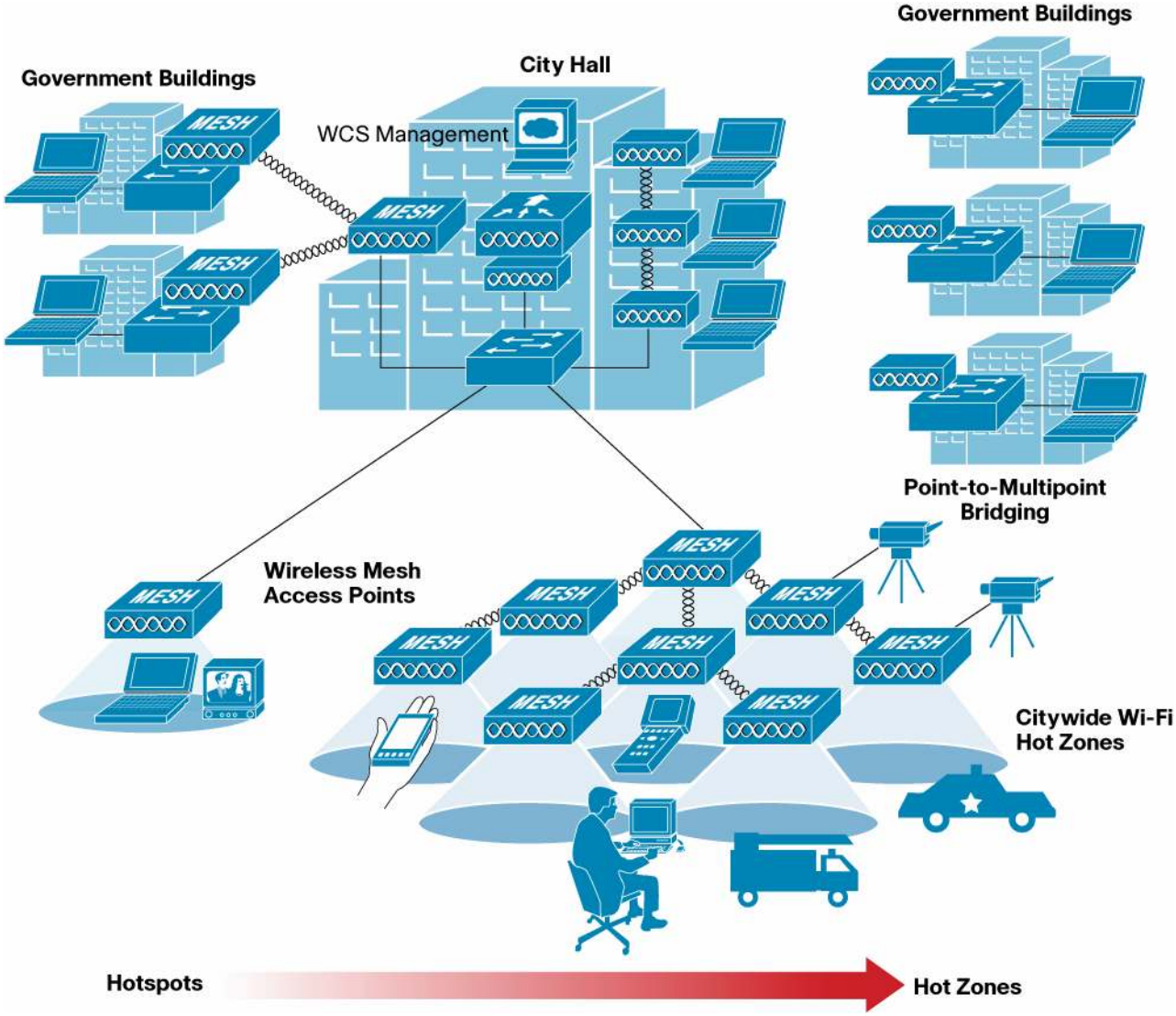
Easy Backhaul Connectivity

There are multiple reasons for limiting the requirement for backhaul to each access point when deploying a hot zone or pervasive Wi-Fi network. Wireless access points typically have a range of 1000 to 2000 feet outdoors, depending on the density of buildings, foliage, and other obstacles; as a result, they must be placed fairly close together to create pervasive coverage. A good average estimate for many suburban cities is 20 to 25 access points per square mile. The higher the access point is placed, the better its range will be. Desirable mounting sites include utility poles, water towers, and the top of city buildings. Existing backhaul at these types of sites is highly unlikely. And the cost of providing network connectivity to these sites is much higher than pulling cable inside a building. To address this problem, linking access points over the wireless medium, also known as mesh networking, allows significant reduction in the number of backhaul points, dramatically reducing the cost of a hot zone or pervasive wireless network.

Cisco Unified Wireless Network Solution for Hot Zones and Pervasive Outdoor Wireless Deployments: Cisco Aironet 1500 Series Lightweight Outdoor Mesh Access Point

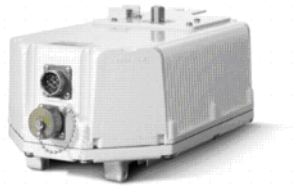
The Cisco Unified Wireless Network meets the two technical requirements for hot zone and pervasive wireless deployments through the Cisco Aironet 1500 Series lightweight outdoor mesh access points, Cisco wireless LAN controllers, and the Cisco Wireless Control System. Figure 2 illustrates the Cisco Aironet 1500 Series outdoor mesh deployment. Figure 3 shows an image of the Cisco Aironet 1500 Series.

Figure 2. Cisco Aironet 1500 Series Outdoor Access Point Deployment



The Cisco Aironet 1500 Series delivers robust connectivity for outdoor wireless LANs. With dual-band, simultaneous support for IEEE 802.11a and 802.11b/g standards, the Cisco Aironet 1500 Series employs a patent-pending Adaptive Wireless Path Protocol to form a dynamic wireless mesh network between remote access points, and delivers secure wireless access to any Wi-Fi-compliant client. Compliant with IEEE 802.11i and Wi-Fi Protected Access 2 (WPA2) and employing hardware-based Advanced Encryption Standard (AES) encryption between wireless nodes, the Cisco Aironet 1500 Series provides end-to-end security.

Figure 3. Cisco Aironet 1500 Series Lightweight Outdoor Mesh Access Point



The Cisco Aironet 1500 Series Lightweight Outdoor Mesh Access Point can be installed anywhere power is available, without the need for a network connection, thus solving the requirement for low-cost backhaul connectivity. Intelligent wireless routing based on the patent-pending Adaptive Wireless Path Protocol, which was designed specifically for wireless environments, enables a remote access point to dynamically optimize the best route to the connected network within the mesh, providing resiliency to interference and helping ensure high network capacity. Deployment and management costs for the Cisco Aironet 1500 Series are reduced through support of zero-configuration deployments and through the ability of the access points to self-heal in response to interference or outages.

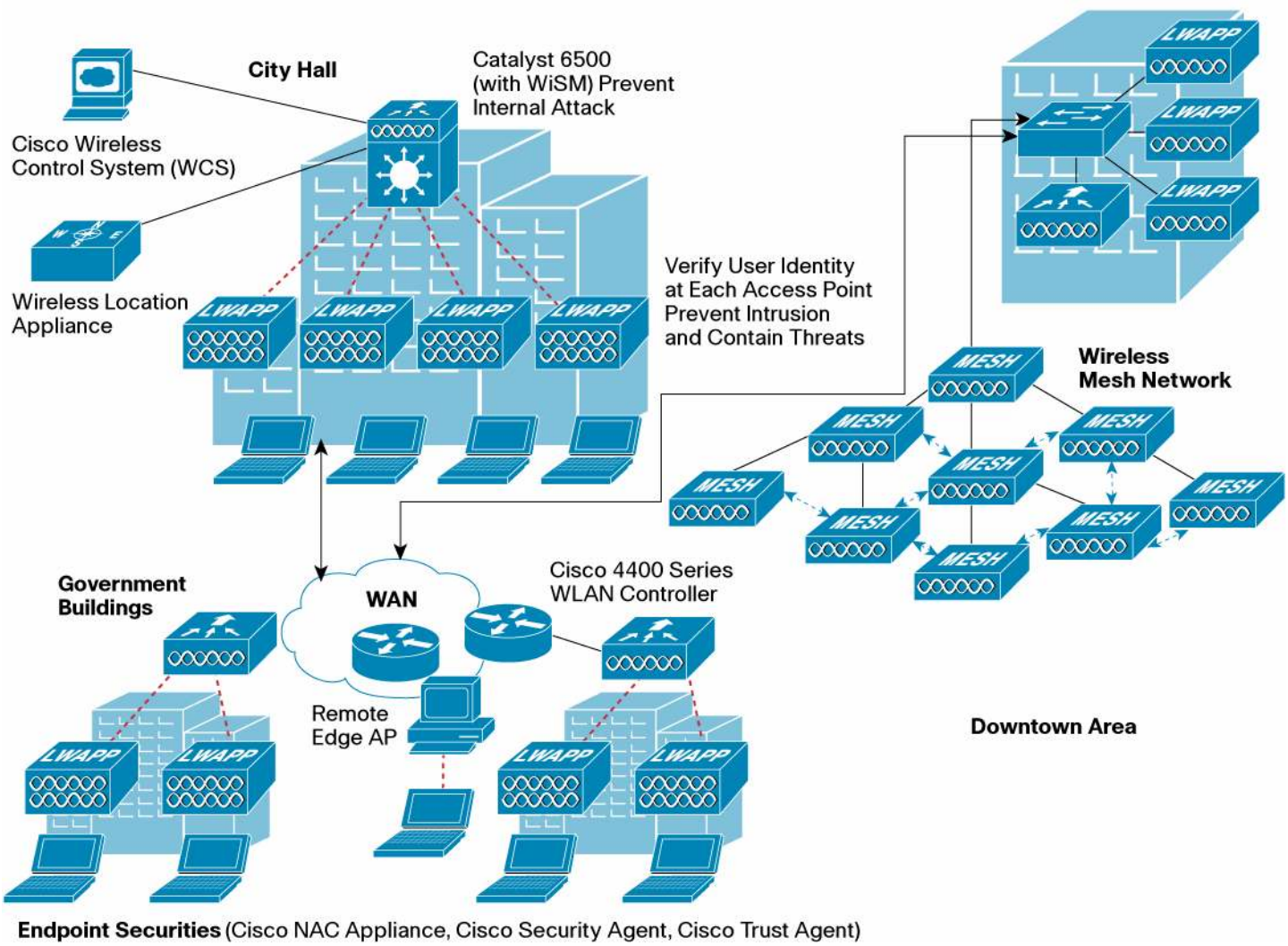
The Cisco Aironet 1500 Series dedicates a radio for access-point-to-access-point communications, allowing the mesh network to maximize use of the total available channels and minimize the occurrence of interference. This results in more capacity than is available with solutions that use only a single radio.

UNIFIED APPROACH FOR INDOOR AND OUTDOOR WIRELESS LAN DEPLOYMENTS

Only Cisco offers a unified approach to deploying indoor and outdoor wireless LANs. The Cisco Unified Wireless Network provides a single platform for management through Cisco wireless LAN controllers and the Cisco Wireless Control System (Figure 4). City and municipal buildings that deploy a wireless LAN indoors can now extend Wi-Fi coverage outdoors to their own campuses or throughout the city itself while maintaining a single interface for monitoring, updates, and troubleshooting. Furthermore, only Cisco offers significantly improved total cost of ownership (TCO) benefits by integrating wireless LAN controller functions in high-performance Cisco routing platforms. Government agencies that already have deployed Cisco Catalyst® 6500 Series switches or Cisco integrated services routers can take further advantage of their investments by adding wireless LAN controller capabilities to these existing platforms.

For more information on reducing TCO with the Cisco Unified Wireless Network, see the white paper *Reducing Large-Scale Enterprise Wireless LAN TCO* at: http://www.cisco.com/en/US/netsol/ns340/ns394/ns348/ns337/networking_solutions_white_paper0900aecd80368807.shtml

Figure 4. A Single Management Platform for Indoor and Outdoor Wireless LAN Deployments



CONCLUSION

Outdoor wireless networks based on IEEE 802.11 can provide a simple, low-cost method for cities and public safety agencies to improve productivity and operate more efficiently, while staying within budget. A variety of applications and users can securely and simultaneously exist on the network, ensuring the fastest possible return on investment. The wireless network delivers a unified, consistent set of network features that allow customers to bring wireless to their existing wired Cisco solutions and to extend intelligent network features and capabilities to mobile users across the city. The Cisco Unified Wireless Network increases the ease of deploying and maintaining outdoor wireless networks, helping to justify the investment for local governments of all sizes.

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 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 the USA C11-339721-01 06/06