# Best Practices for Outdoor Wireless Security

This paper describes security best practices for deploying an outdoor wireless LAN.

Customers are encouraged to migrate to the Cisco IP Phone 7906G when available (approximately May '06). The Cisco IP Phone 7906G will offer a greater feature set than the current Cisco IP Phone 7905G. When ready, information about the replacement product will be found at: http://www.cisco.com/en/US/products/hw/phones/ps379/index.html. Table 3 provides relevant information for migrating to the replacement product.

## CHALLENGE

Many local governments are looking to deploy wireless LANs (WLANs) to help transform their government processes as part of re-engineering efforts. WLANs offer innovative new ways to improve operations and to accelerate communications and service delivery to agency employees and citizens in the community. In addition, outdoor WLANs can extend existing wired-network-oriented services and applications beyond the current physical infrastructures across the city.

Increasingly, mission-critical business applications and services are deployed on open networks with substantial connections to the public Internet. Without proper safeguards and appropriate security measures, Internet connectivity can compromise the gains in productivity that help government agencies become more effective.

As mission-critical information is sent over public and private network infrastructures, security controls and policies for risk mitigation are necessary to ensure that the information is protected and that security level policies meet government regulatory requirements. A well-designed and secure WLAN can help agencies confidently extend the network to mobile workers, law enforcement officers, and citizens, thus improving productivity, enhancing safety, and building new revenue sources.

## SOLUTION

While the idea of a network being physically outside the confines of a building may raise concerns about security, IT administrators can rest assured that with proper measures, outdoor wireless networks can be just as secure as indoor wired and wireless LANs.

### Employ Standard Enterprise Security Methodologies

Public safety and municipal applications conducted over an outdoor wireless network are really an extension of the city's internal network. As such, the same careful provisions used to protect the government network while allowing remote workers to connect at field offices, from home, or on the road should be employed for those personnel accessing the city's network via an outdoor wireless network. The Cisco approach to security is based on the Cisco Self-Defending Network and the SAFE Blueprint architecture which provide integrated secure wired, wireless, data center, and Internet guest access. A security-aware infrastructure is one that will extend from the very core of the network to the end systems. Every device in the network—from mobile devices, to desktops, through the LAN, and across the WAN—plays a part in a globally distributed defense that secures the networked environment. Self-defending networks identify threats; react appropriately to the

severity level; isolate infected servers, desktops, and mobile devices; and reconfigure network resources in response to an attack. Endpoint security applications include Cisco Network Admission Control (NAC), Cisco Security Agent, and Cisco Trust Agent. These technologies provide behavioral protection for PCs and servers to prevent damage from new, previously unknown attacks, and provide posture information about the endpoint where host security policy requires validation prior to permitting network access.

Cisco security solutions are flexible, customizable deployments that use existing investments in platform options (such as dedicated security appliances and router- and switch-based security) and technology options (such as firewalls, threat protection, authentication, authorization, and accounting [AAA], URL filtering, and 802.1x). As Figure 1 illustrates, the components of the Cisco Self-Defending Network work together to protect the network in three areas:

- **Threat defense**, which includes:
  - **Defending the edge**—Using firewalls and intrusion prevention systems (IPSs) to fortify the network edge against intrusion and attack.
  - **Protecting the interior**—Placing safeguards at important points to protect the network against emerging internal attacks.
  - **Guarding the endpoints**—Proactively defending against infection and damage to hosts
- **Trust and identity**, which means ensuring that you always know who is on the network and can control what they have access to
- **Secure communications**, including secure internal and external voice and data communications

**Figure 1.**    Cisco Unified Wireless Network Architecture
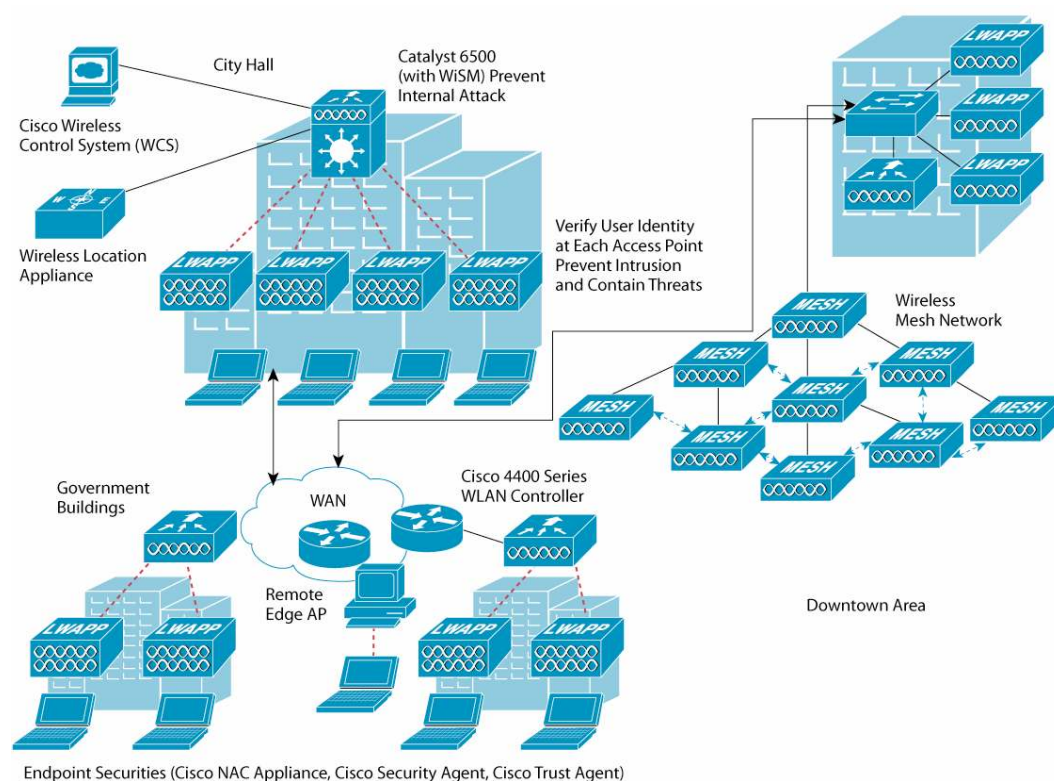
**Using Available Wireless LAN Security Standards and Best Practices**

Securing the WLAN is based on extending the Cisco Self-Defending Network strategy. As with indoor WLANs, outdoor wireless networks should employ the same wireless security best practices to ensure the proper authentication of users on the network and the privacy of the data. The following sections briefly review the best practices for securing a wireless LAN. A more detailed discussion of each of these areas can be found in the white paper *Five Steps to Securing Your Enterprise Wireless LAN and Preventing Wireless Threats.*[1]

**Secure Communications**

The first core principle of the Cisco Self-Defending Network is secure communications. In both wired and wireless environments, this involves both the encryption of data and the authentication of users to the network. Encryption and authentication do not have to be used together, but for most enterprise networks, it is recommended that both be used. A specific exception for outdoor wireless networks is the public usage application, which will be discussed in further detail later. In addition, certain unique characteristics of the wireless medium require adoption of other security techniques to defend the network. These additional security techniques include:

- **Modifying the default SSID**—Changing the manufacturer's default Secure Set Identifier (SSID) prevents casual snoopers from trying to attach to the wireless network. However, public access SSID (guest access SSID) should still be broadcast for public citizen.

- **Set up separate WLAN (SSID/VLAN)**—Could be used to segment different user groups for higher level security policies.

- **Using strong encryption**—Industry-standard Wi-Fi Protected Access (WPA) or WPA2 is preferred if supported by the mobile device. Cisco Aironet® and Cisco Compatible clients (verified to be interoperable with Cisco products through the Cisco Compatible Extensions program) all support WPA and WPA2 out of the box.

- **Deploying mutual authentication between the client and the network**—IEEE 802.1X (the authentication method used by WPA or WPA2) provides robust authentication of the client. An IP Security (IPSec) or Secure Sockets Layer (SSL) VPN will also provide robust mutual authentication.

- **Using VPNs or Wired Equivalent Privacy (WEP) combined with MAC address control lists to secure business-specific devices that do not support WPA or WPA2**—VPNs provide the best protection for the security of the network and device, and are highly recommended. If the mobile device requirement is such that only WEP is supported, it is better to enable this security with regular key rotation and additional MAC address control than to leave the network open.

- **Deploying a lightweight access point architecture that does not store security information locally**—The Cisco Unified Wireless Network is a lightweight access point architecture. This means that sensitive security information is not stored locally in the access points, but centrally in the Cisco wireless LAN controllers. Because the controllers can be deployed inside locked networking closets, they are at much less risk of theft. Any wireless mesh access point that is stolen will not provide any security information that might compromise the network.

---

[1] http://www.cisco.com/en/US/netsol/ns340/ns394/ns348/ns337/
networking_solutions_white_paper0900aecd8042e23b.shtml

- **Ensuring management ports are secured**—Use Simple Network Management Protocol v3 (SNMPv3), Secure Shell (SSH), or Secure Sockets Layer (SSL) to secure management interfaces to the wireless network. A lightweight architecture such as the Cisco Unified Wireless Network is ideal for outdoor wireless networks because all configuration changes are managed centrally through the Cisco Wireless Control System (WCS), which is deployed securely indoors. No configuration changes can be made to Cisco 1500 Series access points over the air. The Cisco WCS also reduces ongoing operating expenses (OpEx) because all updates are accomplished centrally, removing the need for a truck roll to each access point.
- **Physically hiding or securing access points to prevent tampering**—Although they are out in the open, most wireless mesh access points are actually less accessible than those inside an enterprise because of their high mounting location on building rooftops or utility poles. Securely mounting the device further decreases the risk of theft.
- **Change default bridge shared secret**—This will ensure the bridging function is disabled on the mesh access points.

### Threat Control and Containment

The second core principle of the Cisco Self-Defending Network initiative is threat control and containment. The Cisco Unified Wireless Network is designed to actively monitor for and prevent wireless network security types of threats. Cisco Unified Wireless Network access points simultaneously act as air monitors and data forwarding devices, allowing access points to communicate real-time information about the wireless domain, including potential security threats to Cisco wireless LAN controllers, without interrupting service. All security threats are rapidly identified and presented to network administrators through the Cisco WCS, where accurate analysis can take place and corrective action can be taken.

### Policy and Compliance Management

By its very nature, the deployment of an outdoor wireless network creates an amorphous state for the network. Because endpoint devices are outside the city network, monitoring is needed to ensure that system and network policies are not violated and dangerous threats such as viruses, worms, and spyware are not introduced to the government network. Policy and compliance management is the final core principle of the Cisco Self-Defending Network strategy. Proactive monitoring and quarantining is crucial to maintaining network integrity. Without monitoring, IT administrators cannot know if their security policies are enforced. Endpoint visibility and control is needed to help ensure that all wired and wireless devices attempting to access a network meet corporate security policies. Infected or vulnerable endpoints need to be automatically detected, isolated, and cleaned.

Network Admission Control (NAC) is a set of technologies and solutions built on an industry initiative led by Cisco Systems[®]. NAC uses the network infrastructure to enforce security policy compliance on all devices seeking to access network computing resources, thereby limiting damage from emerging security threats such as viruses, worms, and spyware. Customers using NAC can allow network access only to compliant and trusted endpoint devices and can restrict the access of noncompliant devices. Both the Cisco NAC Appliance (Cisco Clean Access) and the Cisco NAC Framework provide security threat protection for wireless LANs. These solutions enforce device security policy compliance when WLAN clients attempt to access the network, by quarantining noncompliant WLAN clients and providing remediation services to ensure

compliance. Both solutions are fully interoperable with the Cisco Unified Wireless Network. Figure 2 illustrates the NAC Appliance architecture for the Cisco Unified Wireless Network. Figure 3 shows the NAC Framework architecture.

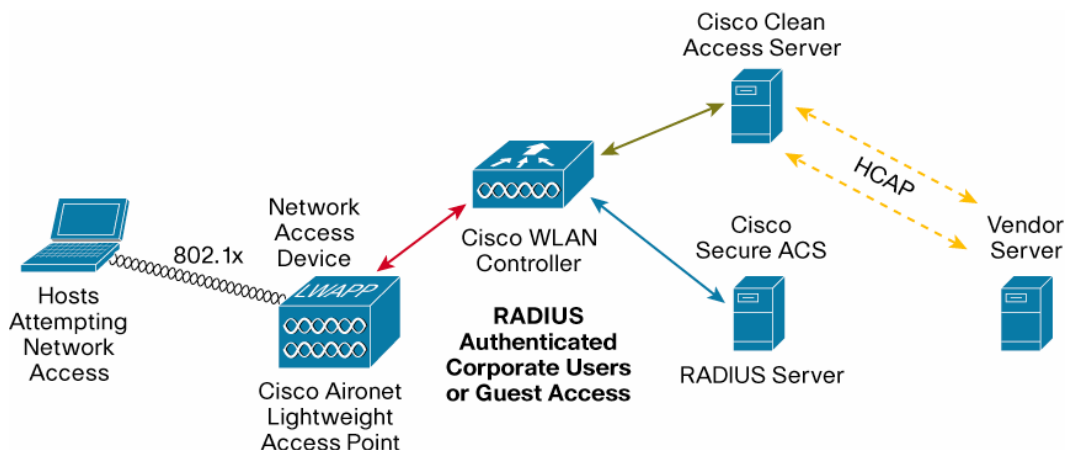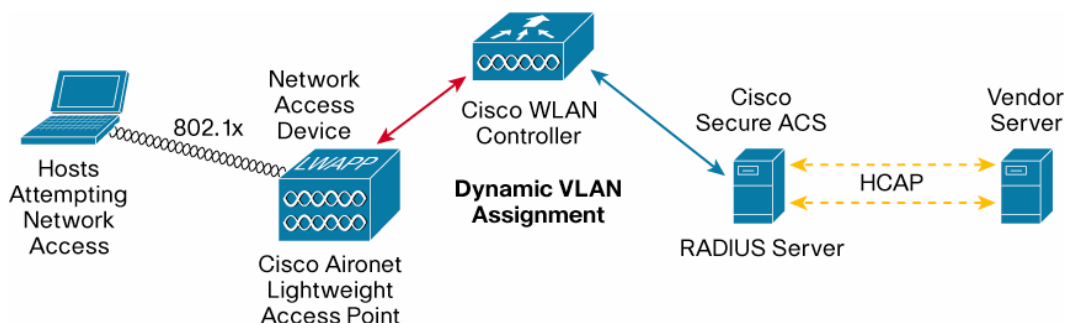**Figure 2.** Cisco NAC Appliance Architecture for Cisco Unified Wireless Network



**Figure 3.** Cisco NAC Framework Architecture for Cisco Unified Wireless Network



**Securing the Mesh Backhaul**

Wireless mesh access points add an additional area of security that must be considered: the wireless link between the access points. If this link is not secure, the network may be at risk.

The Cisco Aironet 1500 Series Lightweight Outdoor Mesh Access Point addresses this concern by providing the highest level of encryption on the mesh access point links. Advanced Encryption Standard (AES) is used to encrypt all communications over the mesh links. This is the same encryption method used in the IEEE 802.11i security standard, which has never been compromised. In addition, each of the mesh access point bridge shared secret and each pair of mesh access points having unique keys.

**Ensuring Municipal and Public Safety Communication Security on Multiuse Networks**

Most city initiatives envision a wireless mesh network that supports multiple users and application types simultaneously. For example, police, building inspectors, and citizens may all concurrently use the network. To support these simultaneous users and applications while maintaining security, the Cisco Unified Wireless Network enables identity networking, in which WLAN policies are assigned and enforced based upon a wireless client's identity, as opposed to its physical location. With identity networking, wireless devices need to authenticate with a WLAN system only once. Context information will follow the devices as they roam, ensuring mobility. When the WLAN is associated with a specific virtual LAN (VLAN), the user can only gain entry to network resources

on that VLAN. As an example, building inspectors might access the wireless mesh network using the SSID "cityhall," which provides access only to specific city databases and e-mail systems. Police personnel might access the wireless network using the SSID "police," which provides access to criminal records and DMV databases. Both of these SSIDs would support strong 802.11i or WPA encryption.

City maintenance workers might incorporate wireless-enabled barcode scanners in their tasks for inventory and field service tracking. These types of devices often do not support today's strong 802.11i or WPA security; instead, they often support the less secure WEP encryption. They too can be segregated on a specific SSID that supports WEP and routes traffic to a VLAN, which only allows access to the specific database or application they are associated with. This, along with frequent encryption key changes and MAC address control lists, mitigates potential security risks.

Finally, many cities are interested in offering a Wi-Fi service to residents, businesses, and tourists. A wireless guest network is an easy way to provide Wi-Fi service while eliminating the need to individually authorize each user. Guest networks use an open security method segregated on a specific SSID that routes traffic to a VLAN that accesses the public Internet only. In this case, the SSID will typically be broadcast so guests can find it without assistance. User login can be accomplished through a captive portal Webpage so that use of the network is audited and any terms and conditions must be agreed to before the guest uses the service.

**Using Specialized Public Safety Security Measures**

The sensitive nature of public safety applications may warrant a further level of security. For emergency situations, the Cisco Unified Wireless Network has the ability to prevent use of the network by nonemergency users. Nonemergency use can be restricted by turning off access to all SSIDs used by nonemergency personnel. In this way, all channels and therefore bandwidth in the network can be dedicated to public safety officials in a time of crisis.

A second permanent method is to distinctly separate public safety communications from municipal or public user communications by allocating a separate portion of the radio spectrum to public safety officials. To address the need for additional privacy when operating in 2.4-GHz/5.8-GHz unlicensed frequency, as well as to help minimize interference, a significant portion of the 4.9-GHz band has been authorized by the FCC for use by public safety agencies. The FCC has authorized the band only for the protection of life, health, and property by public safety agencies. Expected use of this band is for applications such as incident scene management, where mobile data and other emergency applications are required.

As a licensed band, this spectrum offers advantages in terms of privacy and reduced interference that cannot be guaranteed in the unlicensed 802.11 spectrum. Because 4.9-GHz products use a licensed band, the ability of unauthorized end users to connect to the network is greatly reduced. Unlike Wi-Fi solutions, 4.9-GHz products will not be available in retail outlets or on the Web for casual users.

One of the most exciting things about the 4.9-GHz band is that the regulations governing the spectrum have been designed to be identical to those used by wireless LAN products operating in the 5-GHz band. Because only minor modifications are needed to existing 5-GHz 802.11 products, costs will be lower and time-to-market will be faster, helping stretch already tight budgets.

## CONCLUSION

In general, the Cisco Self-Defending Network strategy addresses the outdoor wireless security concerns raised by wireless signal propagation and security threats. The first step is to implement the wired infrastructure using the three principles of secure communications, threat prevention, and policy compliance. The Cisco Unified Wireless Network extends the Cisco Self-Defending Network strategy by delivering specific security measures that are unique to the wireless medium and that also feature the three principles. Employing the Cisco Self-Defending Network strategy for both wired and wireless networks enables outdoor wireless networks to be as safe as allowing city employees to work from remote field offices or at home. For highly sensitive public safety applications, a further layer of preventive measures can be added by employing the licensed 4.9-GHz frequency band, which will distinctly separate communications by public safety officials from those of municipal agencies or public users.