

## CISCO STRUCTURED WIRELESS-AWARE NETWORK

The Cisco® Structured Wireless-Aware Network (SWAN) allows enterprise and service provider network managers to deploy, operate, manage, and secure several, hundreds, or thousands of access points, across a variety of different industries or deployment scenarios. Cisco SWAN extends “wireless awareness” into important elements of the network infrastructure, providing the same level of security, scalability, reliability, ease of deployment, and management for wireless LANs that organizations have come to expect from their wired LANs.

### CHALLENGE

The popularity of wireless LANs (WLANs) has created new challenges for today’s networking professionals. These individuals must respond to the growing demand for enterprise WLANs from end users who have embraced the freedom and flexibility of wireless connectivity, and from business executives who recognize the competitive advantages of business critical mobile applications.

Many organizations are finding that they can no longer choose not to deploy WLANs. They need to make better use of their resources by delivering secure access to business critical information instantly, in several locations, and to numerous users. Organizations are deploying WLANs to enable increased employee productivity, better inform employees, improve employee responsiveness to customers, and enhance employee collaboration.

Networking professionals responding to the growing demand for WLANs are finding that WLANs must be integrated into existing wired networks and must scale to support hundreds to thousands of users located in campuses and remote sites spread over great distances. Organizations are demanding a highly available medium that meets the expectations of enterprise users that are accustomed to the high availability of wired networks. In an era of tight budgets, enterprise network managers need to deliver enterprise-class mobile computing applications across many locations with solid network security, mobility, and control, while achieving the lowest total cost of ownership (TCO).

IT managers are discovering that in the absence of WLANs provided by the organization, employees are establishing their own WLANs using rogue (unauthorized) access points. These rogue access points are creating security breaches that put the entire network at risk. Network managers need to be able to detect and suppress these rogue access points.

A WLAN solution that takes full advantage of existing tools, knowledge, resources, and the wired infrastructure to address critical WLAN security, deployment, and control issues is needed. Network managers need a solution that provides them with the control they need to effectively manage their wired and wireless infrastructures and to keep their networks secure.

## SOLUTION

### Cisco Structured Wireless-Aware Network

The Cisco Structured Wireless-Aware Network (SWAN) allows enterprise and service provider network managers to deploy, operate, manage, and secure several, hundreds, or thousands of access points across a variety of different industries or deployment scenarios. From small businesses to large-scale enterprise multinational companies; within WLAN campus deployments or branch offices; at universities; in retail, manufacturing, or healthcare industries; or at hot spot locations, Cisco SWAN provides the framework to integrate and extend wired and wireless networks to deliver the lowest possible total cost of ownership for companies deploying WLANs.

Cisco SWAN extends “wireless awareness” into important elements of the network infrastructure, providing the same level of security, scalability, reliability, ease of deployment, and management for wireless LANs that organizations have come to expect from their wired LANs. The framework reduces overall operational expenses by simplifying network deployment, operations and management. Cisco SWAN’s flexibility allows network managers to design networks to meet their specific needs, whether implementing a highly integrated network design or a simple overlay network.

### Cisco SWAN Components

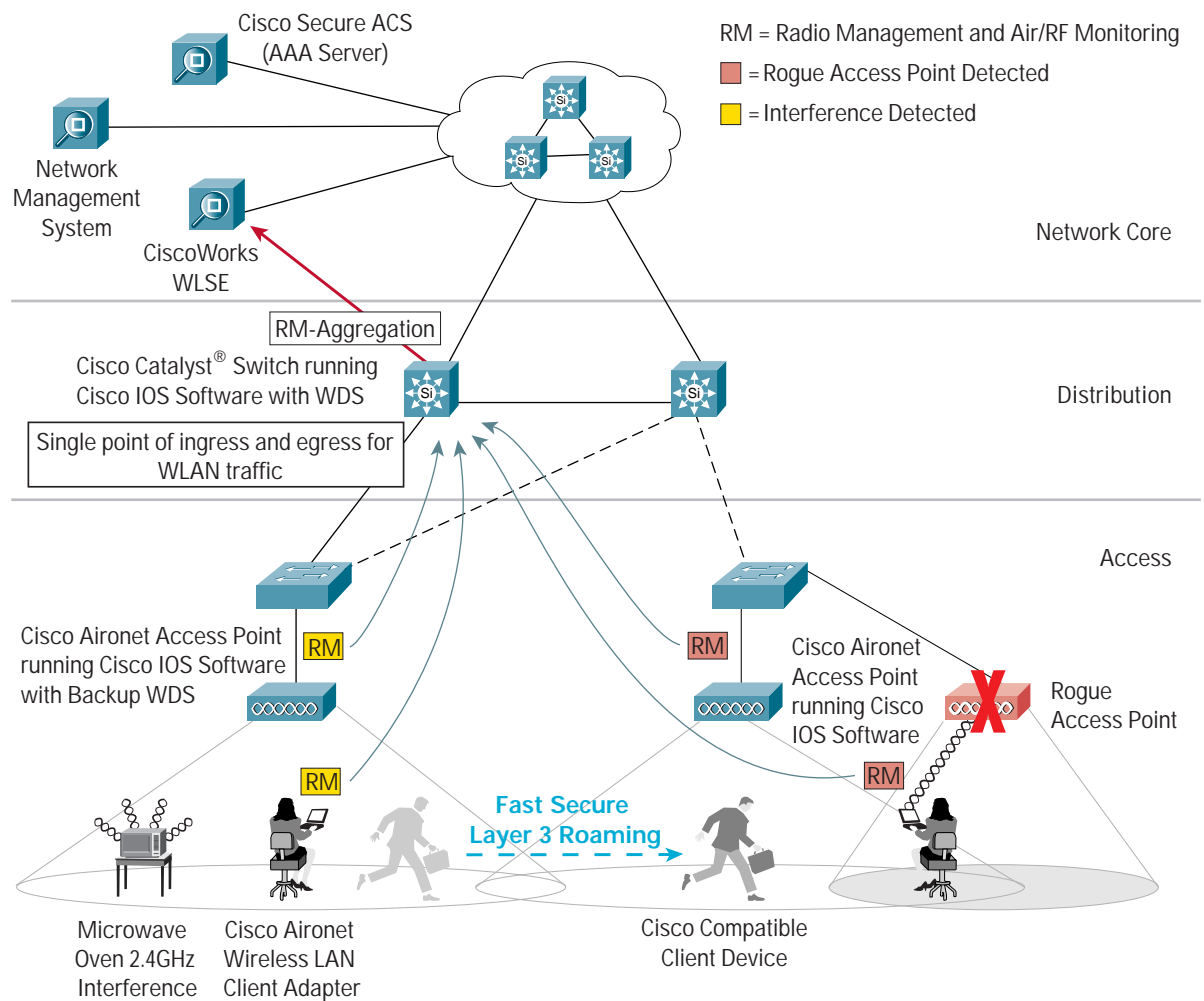
There are four components to the Cisco SWAN framework—access points; management and security servers; WLAN client devices; and infrastructure devices.

- *Cisco Aironet® Series WLAN access points running Cisco IOS® Software*—Cisco Aironet access points are required. These access points offer secure, manageable, and reliable wireless connectivity with exceptional range and performance, as well as integrated radio frequency (RF) management.
- *Management and security servers*—The CiscoWorks Wireless LAN Solution Engine (WLSE) and an IEEE 802.1X authentication server, such as Cisco Secure Access Control Server (ACS), are required to manage and secure the wireless network. These products simplify the deployment and management of the WLAN infrastructure and implement an enterprise-class security solution.
- *WLAN client devices*—Wi-Fi Certified or IEEE 802.11 clients are required. Using Cisco Aironet or Cisco Compatible client devices provides additional benefits, including advanced enterprise-class security, extended air RF radio management, and enhanced interoperability.
- *Infrastructure devices*—As Cisco incorporates wireless capabilities into its switches and routers, customers receive a unified network system that extends to wireless traffic all of the enterprise-class scalability, security, reliability, and simplified manageability of the wired infrastructure. The result of this wired and wireless integration is a lower overall total cost of ownership since existing routers and switches are used for WLAN support, obviating the need for unfamiliar and unproven WLAN point products.

## Cisco SWAN Deployment

Cisco SWAN is deployable today. Network managers can design the Cisco SWAN framework to meet their specific network configuration requirements, using core and optional components, without having to introduce new elements into their wiring closets. Because Cisco SWAN relies on Wireless Domain Services (WDS), it offers flexible deployment configurations (Figure 1). WDS is a collection of Cisco IOS Software features that enhance WLAN client mobility and simplify WLAN deployment and management. WDS can be located in Cisco Aironet access points, Cisco Catalyst® switches, or Cisco routers. WDS is not in the data forwarding path because it maintains separate control and data planes. Data forwarding rates are unaffected by the presence of a WDS device.

**Figure 1**  
Cisco SWAN and WDS



1. Clients and Access Points (AP) send their Radio Management (RM) data to the Cisco AP, switch or router running wireless-aware Cisco IOS Software with Wireless Domain Services (WDS).
2. Cisco AP, switch or router running wireless-aware Cisco IOS Software with WDS uses RM-Aggregation to remove redundant RM data received from the access points and client devices. The WDS device then forwards the aggregated data to the CiscoWorks WLSE.

#### Core Components:

- Cisco Aironet Series WLAN access points running Cisco IOS Software
- CiscoWorks WLSE
- IEEE 802.1X authentication server, such as Cisco Secure ACS
- Wi-Fi certified WLAN client adapters

#### Optional Components:

- Cisco Aironet Series WLAN client adapters or Cisco Compatible WLAN client adapters
- Infrastructure components—For integrated wired and wireless networks, add the Cisco Catalyst 6500 Series Wireless LAN Services Module (WLSM) or additional Cisco switches and routers running wireless-aware Cisco IOS Software (available in calendar year 2004).

### FEATURES AND BENEFITS

Cisco SWAN minimizes the total cost of ownership and maximizes wireless network uptime by optimizing the following deployment, management, and security features:

- Simplified management of several, hundreds, or thousands of central or remotely located access points
- Simplified WLAN deployment with assisted site surveys
- Enterprise-class security and security policy monitoring with smooth delivery of enhanced network security solutions
- Unified wireless and wired infrastructure, delivering a single point of control for all WLAN traffic
- Extension of rich, intelligent Cisco infrastructure device features to wireless traffic
- Streamlined WLAN management and operations support
- Air/RF scanning and monitoring
- Interference detection to isolate and locate network interference
- Enhanced troubleshooting and diagnostic tools for proactive performance and fault monitoring
- WLAN Intrusion Detection System (IDS)
- Self-healing WLANs that provide high availability
- Fast secure Layer 3 roaming

#### Integrated Wired and Wireless LAN Services

Cisco SWAN integrates and extends wired and wireless networking—making wireless a true extension of the wired network. The framework uses familiar Cisco IOS Software access point, switch, and router management features for integrated management of Cisco access points and client devices. End-to-end delivery of WLAN services such as fast secure roaming, rogue access point detection, security, mobility, quality of service (QoS), and management are enabled today on access points, client devices, and the Cisco Catalyst 6500 Series WLSM, with integration on additional switches and routers starting in 2004.

Cisco SWAN tightens the integration between wired and wireless networking to simplify the management and control of WLANs. It delivers wireless-aware capabilities into Cisco infrastructure devices. This integrated framework allows an IT professional to deploy a wireless network without introducing new elements into the wiring closet—or the data path.

The Cisco Catalyst 6500 Series WLSM, a Cisco SWAN infrastructure component, integrates wired and wireless networking into the industry-leading Cisco Catalyst 6500 Series switch. Scaling to support 300 Cisco Aironet Series access points and 6000 client devices, the Cisco Catalyst 6500 Series WLSM centralizes WLAN functions in the Cisco Catalyst 6500 Series switch, enabling features such as out-of-box access point deployment, centralized security and QoS policies, and fast secure Layer 3 mobility.

The CiscoWorks WLSE is the Cisco SWAN management component responsible for access point radio control plane and security functions such as self-healing WLANs, site surveys, auto-RF optimization, rogue access point detection and suppression, wireless client location and tracking, and other wireless intrusion detection functions. The CiscoWorks WLSE also manages access point configurations, Cisco IOS Software images, and security policy monitoring, and provides diagnostic tools for proactive performance and fault monitoring.

## **WDS**

Introduced with Cisco SWAN, WDS is a collection of Cisco IOS Software features that enhance WLAN client mobility and simplify WLAN deployment and management. A WDS device can be a Cisco Aironet Series access point, Cisco router, or Cisco Catalyst switch (Figure 1).

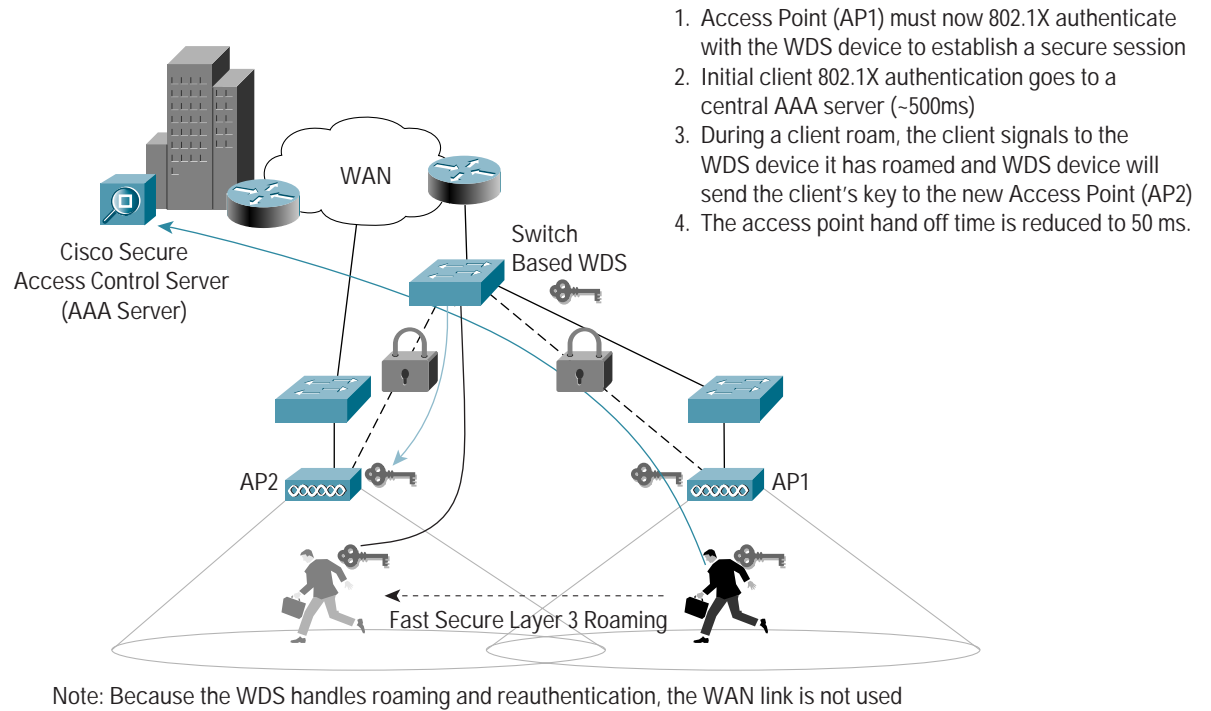
All access points in a subnet detect and securely register, via IEEE 802.1X, with the WDS. The WDS aggregates client and access point RF measurements for RF-managed services such as rogue access point detection, interference detection (demonstrated by the microwave oven in Figure 1), and assisted site surveys. The currently supported WDS feature set includes fast secure roaming, radio management aggregation, and client tracking. Additional WDS feature sets are planned for future software releases.

## **Fast Secure Roaming**

Fast secure roaming is a mechanism that enables a client to roam between access points in the same subnet (Layer 2 roaming) or between subnets (Layer 3 roaming) to support time-sensitive applications. Fast secure roaming includes two features—access-point-assisted channel scanning and fast IEEE 802.1X rekeying. Cisco's fast secure roaming solution allows authenticated client devices to roam securely within and between IP subnets (both Layer 2 and Layer 3 roaming), without sacrificing security or being forced to implement campus spanning VLANs. With Cisco SWAN, Cisco is delivering the industry's fastest, secure Layer 3 mobility with access point handoff times of 50 ms, with no perceptible delay during reassociation (Figure 2).

Fast secure roaming supports latency-sensitive applications such as wireless voice over IP (VoIP), video streaming, video on demand, VPN over wireless, and client/server-based applications such as enterprise resource planning (ERP) or Citrix-based solutions, without dropping connections during roaming. Cisco fast secure roaming requires Cisco Aironet or Cisco Compatible client devices that support the Cisco Centralized Key Management protocol and Cisco LEAP or Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST).

**Figure 2**  
Fast Secure Roaming



## Radio Management Aggregation

The WDS radio management aggregation feature aggregates and eliminates redundant radio management information. This reduces the bandwidth required for radio management information transmitted across the network and WAN link to remote sites and campus locations. Aggregated radio management information is sent from the WDS to the CiscoWorks WLSE. Radio management aggregation enables Cisco SWAN air/RF scanning and monitoring capabilities, including rogue access point detection and location, air/RF interference detection, assisted site surveys, re-site surveys, self-healing WLANs, and future enhancements.

## Client Tracking

WDS client tracking provides additional information on client authentication and roaming events. It supports near-real-time tracking notifications to the CiscoWorks WLSE about client associations to individual access points.

## WLAN IDS

Cisco SWAN includes a WLAN IDS to secure WLANs from malicious and unauthorized access. Cisco SWAN IDS detects and suppresses rogue access points, detects unassociated clients, and mitigates network attacks. The system is deployable as either an integrated or dedicated solution.

## Rogue Access Point Detection, Location, and Suppression

Cisco SWAN detects, isolates, and mitigates rogue access points. Employee-installed rogue access points are becoming more common as the demand for wireless networking increases and access point installation becomes easier. Unauthorized employee-installed access points are usually in the manufacturer's default configuration that

allows open and unauthenticated access to the WLAN. This creates an unsecured WLAN connection that puts the entire network at risk. Not surprisingly, employee-installed access points are greatly reduced in companies that have corporate-sanctioned WLAN infrastructures.

### Unassociated Client Devices

Unassociated client devices are Wi-Fi client devices or adapter cards that have not associated to an authorized access point. These devices are susceptible to association with rogue access points. These clients are deployed either by employees searching for a WLAN access point or by unauthorized intruders probing the network for weaknesses. If left undetected, they pose a security risk—employees deploying these client devices may inadvertently connect to a rogue access point. Intruders deploying these client devices may run WLAN denial of service (DoS) attacks on the WLAN, attempt to run cryptographic attacks on the WLAN security mechanisms, or find unsecured employee-installed rogue access points that allow them to associate and access the network.

### Detecting RF Network Intrusion with Cisco SWAN IDS

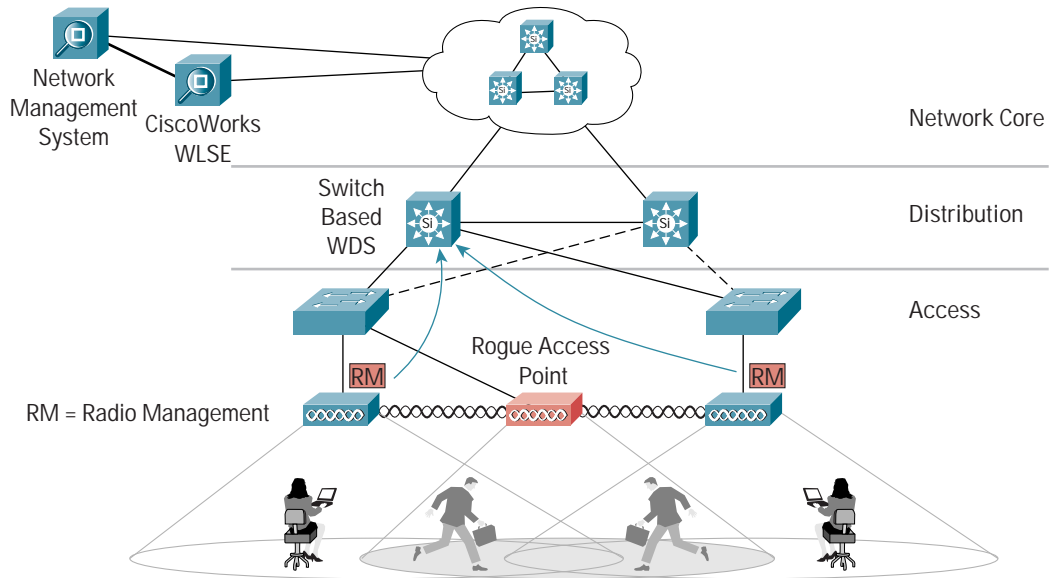
Until Cisco SWAN, network managers had difficulty finding and disabling rogue access points, locating unassociated client devices, and securing WLANs from intruders. Network managers needed to walk the entire coverage area of the network with an air-sniffing device to detect network intrusion. This manual, time-consuming, and costly task had to be repeated on a regular basis in order to detect network intrusion. With Cisco SWAN IDS, this process is automated. IT managers can now easily and automatically detect RF network intrusion events.

With Cisco SWAN IDS, intrusion detection information is automatically gathered from Cisco Aironet access points scanning the RF environment. IT managers can easily detect rogue access points and shut down the switch ports to which they are connected. Optionally, Cisco Aironet client adapters and Cisco Compatible client devices can also participate in RF environment monitoring to expand the coverage area.

### Cisco SWAN Dedicated IDS

With Cisco SWAN Dedicated IDS, a Cisco Aironet access point is deployed with its radio (802.11a, b, or g) placed in Access Point Scanning-Only Mode to support only WLAN intrusion monitoring. In this configuration, an access point functions as an 802.11 scanning-only device providing continuous, stateful 24x7 monitoring of the RF environment. The access point's full bandwidth is dedicated to intrusion detection RF monitoring. Figure 3 illustrates Cisco SWAN Dedicated IDS using Access Point Scanning-Only Mode. In this scenario, rogue access points within the RF range of the deployed access points are detected.

**Figure 3**  
Cisco SWAN Dedicated IDS Access Point Scanning-Only Mode



### Cisco SWAN Integrated IDS

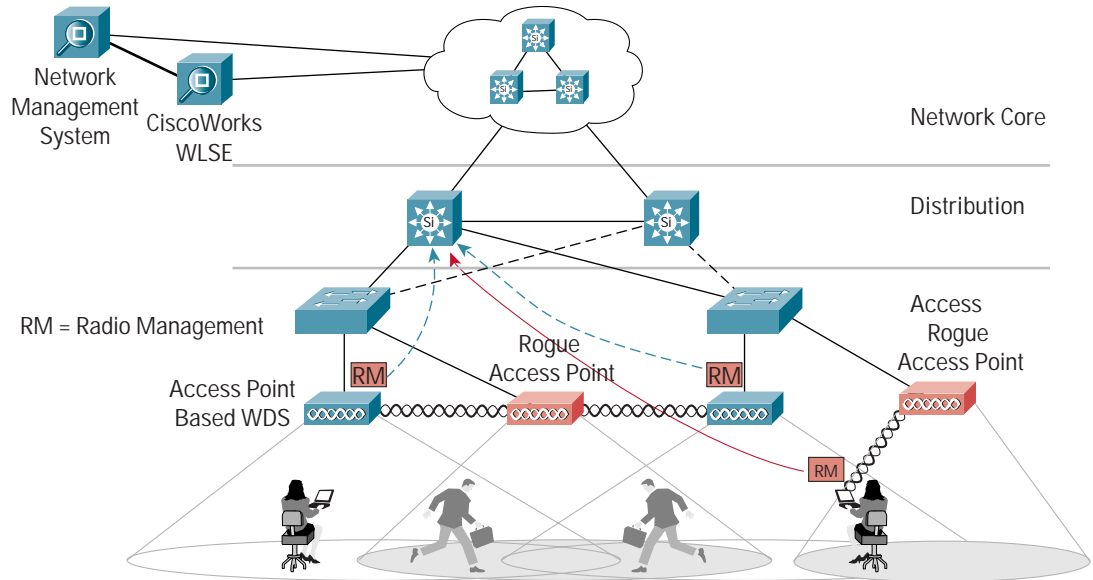
With Cisco SWAN Integrated IDS, a Cisco Aironet access point is deployed with its radio (802.11a, b, or g) placed in Access Point Multifunction Mode to service client devices and provide WLAN intrusion monitoring. In this configuration, an access point functions as both an active 802.11 infrastructure device and as an 802.11 scanning device.

### Optional Client Air/RF Scanning

With Cisco SWAN Integrated IDS, Cisco Aironet and Cisco Compatible client devices can be optionally participate in continuous scanning and monitoring of the RF environment. These client devices work together with Cisco Aironet access points to monitor the RF environment and provide regular RF measurements. This unique optional access point and client-based solution provides advantages over access point only scanning.

With Cisco SWAN Integrated IDS, Cisco Aironet and Cisco Compatible clients can be optionally added to detect and report on obscure and potential rogue access point deployments using client assisted rogue access point detection (Figure 4).

**Figure 4**  
Cisco SWAN Integrated IDS Client Assisted RF Scanning

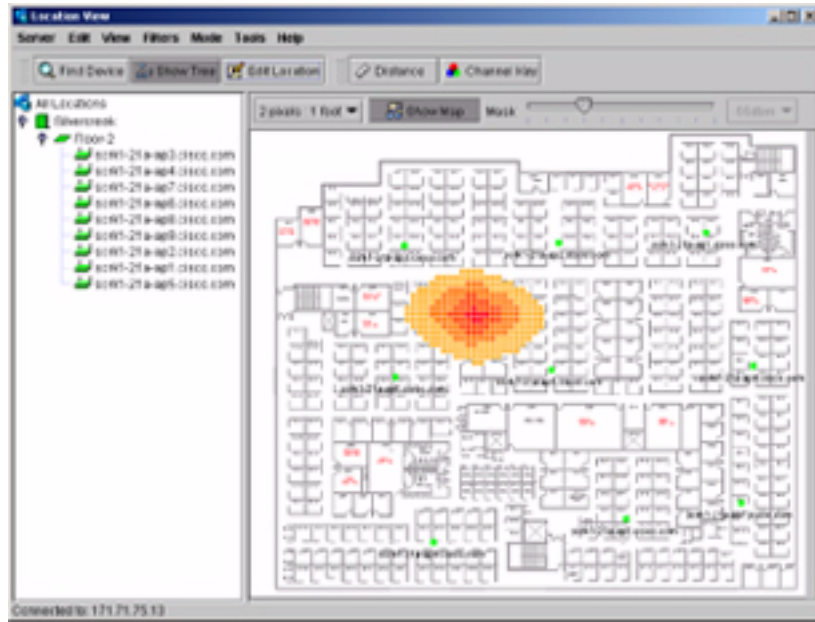


Since WLAN clients can potentially move through a large physical area, the addition of client-assisted rogue access point scanning and monitoring into the framework greatly increases the RF coverage area. Client air management provides 10 to 20 times more RF measurement data than access point RF measurements alone. This extends RF monitoring to areas most likely to contain rogue access points and allows for more accurate rogue access point detection.

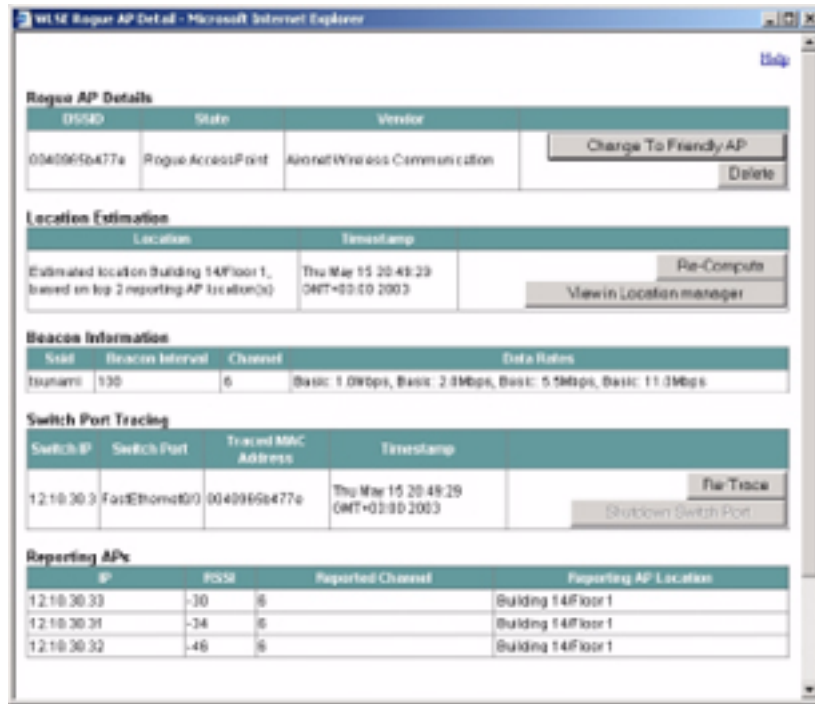
#### Cisco SWAN IDS Display Screens

All Cisco SWAN IDS data captured from the access points and optional Cisco Aironet and Cisco Compatible client devices is compiled by WDS and sent to the CiscoWorks WLSE. The CiscoWorks WLSE processes these received samples, calling out those that indicate the presence of rogue access points in the CiscoWorks WLSE Location Manager (Figure 5) and CiscoWorks WLSE Fault Summary (Figure 6).

**Figure 5**  
CiscoWorks WLSE Location Manager



**Figure 6**  
CiscoWorks WLSE Fault Summary



## **SIMPLIFIED WLAN DEPLOYMENT**

Site surveys are a necessary part of the WLAN deployment process. It is only with a detailed, onsite site survey that complete and reliable WLAN coverage can be achieved. Most organizations either contract consultants to perform their site surveys or use existing IT staff who may not know RF very well. Training a member of the IT staff to manually perform site surveys is not cost-effective; site surveys are typically one-time events that need to occur at each location—potentially hundreds of miles away for large-scale branch office deployments.

With Cisco SWAN, IT managers can perform cost-effective site surveys without requiring RF expertise, which simplifies the deployment tasks significantly. With a wireless-aware network, site surveys are completed using site survey tools integrated into the CiscoWorks WLSE. With these tools, IT professionals who are not well versed in RF propagation and measurement can successfully complete a site survey.

## **STREAMLINED WLAN MANAGEMENT AND OPERATIONS**

Cisco SWAN simplifies WLAN management, which results in enhanced productivity for network administrators. Using the CiscoWorks WLSE, many repetitive time-consuming tasks are automated. Automated tasks include access point firmware updates, VLAN configuration, dynamic grouping, and switch monitoring. To optimize performance and provide high availability, Cisco SWAN supports the following advanced management and operations features:

- Self-healing WLANs—Failed or disabled access points are quickly detected and compensated for by automatic adjustments in the power and cell coverage of surrounding access points. The self-healing process provides contiguous coverage to maximize the available coverage of the WLAN with minimal impact to WLAN clients.
- Interference detection—Points of interfering RF energy that are affecting network performance are easily detected. The source of this unknown RF energy could be a rogue access point or a device that operates in the same frequency range, such as a 2.4-GHz cordless telephone or a leaky microwave oven.
- Mass conversion to Cisco IOS Software—Cisco Aironet 1200 Series and 350 Series access points running the VxWorks operating system may be upgraded all at once to Cisco IOS Software format (RF management requires that access points run Cisco IOS Software).
- Automated resite surveys—Radio throughput and coverage is automatically reassessed. Notification is given if WLAN performance falls below administrator-defined thresholds. New optimal settings can then be found by running the site survey wizard.

## **Enhanced Troubleshooting and Diagnostic Tools**

Network downtime is a great expense for any enterprise. When WLAN network users lose connectivity, their productivity is compromised. Helping to ensure network uptime and reliability is a central requirement for WLANs, but, due to the nature of the RF infrastructure, troubleshooting WLANs is complicated and time-consuming.

Cisco SWAN provides intuitive and comprehensive reports for troubleshooting and capacity planning. It assists in pinpointing problems with utilizations and client associations to help maximize network uptime. It also allows client tracking, WLAN performance reports, and fault monitoring to make network troubleshooting easier.

### **IEEE 802.1X Local Authentication Service**

Cisco SWAN provides authentication services for remote or branch-office WLANs without a RADIUS server, and backup authentication services during WAN link or server failure to provide access to local resources like file servers or printers. This service is called IEEE 802.1X local authentication service, or WAN link remote site survivability. With this service, Cisco Aironet access points are configured to act as a local authentication server to authenticate wireless clients when the authentication, authorization, and accounting (AAA) server is not available.

WAN link remote site survivability can support the authentication of up to 50 user accounts for a given deployment in the local Cisco LEAP authentication database on the access point. One account is equal to one user name and password. The configuration of the IEEE 802.1X local authentication database can be centrally managed with the CiscoWorks WLSE management appliance. The access point with the IEEE 802.1X local authentication service does not need to be dedicated to the IEEE 802.1X local authentication service. This access point can function as a regular access point in addition to providing IEEE 802.1X local authentication.

### **Enterprise-Class Security**

Cisco SWAN provides extensive enterprise-class security management features that use inherited Cisco infrastructure security features and the Cisco Wireless Security Suite, including:

- Integrated wired and wireless security—Cisco infrastructure security features and command-line interfaces (CLIs) are extended to wireless traffic with rich, intelligent features applied on a per mobility group basis.
- Cisco Catalyst services module support—Services module chaining and additional integrated service modules such as the firewall services module (FWSM), intrusion detection module (IDSM), network analysis module (NAM), and IPSec VPN services module (VPNSM) are supported.
- Security policy monitoring—Monitoring of security policies for predefined Cisco Wireless Security Suite parameters across all access points is included. Alerts are generated for violations.
- Centralization of security settings—Centralized WLAN management of all local and remote access point settings helps to ensure parameters such as 802.1X EAP, Wired Equivalent Privacy (WEP), and Wi-Fi Protected Access (WPA).
- Authentication server monitoring—The RADIUS or AAA server providing EAP support is monitored, and the availability of Cisco Secure ACS and committed access rate (CAR) EAP servers is verified.
- Client device response time monitoring—Client device response times are monitored by simulating a client device via CiscoWorks WLSE.
- Notification of authentication server thresholds—Notifications of user-defined security thresholds are managed via e-mail, Syslog, and Simple Network Management Protocol (SNMP) trap notifications.
- IEEE 802.11i Advanced Encryption Standard (AES) encryption support—Future support for IEEE 802.11i AES encryption is planned.

### **SUMMARY**

As WLANs provide network users with a new level of freedom, flexibility, and competitive advantage, they also present IT professionals with new challenges. Cisco SWAN meets these challenges by integrating the wireless and wired LAN to deliver the same level of security, scalability, and manageability for wireless LANs that organizations have come to expect in their wired LANs.

Cisco SWAN has the flexibility to meet the requirements of a variety of networks, from small businesses to large-scale enterprise multinational companies; within WLAN campus deployments or branch offices; at universities; in the retail, manufacturing, and healthcare industries; or in hot spot locations. Using familiar Cisco IOS Software tools, Cisco Aironet access points and client devices, and Cisco switches and routers, this framework brings structure, control, and tightened security to the WLAN, while delivering a compelling low total cost of ownership.

## FOR MORE INFORMATION

Contact your local account representative or visit the locations below for more information.

For more information about Cisco SWAN, visit <http://www.cisco.com/go/swan>

For more information about Cisco Aironet products, visit <http://www.cisco.com/go/aironet>

For more information about the Cisco Catalyst 6500 Series WLSM, visit [http://www.cisco.com/en/US/products/hw/switches/ps708/products\\_relevant\\_interfaces\\_and\\_modules.html](http://www.cisco.com/en/US/products/hw/switches/ps708/products_relevant_interfaces_and_modules.html)

For more information about the CiscoWorks WLSE, visit <http://www.cisco.com/go/wlse>

For more information about the Cisco Compatible Extensions program for interoperable WLAN devices, visit <http://www.cisco.com/go/ciscocompatible/wireless>

For more information about Cisco Secure ACS products, visit <http://www.cisco.com/go/acs>

For more information about the Cisco Wireless Security Suite, visit <http://www.cisco.com/go/aironet/security>



Corporate Headquarters  
Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
[www.cisco.com](http://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](http://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](http://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](http://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 Web site at [www.cisco.com/go/offices](http://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

All contents are Copyright © 1992–2004 Cisco Systems, Inc. All rights reserved. CCIP, CCSP, the Cisco Powered Network mark, Cisco Unity, Follow Me Browsing, FormShare, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MGX, MICA, the Networkers logo, Networking Academy, Network Registrar, Packet, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, ScriptShare, SlideCast, SMARTnet, StrataView Plus, Stratm, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company.  
(0403R) 203179\_ETMG\_JS\_05.04