

# SECURING ENTERPRISE AIR: DETECTING ROGUES IN YOUR WIRELESS LAN

TECHNICAL WHITE PAPER

September 2005

**This paper provides an overview of the different types of rogue devices in existing or constituting new wireless LANs (WLANs), the risks faced due to their proliferation, and multiple approaches to detecting and mitigating rogue devices and networks.**

## OVERVIEW

Enterprises that delay the deployment of 802.11 WLANs are facing increasing risks of employees installing their own rogue WLANs onto the enterprise network. Driven by the need for mobility and fueled by the decreasing prices of WLAN hardware, these employees circumvent an enterprise's investment in IT security by plugging a \$60 WLAN access point into an Ethernet jack and connecting a \$50 wireless access card to a station.

These rogue WLANs are easy to install and provide the connectivity that employees seek. However, the end result is a wide-open entry point to the greater enterprise network. A rogue WLAN effectively extends an Ethernet connection to anyone inside and outside the building. Enterprises that have decided not to deploy WLANs must first set a policy banning employees from installing their own wireless networks, and then determine how to enforce that policy.

This paper provides an overview of the risks organizations are facing due to proliferation of rogue WLANs, and describes multiple approaches to detecting and terminating rogue networks.

## INSECURE NATURE OF WLANS

To understand the risks of rogue WLANs, one must first understand the security vulnerabilities of all WLANs. In addition to the new risks introduced by the wireless medium that connects stations and access points, WLANs face all of the security challenges of wired networks.

First, the medium over which a WLAN operates is air, which by its nature is insecure. Additionally, wireless devices self deploy and have the capability to connect to unknown clients and devices. Due to the growth of WLAN-enabled laptops and the increasingly wireless-friendly Windows XP Operating System, laptops in the default setting automatically search

for a wireless connection via any available access point (AP). Lastly, wireless devices are transient in the way they connect. If a wireless device picks up a strong signal, it may connect with the new access point, even if that AP is the laptop of an intruder in the parking lot.

Any wireless AP attached to a wired network essentially broadcasts an Ethernet connection and is a ramp to the entire enterprise network. Layer 1 and Layer 2 of a network is typically protected by the CAT5 wire within a building in a traditional wired network, but is exposed in a WLAN.

Without proper security measures for authentication and encryption, any mobile device with a wireless adapter can connect to the network or stealthily eavesdrop on all network traffic across that AP. Most rogue WLANs are deployed with consumer-grade hardware in default settings that lack basic security measures of encryption, personalized Service Set Identifiers (SSIDs), and Media Access Control (MAC) address filtering.

However, even these basic steps of WLAN security provided by consumer-grade vendors are not sufficient to secure enterprise WLANs, which require encryption beyond WEP, additional access control filtering, intrusion detection, and 24x7 monitoring.

## WHAT IS AT RISK?

Wireless computing has had a profound impact on information security. In many enterprises it has accelerated the concept of the "disappearing perimeter." Previously,

**“Rogues can be hardware or software, access points or peer devices. All may expose and bridge networks.”**

*Gartner, February 2004*

malicious users would compromise networks by tunneling in through the Internet perimeter, gaining physical wired access to the network on premises, or deceiving users into downloading software that has a negative impact on their systems. Wi-Fi has given rise to a new class of attacks that can breach defenses without accessing the physical premises or triggering sophisticated perimeter firewall alarms.

War driving — driving around with a laptop or a PDA in one’s vehicle to detect Wi-Fi wireless networks — enables hackers to obtain unauthorized access to corporate resources and proprietary intellectual property. The login credentials of legitimate wireless users can be sniffed or cracked. Malicious insiders can move throughout an enterprise network with impunity via sessions with insecure wireless access points.

The consequences of these risks are significant. Spammers and phishers (people who send out e-mails that appear to be from a legitimate and trusted source to obtain personal and other information from recipients) can leverage open access points to send unsolicited and malicious e-mail in stealth mode. Worms can be introduced through a new infection vector. Customer lists and account numbers may be downloaded to portable devices. Enterprise databases may be accessed and modified by unauthorized users. The bottom line is, wireless insecurity that goes unaddressed can lead to theft of data, lower productivity, and quantifiable financial losses.

Once accessed, an unsecured WLAN can compromise:

- Financial data, leading to financial loss
- Reputation, damaging the efforts spent building the brand
- Proprietary information, leaking trade secrets or patents
- Regulatory information, foregoing customer privacy or ignoring government mandates

...all which could cause legal ramifications.

## **EVOLUTION OF ROGUE WLANS**

Just as employees first brought personal computers to the office in the 1980s for their many benefits, and brought personal modems in the 1990s, employees are installing their own WLANs to corporate networks when IT departments are slow to adopt the new technology. Even enterprises that are deploying WLANs must tackle the problem of rogue WLANs set up by employees who do not yet have wireless access, or vendors operating within the office.

WLANs are comprised of access points that are attached to the enterprise network and WLAN access cards for laptops, hand-held devices, and desktop computers. Both unauthorized access points and unauthorized activity from WLAN access cards can pose significant security risks.

### **Rogue access points**

Rogue WLANs most commonly refer to rogue access points, which broadcast a network connection when attached to the corporate network. A rogue access point is any access point unsanctioned by network administrators. Most rogue access points are improperly secured with default configurations that are designed to function right out of the box, without any security features activated. Employees or even business units seeking to enhance their productivity deploy rogue access points innocently, without comprehending overall security risks.

### **Laptops with built-in WLAN access cards**

Major computer vendors are selling an increasing number of laptops with built-in WLAN access cards. A rogue WLAN has traditionally been thought of as a physical access point unsanctioned by network administrators. Today, rogue WLANs are further defined as laptops, handhelds with wireless cards, barcode scanners, printers, copiers or any WLAN device. These devices have little to no security built in, making it easy for intruders to find an entry point. Wireless-enabled laptops can pose several security risks from accidental associations with neighboring networks and ad-hoc, peer-to-peer networks.



**“Once a hacker is associated with a LAN, the hacker is in that LAN and difficult to detect.”**

*Gartner, February 2004*

#### **Accidental and malicious associations**

Accidental associations are created when a neighboring access point across the street or on adjacent floors of a building bleeds over into another organization’s air space, triggering its wireless devices to connect. Once those devices connect with the neighboring network, the neighbor has access back into the organization. Accidental associations between a station and a neighboring WLAN are recognized as a security concern. A malicious association is when a company laptop is induced to connect with a malicious device such as a soft AP or laptop. The scenario also exists when a malicious laptop connects with a sanctioned AP. Once the association has been made, the hacker can use the wireless device as a launch pad to attack servers and other systems on the corporate network.

#### **Ad-hoc networks**

Similar to rogue access points, ad hoc wireless networks represent another major concern for WLAN security because they can put a network at risk without security managers ever seeing the vulnerability. WLAN cards enable peer-to-peer networking between laptops without an access point. These ad hoc networks can allow an authorized user to transfer private corporate documents and intellectual property to unauthorized users without going over the corporate network. While WLAN cards operate in ad hoc mode, the user must be able to trust all stations within range because ad hoc networks offer little or no authentication management. Any station can connect directly to an authorized user, and thus gain access to the entire network.

#### **REQUIREMENTS TO DETECT ROGUE WLANS**

When an organization’s network is left exposed by insecure WLAN devices, hackers can compromise an organization’s network backbone, rendering the investment in IT security useless. Not only are there financial implications from a security standpoint, the breach can potentially impact the company’s reputation and proprietary and regulatory information. These scenarios can lead to additional financial loss and legal ramifications.

Hence various regulatory bodies have defined policies that require compliance. Regardless of the WLAN deployment status, organizations have to ensure that they track all wireless activity and prevent the transmission of wireless data in clear text.

The Department of Defense (DoD) issued a wireless directive, Number 8100.2 on April 14, 2004. This directive establishes policy and assigns responsibilities for the use of commercial wireless devices, services, and technologies in the DoD Global Information Grid. Healthcare organizations have to main the sanctity of patient data by complying with the HIPAA regulations. Various regulations, such as the OCC Wireless Advisory and the GLBA – Safeguards Rule, have been defined for banking and financial institutions. A new section of the Sarbanes- Oxley Act, Section 404, requires all publicly traded firms to file an internal control statement which must attest to management’s responsibility for establishing and maintaining adequate internal control over financial reporting for the company. While corporate officers are accountable, IT systems and infrastructure are critical to the financial reporting process, and the burden falls on the IT department to ensure integrity of the established processes. The IT department must document, test, monitor and report the effectiveness of internal control processes.

In confronting the issue of rogue WLAN detection, the buyer must consider the functional requirements and return on investment (ROI) of the solution. In confronting the issue of rogue WLAN detection and protection, IT security managers should evaluate various approaches based upon technical requirements, enterprise scalability, cost, and ability to cover the future needs of network security. Securing an enterprise wireless network is not merely a matter of purchasing a few point solutions. Instead, there are a number of considerations that must be made to ensure that the network is optimized to fulfill your business objectives, and to do so securely.

### **Functional requirements**

A comprehensive solution to detect rogue WLANs must detect all WLAN hardware and activity that includes:

- Detection of all rogue devices and associations
- Detailed analysis of rogue devices and associations
- Assessment of threat of rogue devices
- Location of rogue devices
- Termination of devices

### **Scalable and cost effective for the enterprise**

Rogue detection must scale to fit the specific needs of an enterprise. Some basic solutions work for smaller organizations and provide rogue detection and basic rogue containment features. These basic solutions are built into the wireless access point. Large enterprises also require a cost-effective solution that can be centrally managed and goes beyond just rogue detection to provide enhanced and effective rogue containment and RF security. In determining the cost of rogue detection, IT security managers must consider the initial costs of the solution and additional costs needed for on-going support.

### **Scales to cover future requirements**

Rogue detection should scale to meet the future needs of enterprise network security. An organization that bans all WLANs today is likely to move ahead with a pilot deployment in the next year. At this time, an enterprise with pilot WLANs deployed only in specific areas of the business must maintain its rogue detection for unauthorized areas and secure the pilot WLANs from accidental associations and ad-hoc networks. As WLANs are deployed throughout an enterprise, rogue detection must be complemented with 24x7 monitoring and intrusion detection.

#### *Detection of rogue and sanctioned devices*

First, the organization has to monitor what is happening in its airspace. To properly secure the airwaves, organizations need a comprehensive solution to detect all WLAN hardware and WLAN activity. This includes detecting hardware APs, software APs, WLAN stations, probing laptops and stations in ad hoc mode. The inventory process cannot be accomplished without a solution that supports 802.11a, b and g protocols. Taking an inventory of the air space is a form of asset management, in which the network administrator should be able to authorize access points and

stations on the network. The network administrator also has to identify APs on neighboring networks and ignore activity from them as needed.

#### *Detection of associations of devices*

Stations can connect to authorized or unauthorized APs or to other stations, forming an ad hoc network. A monitoring system should monitor these associations, and report both allowed relationships as well as restricted relationships that should be prevented or terminated.

#### *Notification services*

A system should provide multiple notification options for alarms. This includes notifications via e-mail or digital pagers, SNMP traps to SNMP managers, and integration with other systems via Syslog.

#### *General and forensic analysis of rogue devices and incidents*

Once the system has identified a rogue AP and the associations it has made, it is important for a system to analyze the data. Consider a spy inside a corporation. Finding a spy is not necessarily sufficient information. The corporation will want to know when the spy entered and what the spy found out or accomplished. This is information, similar to identifying a rogue that will be helpful in determining the appropriate course of action. Information that is important to gather on a rogue includes time of entry, what it connected with and for how long. It is also important to note what data and how much of it was exchanged. Typically this information can be reviewed on a periodic basis, but to assess the nature of a particular instance, the system should provide the ability to analyze data down to the minute.

#### *Action on rogue devices*

Once a rogue AP, station or association has been identified, the solution should offer the ability to disconnect the activity from a centrally managed location.

#### *Detect leakage of wired network traffic*

Access points can behave like simple bridges that take information from the wired side and pass it to the wireless

side. Unless the access point is properly configured and installed with the right gateways, they can leak sensitive information, network protocols and/or multicast and broadcast traffic in the air. For example, if spanning tree protocol information is leaked, freeware tools can sniff this information and launch a spanning tree attack. These types of attacks can meltdown the network backbone. A monitoring system should detect if and what network protocol is leaking in the air. This information will allow the network manager the knowledge to take corrective action.

#### *Reporting*

The solution should offer real-time reporting and the ability to produce automated weekly, daily and down-to-the-minute reports to provide information about the security and performance of the network. The reports should have the ability to be broken down by locations, departments and groups.

### **Technical Requirements**

#### *Architecture*

An organization looking to deploy a wireless security system that can accomplish all of the above functional requirements should look for a distributed architecture with sensors and servers that are centrally managed.

#### *Server*

To deploy a centrally managed solution, the solution should be easy to deploy and complete with operational and database information. The solution must have a failover system in place to compensate for primary server failure. Additionally, the server should run on a hardened operating system so that it cannot be easily compromised or attacked.

#### *Sensor*

A centrally managed system is only as good as a sensor is reliable. Sensors should be guards, passing information to the server. Sensors must be able to monitor both 2.4GHz (802.11 b and g) and 5 GHz (802.11a) simultaneously. Sensors must have authentication and encryption to prevent secure communications from being compromised. Additionally, sensors must have bandwidth control to prevent the sensor from clogging WAN bandwidth.

#### *Deployment*

Sensors should be “plug and play”, requiring minimum configuration and installation. The sensors should not require an IT organization to modify its wired network configuration or firewall settings.

#### *Ongoing maintenance*

The solution should have the ability to perform mass updates of firmware. As an example, imagine an organization with 300 sensors deployed worldwide.

In order to upgrade the sensors with the latest updates, the system should be able to download the patch from a centrally managed location.

#### *System health monitoring*

Using a centralized server approach, companies can see when a sensor goes down, when a sensor is having problems, or if the server is not functioning properly.

#### *Return on Investment (ROI)*

The overall cost of a solution and the ROI are two important considerations. When looking at the overall cost, it is important to consider the total cost of ownership, including the:

- Upfront cost of acquiring hardware, operating system, database and other associated software
- Cost of installing, hardening and securing the server, sensors and communication between the two
- Ongoing support and maintenance costs, including updates to the sensors and server

### **FIVE APPROACHES TO DETECT ROGUE WLANS**

Once an organization decides on a policy that bans WLANs completely, or more precisely prohibits employees from deploying their own networks, the organization must decide how to enforce that policy across the enterprise. This section outlines five approaches to detect rogue WLANs:

- 1.) Wired-side Intrusion Detection System
- 2.) Wired-side SNMP polling
- 3.) Wired-side network scanners
- 4.) Wireless scanners and sniffers
- 5.) 24x7 monitoring and centralized management for enterprise rogue detection

#### **Wired-side Intrusion Detection System (IDS)**

A wired-side intrusion detection system (IDS) offers absolutely zero ability to detect rogue WLANs, but can be useful in a limited capacity. While intruders entering the network through a rogue WLAN appear mostly as authorized users, wired-side IDS may alert IT security managers when the intruder tests wired-side security measures. A wired-side IDS fails as an effective approach to detecting rogue WLANs because it cannot identify access points attached to the wired network, soft APs, accidental associations and ad hoc networks.

### **Wired-side SNMP Polling**

Simple Network Management Protocol (SNMP) polling can be used to query information from IP devices attached to the wired network, such as routers, stations, and authorized access points. This process requires the IT security manager conducting the SNMP poll to know the IP address of all devices being polled, which must also be configured to enable SNMP. For these reasons, SNMP polling is not an effective approach to detecting rogue WLANs. The IT security manager is not likely to know the IP address of the rogue access point, and the rogue access point is not likely to have SNMP enabled. In addition, an SNMP poll against an authorized station that is operating as a soft AP would not detect any WLAN activity. SNMP polling also would not detect accidental associations or ad hoc networking between stations.

### **Wired-side network scanners**

Wired-side network scanners work similar to SNMP polling, identifying IP devices attached to the network and key characteristics of those devices, such as MAC addresses and open ports. Rather than the SNMP protocol, scanners typically use TCP fingerprints to identify various types of devices. Network scans can also be extremely intrusive in that they require an IT security manager have access to all the IP devices on the network and to know all their IP addresses. To locate every rogue access point, a scan would have to be performed on the entire network, which would cause personal firewall alerts and multiple alarms from network intrusion detection systems. Wired-side network scanners are not an effective solution for enterprise rogue WLAN detection because wired-side scanners:

- Require an accurate database of all IP devices
- Are limited to subnets unless routers are reconfigured
- Produce multiple false positives from network IDS and personal firewalls
- Cannot detect soft APs, accidental associations, or ad hoc networks

### **Wireless scanners and sniffers**

Wireless sniffers and scanners differ greatly from wired-side tools because they capture and analyze WLAN packets from the air. By monitoring the airwaves for all WLAN activity, wireless sniffers and scanners detect most access points and active wireless stations within range. They also can provide detailed information about the configuration and security employed by each device.

Both sniffers and scanners are limited by their need for a network administrator to physically walk the area with a laptop or hand-held device that is running the sniffer or scanner application. A research brief from META Group questioned the viability of wireless sniffers and scanners for enterprise security.

While this process requires the physical presence and valuable time of a network manager, the effectiveness is limited because it only samples the airwaves for threats. New rogue access points and other vulnerabilities can arise after a scan and will not be detected until the next time a network administrator surveys the network. This approach is particularly unreasonable for enterprises operating dozens of offices around the country or retailers with hundreds of stores. Even if these organizations could feasibly devote a network administrator's full attention to survey each site on a monthly basis, rogue access points and other vulnerabilities could pop up the minute the survey is completed.

Smaller organizations operating in a single location without potential for growth may find sniffers and scanners to be their most cost-effective solution if the organization is willing to accept the threat of rogue WLANs popping up between network audits.

The vast limitations of physical site surveys and the demands for personnel time limit the effectiveness of sniffers and scanners for large enterprises. Sniffers and scanners simply are not cost-effective for an enterprise with multiple locations or sensitive information that cannot risk rogue networks operating between security audits. In addition, IT security administrators would find this decentralized approach extremely difficult to manage and collect information from multiple locations.

### **24x7 monitoring and centralized management for enterprise rogue detection – Symbol Wireless IPS**

Enterprise class rogue WLAN detection requires a scalable solution that combines the centralized management of wired-side scanners and radio frequency analysis of wireless scanners. Symbol Wireless IPS provides this comprehensive solution with an innovative approach to WLAN security that includes a distributed architecture of remote sensors to monitor the airwaves for all WLAN activity, and to report that activity back to a centrally managed server appliance.

Symbol AP300 Access Points, configured as remote sensors, are equivalent to wireless scanners but add 24x7 monitoring to provide 100 percent coverage against rogue WLANs the moment they are connected to the network, or

enter the coverage area. This approach to rogue WLAN detection and mitigation is akin to the physical security of buildings whereby video cameras are deployed at key locations for 24x7 monitoring, and a central security station analyzes the incoming video for security risks. The video cameras reduce the need for costly security guards to walk through the

building, just as the remote sensors of Symbol Wireless IPS replace the need for wireless scanners.

The centralized management and 24x7 monitoring of the airwaves provides a scalable and cost-effective solution

**Figure 2: Symbol Wireless IPS Architecture: Comprehensive WLAN Security**

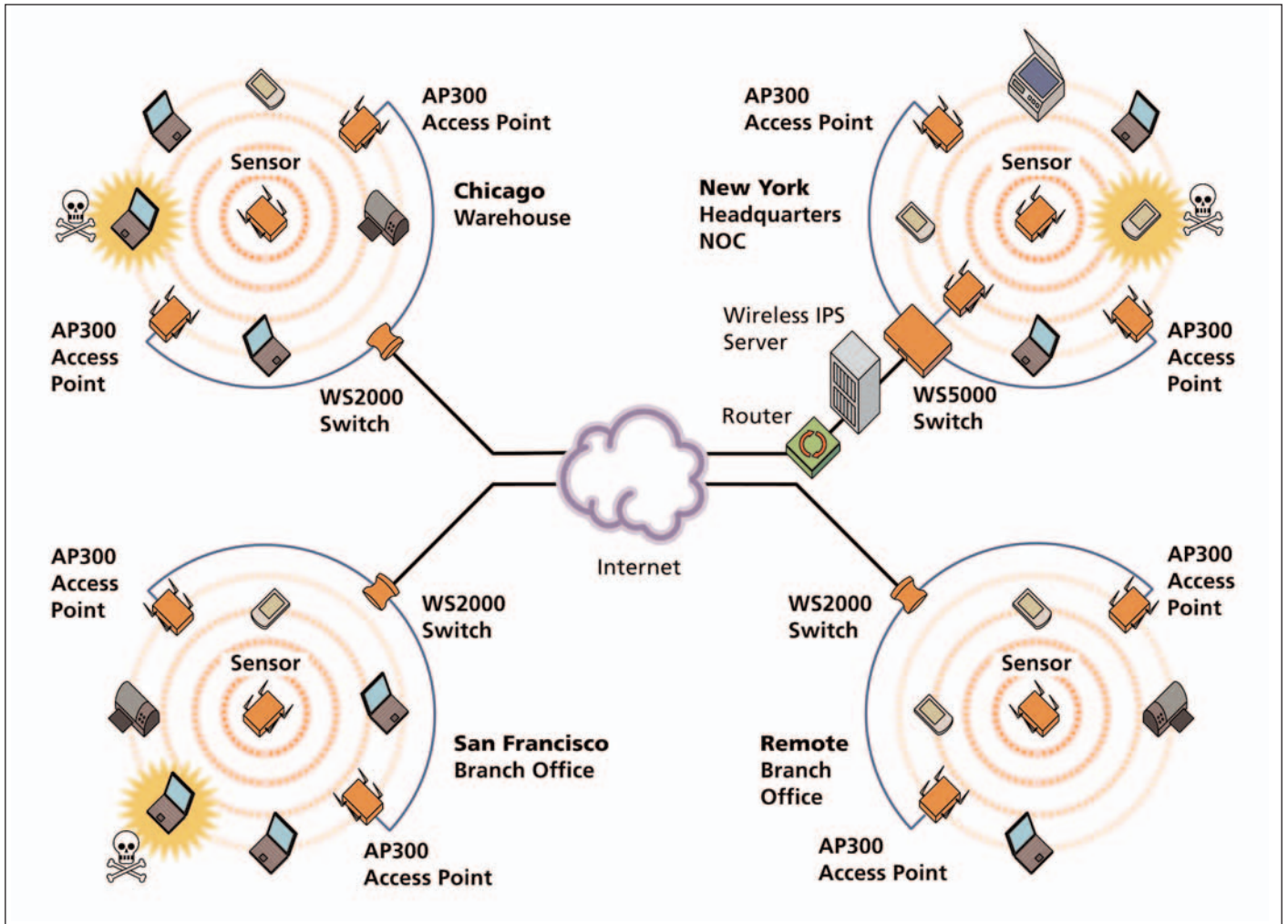


Figure 2 illustrates how Symbol Wireless IPS secures and protects all enterprise locations from rogue access.

that enables enterprise WLAN detection throughout multiple locations of an organization. A few sensors are deployed in each location to provide comprehensive, 24x7 detection of rogue WLANs. As new offices are opened, Symbol Wireless IPS easily scales to secure that office with the addition of a sensor deployed in the new location. Symbol provides comprehensive and advanced rogue management capabilities that go beyond simple alerts of broadcasting access points. For more details on the Symbol wireless IPS solution, please visit our website.

Symbol also offers rogue detection features in its award winning wireless switch platforms, the WS2000 and the WS5100. The Wireless Switch WS5100 from Symbol Technologies delivers security and scalability, manageability, availability, reliability and total cost of ownership (TCO) savings. The Wireless Switch WS5100 redefines the standard for enterprise class wireless networks, delivering extensive functionality, security, scalability and management at a much lower total cost of ownership than first-generation access point-based networks. By centralizing intelligence that was previously distributed throughout a wireless network via access points, this second generation wireless switch architecture delivers an unparalleled level of WLAN control, performance and management simplicity.

The WS 2000 Wireless Switch from Symbol Technologies is an integrated wired and wireless networking solution, priced and designed to meet the needs of healthcare clinics, schools and colleges to warehouses, branch offices of government agencies, retail stores, manufacturing plants and more. Built on the same centralized packet switching architecture as Symbol's award-winning WS 5000 Wireless Switch, the WS 2000 offers enterprise class security (802.11i, site-to-site IPSec VPN), public/private network segmentation and 802.11abg standards support. The WS2000 provides:

- Extensive WLAN functionality and high performance
- Power and simplicity of centralized remote management
- Ability to scale to support future growth

## CONCLUSION

It is becoming harder to find a laptop without a built-in wireless access card. And for a mere \$50, an employee can purchase and plug a WLAN access point into an Ethernet jack, providing a wireless gateway into a wired network. As wireless networks become ubiquitous extensions of

wired networks, the threat of intruders becomes more pervasive. But it is no longer the rogue APs companies are concerned about, but rather the evolution of the rogue and the association rogues are able to make with devices on the corporate network.

The risks and costs to corporations are increasing as a function of the growing number of Wi-Fi devices and associations. This "Wi-Fi Effect" is creating ramifications far beyond convenience and efficiency of employees. It is demanding continuous monitoring of the wireless network to ensure rogue APs and unsanctioned associations are prevented. Wireless scanners, freeware, and SNMP polling, while useful for troubleshooting wired networks or pinpointing the exact location of an access point, do not have the technical or functional capabilities to meet the needs of a global wireless-enabled organization. The answer is a centrally managed, distributed monitoring solution.

### **Symbol WIPS — centrally managed 24x7 distributed monitoring**

Wireless IPS is the comprehensive WLAN security and monitoring solution based on patent-pending technology that incorporates distributed sensors and a server appliance built for enterprise deployment. The remote sensors monitor all WLAN activities 24x7 and communicate with the server, which correlates and analyzes the data to provide scalable, centralized management of real-time rogue detection, policy enforcement, intrusion protection and health monitoring of the WLAN. Using wireless technology means total freedom from the constraints of wired environments. However, more than 90% of mobile devices lack protection, according to industry analyst firm Gartner, leaving an open door for intruders to come into the corporate network. Symbol allows corporations to understand what devices are present in their air space, and how and to whom the devices communicate. By identifying security holes and back doors created by innocent users or intruders using wireless, Symbol's holistic approach to monitoring ensures that WLAN

policies are being enforced across all stations and access points, enabling organizations to create a secure environment. Organizations spend millions of dollars securing their wired network. When an organization's network is left exposed by insecure or rogue WLANs, hackers can compromise an organization's network backbone, rendering the IT investment in wired security useless. Symbol's Wireless IPS is the industry's leading monitoring solution that enables companies to take proactive steps to close any security holes or back doors, mitigating the risk of security breaches and preserving previous security investments.

## **REFERENCE AND FURTHER READING**

### **Securing Enterprise Air: Understanding and Achieving Next-Generation Wireless Security with Symbol Technologies and 802.11i**

*[http://www.symbol.com/category.php?fileName=WP-27\\_enterprise\\_air.xml](http://www.symbol.com/category.php?fileName=WP-27_enterprise_air.xml)*

### **The Use of Digital Certificates for Authentication to a Wireless LAN**

*[http://www.symbol.com/products/whitepapers/digital\\_certificates.html](http://www.symbol.com/products/whitepapers/digital_certificates.html)*



## About Symbol Technologies

Symbol Technologies, Inc., The Enterprise Mobility Company™, manufactures and services enterprise mobility systems, delivering products and solutions that capture, move and manage information in real time to and from the point of business activity. Symbol enterprise mobility solutions integrate advanced data capture products, radio frequency identification technology, mobile computing platforms, wireless infrastructure, mobility software and services programs under the Symbol Enterprise Mobility Services brand. Symbol enterprise mobility products and solutions are designed to increase workforce productivity, reduce operating costs, drive operational efficiencies and realize competitive advantages for the world's leading companies.



### *Corporate Headquarters*

**Symbol Technologies, Inc.**  
One Symbol Plaza  
Holtsville, NY 11742-1300  
TEL: +1.800.722.6234/+1.631.738.2400  
FAX: +1.631.738.5990

### *For Asia Pacific Area*

**Symbol Technologies Asia, Inc.**  
(Singapore Branch)  
Asia Pacific Division  
230 Victoria Street #05-07/09  
Bugis Junction Office Tower  
Singapore 188024  
TEL: +65.6796.9600  
FAX: +65.6337.6488

### *For Europe, Middle East and Africa*

**Symbol Technologies**  
EMEA Division  
Symbol Place, Winnersh Triangle  
Berkshire, England RG41 5TP  
TEL: +44.118.9457000  
FAX: +44.118.9457500

### *For North America, Latin America and Canada*

**Symbol Technologies**  
The Americas  
One Symbol Plaza  
Holtsville, NY 11742-1300  
TEL: +1.800.722.6234/+1.631.738.2400  
FAX: +1.631.738.5990

### **Symbol Website**

For a complete list of Symbol subsidiaries and business partners worldwide contact us at:  
**[www.symbol.com](http://www.symbol.com)**  
Or contact our pre-sales team at:  
**[www.symbol.com/sales](http://www.symbol.com/sales)**



WP-ROGUES 09/05

Part No. WP-ROGUES Printed in USA 09/05 © Copyright 2005 Symbol Technologies, Inc. All rights reserved. Symbol is an ISO 9001 and ISO 9002 UKAS, RVC, and RAB Registered company, as scope definitions apply. Specifications are subject to change without notice. Symbol® is a registered trademark, and The Enterprise Mobility Company is a trademark of Symbol Technologies, Inc. All other trademarks and service marks are proprietary to their respective owners. For system, product or services availability and specific information within your country, please contact your local Symbol Technologies office or Business Partner.