

## Guidelines and Tools for Migrating to the Cisco Unified Wireless Network

Cisco is encouraging customers to migrate to the Cisco Unified Wireless Network. This paper presents guidelines, tools, and programs to assist organizations with planning their migration strategy. Discover why now is the right time to migrate to the Cisco Unified Wireless Network.

### Challenge

Customers that have deployed a Cisco® wireless solution using Cisco Aironet® standalone (autonomous) access points, the [CiscoWorks® Wireless LAN Solution Engine \(WLSE\)](#), the [CiscoWorks WLSE Express](#), or the [Cisco Catalyst® 6500 Series Wireless LAN Services Module \(WLSM\)](#) need guidelines and tools to assist them in migrating to the Cisco Unified Wireless Network.

### Solution

As the worldwide wireless networking technology innovator and market leader, Cisco offers the industry's most comprehensive product line for enterprise WLANs. The Cisco Unified Wireless Network solution combines the best elements of wireless and wired networking to deliver the same level of security, scalability, reliability, ease of deployment, and management for wireless LANs that organizations expect from their wired LANs.

Customers that have deployed a legacy wireless LAN or a Cisco wireless solution using Cisco Aironet standalone access points, the CiscoWorks WLSE, and Cisco Catalyst 6500 Series WLSM are encouraged to migrate to the Cisco Unified Wireless Network and reap numerous benefits including ease of management, scalability, advanced feature velocity, lowered total cost of ownership, high performance, and mobility services such as voice services, guest access, location services, and enhanced security.

Just follow these five simple steps to migrate to the Cisco Unified Wireless Network: Step 1. Lightweight Access Points, Step 2. Cisco Wireless LAN Controllers, Step 3. Cisco Wireless Control System (WCS), Step 4. Mobility Services, and Step 5. Unified Wired and Wireless Security. This paper presents guidelines and tools to assist organizations in addressing these five steps. To review the advantages of and reasons for migrating to the Cisco Unified Wireless Network please read the white paper [Why Migrate to the Cisco Unified Wireless Network?](#)

### Step 1. Lightweight Access Points

Customers have four options when migrating from Cisco Aironet standalone access points to lightweight access points:

- Use the software upgrade tool to upgrade existing 802.11a/b/g standalone access points to operate as 802.11a/b/g lightweight access points
- Trade out existing 802.11a/b/g standalone access points to 802.11a/b/g lightweight access points

- Upgrade existing 802.11a/b/g standalone access points to 802.11n
- Upgrade existing 802.11a/b/g standalone access points to operate as 802.11a/b/g indoor enterprise wireless mesh access points

#### Software Upgrade Tool

Cisco has released a free tool called the “Autonomous to Lightweight Mode Upgrade Tool” that allows selected Cisco Aironet standalone access point models to be configured for lightweight mode operation. This tool is available for downloading from the [Cisco Software Center](#).

The Autonomous to Lightweight Mode Upgrade Tool supports the following models:

- Cisco Aironet 1240AG Series access points
- Cisco Aironet 1230AG Series access points
- Cisco Aironet 1200 Series access points that contain 802.11g (AIR-MP21G-x-K9) and/or second-generation 802.11a radios (AIR-RM21A-x-K9 or AIR-RM22A-x-K9)
- Cisco Aironet 1130AG Series access points
- Cisco Aironet 1100 Series Access Points that contain 802.11g radios (AIR-AP1121G-x-K9)
- Cisco Aironet 1300 Series Access Points/Bridges (AIR-BR1310G-x-K9 or AIR-BR1310G-x-K9-R). A Cisco Aironet 1300 Series operating in Lightweight Access Point Protocol (LWAPP) mode only operates as an access point. This series does not support LWAPP bridging mode.

The Autonomous to Lightweight Mode Upgrade Tool supports a process to migrate a standalone access point from autonomous mode to lightweight mode. Unlike a VxWorks to Cisco IOS<sup>®</sup> Software upgrade, this process is a Cisco IOS Software upgrade to the existing Cisco IOS Software image—not an operating system “swapout”. In converted access points operating in lightweight mode, Cisco IOS Software continues to run on the access point, while LWAPP is used to communicate with a wireless LAN controller. Since LWAPP supports automatic access point configuration, there is no need to retain or convert the original standalone Cisco IOS Software access point configuration.

Accelerated migration of standalone access points can be performed with a built-in Cisco WCS tool. This tool simplifies the migration of Cisco Aironet standalone access points to operate as lightweight access points and run LWAPP. Up to 10 Cisco Aironet standalone access points of the same model number can be upgraded simultaneously using the tool. This tool is available with Cisco Unified Wireless Network Software Release 4.2 and later.

For more information on upgrading Cisco Aironet standalone access points to LWAPP, please read the [Cisco Aironet Access Point Support for Lightweight Access Point Protocol Product Bulletin](#) or [Upgrading Autonomous Cisco Aironet Access Points to Lightweight Mode Deployment Guide](#).

**Note:** Cisco 3800, 2800, 1800 and 800 Series Integrated Services Routers with integrated access points cannot be migrated from autonomous mode to lightweight mode. These access points can only function as standalone access points. They cannot function as lightweight access points. However, these access points can be monitored for status and alarms by a Cisco WCS running Cisco Unified Wireless Network Software Release 4.2 or later.

### Trading Out Standalone Access Points

Many customers have decided to trade out their existing standalone 802.11 a/b/g access points with 802.11a/b/g lightweight access points as part of a normal or accelerated access point refresh cycle. These customers are eager to take advantage of the ease-of-use, enhanced security, advanced feature velocity, and mobility services available with the Cisco Unified Wireless Network. Many Cisco 802.11a/b/g lightweight access point models are now available, giving organizations numerous access point styles and antennas for indoor office environments, challenging RF environments, and the outdoors to select from.

Because several 802.11a/b/g standalone access point models are available as either standalone or lightweight models, it is important to order the correct lightweight model. Orderable access points configured for lightweight operation contain an “LAP” prefix in the part number, such as AIR-LAP1242AG-x-K9. Orderable access points configured for standalone operation contain the standard “AP” prefix, such as AIR-AP1242AG-x-K9.

If your current 802.11a/b/g access points are not supported by the Autonomous to Lightweight Mode Upgrade Tool, or you are migrating to Cisco wireless products from another wireless vendor's products, you will need to physically replace your existing standalone access points with lightweight access points to migrate to the unified architecture.

An access point replacement program can be designed for small pilot programs, campus deployments, or large international wireless LAN deployments. Your Cisco account manager can help you determine the best process for your access point refresh.

### Upgrading Standalone Access Points to 802.11n

Organizations migrating to the Cisco Unified Wireless Network can choose to upgrade their existing 802.11a/b/g standalone access points to the [Cisco Aironet 1250 Series](#) access point to enjoy the enhanced reliability, throughput, and predictability of 802.11n.

The Cisco Aironet 1250 Series access point is the industry's first business-class access point based on the IEEE 802.11n draft 2.0 standard. Cisco Aironet 1250 Series provides reliable and predictable WLAN coverage to improve the end-user experience for both existing 802.11a/b/g clients and new 802.11n clients. The access point offers combined data rates of up to 600 Mbps to meet the most rigorous bandwidth requirements. With this access point, users can rely on wireless networks to deliver a similar experience to wired networks, providing mobile access to high-bandwidth data, voice, and video applications, regardless of location.

The robust Cisco Aironet 1250 Series is a modular platform designed to be easily field-upgradeable to support a variety of wireless capabilities. This modularity allows businesses to deploy existing wireless technologies today with the confidence that their network investment will extend to support emerging and future wireless technologies.

Your Cisco account manager can help you determine if upgrading to 802.11n and the Cisco Aironet 1250 Series is the best choice for your unified wireless network deployment. They can also help you design an access point replacement program to fit your needs.

### Upgrading Standalone Access Points to Enterprise Wireless Mesh

Organizations now have the option to upgrade selected Cisco Aironet standalone access points to operate as indoor enterprise wireless mesh access points. Enterprise wireless mesh provides connectivity to indoor areas that are difficult or hard-to-wire. Enterprise wireless mesh allows

organizations to extend wireless connectivity to areas of an enterprise facility or structure where running Ethernet cable would be too difficult, aesthetically undesirable, or simply impossible.

Upgrading standalone access points to operate as enterprise wireless mesh access points is a two-step process.

- Step 1: Migrate the standalone access points from autonomous mode to lightweight mode using the Autonomous to Lightweight Mode Upgrade Tool. This tool is available for downloading from the [Cisco Software Center](#). The Cisco Aironet access point model numbers supported by this tool are listed in the Software Upgrade Tool section of this document.
- Step 2: Configure the migrated standalone access points with the correct enterprise wireless mesh software release. Your Cisco account manager can provide you with the correct enterprise wireless mesh software release number. This software is expected to be available from the Cisco Software Center in the fourth-quarter of calendar year 2007.

## **Step 2. Cisco Wireless LAN Controllers**

Cisco wireless LAN controllers are responsible for system wide wireless LAN functions, such as security policies, intrusion prevention, RF management, quality of service (QoS), and mobility. They work in conjunction with Cisco Aironet lightweight access points and the Cisco WCS to support business-critical wireless applications. From voice and data services to location tracking, Cisco wireless LAN controllers provide the control, scalability, security, and reliability that network managers need to build secure, enterprise-scale wireless networks-from branch offices to main campuses.

### **Wireless LAN Controller Family**

The Cisco wireless LAN controller family includes standalone controllers, integrated controllers, and modular wireless LAN controllers that plug into selected Cisco switches and routers. Cisco 4400 and 2100 Series Wireless LAN Controllers are standalone, one-rack-unit devices. The Catalyst 3750G Integrated Wireless LAN Controller is integrated into a Cisco Catalyst 3750G switch. The Cisco WiSM and the Cisco WLCM are wireless LAN controller modules that slide into an existing Cisco Catalyst 6500 Series switch or an Integrated Services Router, respectively.

All wireless LAN controllers deliver the same features and benefits, but each controller supports a different number of lightweight access points. Additionally, wireless LAN controller modules for the Catalyst 6500 Series switch and Integrated Services Routers as well as the Catalyst 3750G Integrated Wireless LAN Controller can take advantage of the access control list (ACL), policies and advanced features of the switch or router that they reside in.

Each controller can be managed centrally via the Cisco WCS or locally via the onboard wireless LAN controller GUI or CLI. Up to 24 controllers and 3600 lightweight access points can be clustered together to provide mobility and system wide RF management (Table 1).

**Table 1.** Cisco Wireless LAN Controllers

	Cisco 2100 Series Wireless LAN Controller	Cisco 4400 Series Wireless LAN Controller	Cisco Wireless LAN Controller Module (WLCM) <sup>1</sup>	Cisco Catalyst 3750G Integrated Wireless LAN Controller <sup>2</sup>	Cisco Catalyst 6500 Series WiSM <sup>3</sup>
<b>Controller Type</b>	Standalone	Standalone	Module	Integrated	Module
<b>Platform Integration</b>	–	–	Cisco 2800 and 3800 Series Integrated Services Routers and Cisco 3700 Series Multiservice Access Routers	Catalyst 3750G Series Switches	Cisco Catalyst 6500 Series Switch
<b>Number of Lightweight Access Points Supported</b>	6	12, 25, 50, or 100	6, 8, or 12	25 and 50	300
<b>Deployment Location</b>	Remote location, branch office, or small office	Remote location, branch office, or campus	Remote location, branch office, or small office	Midsized organizations and enterprise branch offices	Large campus
<b>Interface Ports and Speed</b>	Eight 10/100-Mbps ports	<ul style="list-style-type: none"> <li>• Cisco 4402: Two 1-Gbps ports</li> <li>• Cisco 4404: Four 1-Gbps ports</li> </ul>	One 10/100-Mbps port	<ul style="list-style-type: none"> <li>• 24 PoE 10/100/1000 ports</li> <li>• 32-Gbps, high-speed stacking bus</li> </ul>	Eight 1-Gbps ports
<b>Forwarding Engine</b>	Software	ASIC based (Hardware)	Software	ASIC based (Hardware)	ASIC based (Hardware)
<b>Supports Cisco Aironet Lightweight Access Points</b>	Yes	Yes	Yes	Yes	Yes
<b>Supports Enterprise Wireless Mesh</b>	Yes	Yes	No	No	Yes
<b>Supports Cisco REAP and Hybrid REAP over a WAN</b>	Yes	Yes	Yes	Yes	Yes
<b>Supports Cisco Aironet Lightweight Outdoor Mesh Access Points</b>	Yes	Yes	Yes	Yes	Yes
<b>Responsible for System Wide Wireless LAN Functions<sup>4</sup></b>	Yes	Yes	Yes	Yes	Yes
<b>Supports Zero-Touch Configuration</b>	Yes	Yes	Yes	Yes	Yes
<b>Supports Mobility Services<sup>5</sup></b>	Yes	Yes	Yes	Yes	Yes
<b>Manageable by the Cisco WCS</b>	Yes	Yes	Yes	Yes	Yes

<sup>1</sup> Must be deployed with Cisco IOS® Software Release 12.4(2)XA1 or later

<sup>2</sup> The Cisco Catalyst 3750G Integrated Wireless LAN Controller must be purchased as a complete unit. An existing Cisco Catalyst 3750G switch cannot be upgraded to operate as a wireless LAN controller.

<sup>3</sup> Requires a Cisco Catalyst 6500 Series Supervisor Engine 720.

<sup>4</sup> Supports functions such as security policies, intrusion prevention, RF management, QoS, and mobility.

<sup>5</sup> Mobility services include voice, guest access, location services, and advanced security

## Selecting the Right Wireless LAN Controller

Selecting the right wireless LAN controller is easy. Review the steps below to determine which Cisco wireless LAN controller is right for your WLAN.

1. Decide how many lightweight access points you will be deploying now and in the future (within 1 to 2 years).
2. For 802.11 a/b/g deployments, select your wireless LAN controller based on the number of lightweight access points you will deploy today and in the future to reduce deployment costs.
  - For example, if you are rolling out 10 lightweight access points in your campus environment today but know you will deploy an additional 10 lightweight access points within the next year, it is recommended that you deploy a wireless LAN controller that supports 25 access points (Cisco 4402-25) rather than a controller that supports only 12 access points (Cisco 4402-12).

For 802.11n deployments, discuss your network capacity requirements with your account manager to determine the best wireless LAN controller model(s) for your network.

You will also want to consider adding a second controller for redundancy. See step 6 below.

3. Decide if you want a standalone controller, integrated controller or controller module.
  - The advantage of a standalone wireless LAN controller (Cisco 2100 and 4400 Series) is that it can be deployed in any rack, in any location, as an independent unit. Also, the per-access-point throughput on the Cisco 4400 Series wireless LAN controller and the WiSM is greater than the per-access-point throughput on WLCM or the Cisco 2100 Series.
  - The Cisco Catalyst 3750 Series Integrated Wireless LAN Controller is fully integrated into the Cisco Catalyst 3750 Series switch allowing it to use the existing power, A/C, and rack space of the switch as well as support the application of ACLs, policies, and advanced switch features.
  - Controller modules (WiSM and WLCM) slide into a slot on an existing Cisco router or switch. The advantage of controller modules is that they use the existing power, A/C, and rack space of the Cisco router or switch. ACLs, policies, and advanced features of the router or switch (firewall, call manager, network analysis) can also be easily applied to the traffic to and from these modules.
4. Decide where to deploy your wireless LAN controller. All wireless LAN controllers can be placed in the wiring closet or data center.
  - For best results, it is recommended that the connection between the wireless LAN controller(s) and lightweight access points is over a campus LAN or high-speed connection.
  - Connecting lightweight access points to the wireless LAN controller over a WAN is not recommended unless a remote-edge lightweight access point (REAP) or Hybrid REAP is used.
  - For HREAP's connected to a centralized wireless LAN controller, the WAN link must support a minimum speed of 128-kbps WAN throughput and 100-ms maximum roundtrip latency between each HREAP and the wireless LAN controller.

5. For branch office deployments, decide which deployment option meets your needs. Most branch offices require 1 to 6 access points.
  - **Option 1:** If 1 to 3 lightweight access points are needed at a branch office, REAP or Hybrid REAP may be used. REAP and Hybrid REAP lightweight access points are connected to a central wireless LAN controller over the WAN link enabling several branches to share one or more central controllers.
    - REAP can bridge WLAN traffic locally or tunnel the traffic back across the WAN to a controller. This allows users to maintain WLAN connectivity during WAN outages. With a REAP, wireless access to local resources will persist if the central wireless LAN controller or WAN goes down.
    - Be aware that if the WAN link does goes down, configuration management and visibility into the branch office is lost until the WAN link comes back up.
  - **Option 2:** If the branch office requires more than three access points, then Cisco recommends using a wireless LAN controller at the branch location. The local wireless LAN controller is easily managed over the WAN via Cisco WCS or the onboard wireless LAN controller GUI or CLI.
  - **Option 3 (not recommended):** Some organizations are choosing to deploy three or more REAP or Hybrid REAP per branch office based on the WAN bandwidth from the branch office to the central wireless LAN controller. Cisco does not recommend or support the deployment of more than three REAP or Hybrid REAP at one location. This option is not recommended; it is listed for clarification purposes only.
6. Decide the level of redundancy required. Cisco wireless LAN controllers support an N+1 redundant architecture. If a Cisco wireless LAN controller fails, the lightweight access points automatically transition into an LWAPP discovery phase. In this phase, the access points search the network for a wireless LAN controller with available capacity. The lightweight access points then associate with this available wireless LAN controller.

#### Migrating from Cisco WLSM to Cisco WiSM

Cisco currently has two wireless LAN controller modules available for the Catalyst 6500 Series: [Cisco Catalyst 6500 Series Wireless LAN Services Module \(WLSM\)](#) and [Cisco Catalyst 6500 Series Wireless Services Module \(WiSM\)](#).

The Cisco Catalyst 6500 Series WLSM supports Cisco Aironet standalone access points by serving as a Wireless Domain Services (WDS) device.

The Cisco Catalyst 6500 Series WiSM is an important component of the Cisco Unified Wireless Network and a member of the Cisco wireless LAN controller family. Numerous feature enhancements are planned for the Cisco WiSM. Feature development on the Cisco WiSM will continue at an accelerated rate in conjunction with the release of new features for the Cisco wireless LAN controller family.

Customers that have purchased the Cisco WLSM are encouraged to transition to the Cisco WiSM and the Cisco Unified Wireless Network. In conjunction with this transition, customers will need to migrate their existing standalone access points to lightweight mode or replace their standalone access points with new lightweight access points.

### Step 3. Cisco Wireless Control System (WCS)

Cisco currently has two management platforms available to support Cisco WLANs: the [Cisco WCS](#) and the [CiscoWorks Wireless LAN Solution Engine \(WLSE\)](#) or [CiscoWorks WLSE Express](#).

The CiscoWorks WLSE and CiscoWorks WLSE Express support standalone access points and standalone WLAN bridges.

Cisco WCS is a component of the Cisco Unified Wireless Network. Cisco WCS supports Cisco Aironet lightweight access points and Cisco wireless LAN controllers. With Cisco Unified Wireless Network Software Release 4.2, Cisco WCS also supports status and alarm monitoring of Cisco Aironet standalone access points and includes a built-in tool that simplifies the process to migrate these access points to operate as lightweight access points. Feature development on the Cisco WCS will continue at an accelerated rate in conjunction with the release of new features for the Cisco wireless LAN controller family.

Large-scale deployments can also add the [Cisco WCS Navigator](#) for enhanced scalability, manageability, and visibility of large-scale implementations of the Cisco Unified Wireless Network. This powerful, software-based solution gives network administrators cost-effective, easy access to information from multiple, geographically diverse Cisco WCS management platforms.

Customers that have purchased the CiscoWorks WLSE are encouraged to transition to the Cisco WCS and the Cisco Unified Wireless Network. Customers can use the CiscoWorks WLSE to Cisco WCS conversion CDs (Cisco WCS SKU Family WCS-WLSE-UPG-K9) to convert an existing CiscoWorks WLSE (Model 1130-19 and 1133) to operate as a Cisco WCS server. This SKU family is price adjusted to make transitioning from CiscoWorks WLSE to Cisco WCS cost-effective. Learn more by reading the [Cisco Wireless Control System \(WCS\) Licensing and Ordering Guide](#).

**Note:** A CiscoWorks WLSE that has been converted to Cisco WCS cannot be reverted back to operate as a CiscoWorks WLSE. Conversion of CiscoWorks WLSE Express to Cisco WCS is NOT supported. DO NOT install the CiscoWorks WLSE CDs on to the CiscoWorks WLSE Express (Model 1030) appliance or CiscoWorks WLSE (Model 1105) because this conversion will not work and it is not supported by Cisco Systems.

Customers migrating from CiscoWorks WLSE to Cisco WCS will also need to migrate their existing access points from autonomous mode to lightweight mode or replace their standalone access points with new lightweight access points in conjunction with this transition.

### Step 4. Mobility Services

Support for wireless LAN mobility services is built into the Cisco Unified Wireless Network. By migrating to this innovative solution and deploying lightweight access points, wireless LAN controllers, Cisco WCS, and the [Cisco Wireless Location Appliance](#), organizations can cost-effectively implement mobility services in conjunction with their migration plans. Cisco Unified Wireless Network mobility services include:

- **Voice services**—Organizations can provide cost-effective, real-time wireless voice services using their existing wireless infrastructure and the [Cisco 7900 Series Unified IP Phones](#) or other Wi-Fi phones.
- **Location services**—With location services, an organization can simultaneously track hundreds to thousands of authorized and unauthorized active Wi-Fi devices to within a few meters. This service enhances business applications, improves productivity and supports

critical applications, such as high-value asset tracking, location-based security, enhanced network management, and business policy enforcement. For areas requiring very high fidelity, deterministic location, Cisco Compatible Extensions Wi-Fi tags can be used with the Cisco Unified Wireless Network to support third party chokepoint-based notifications to within a few feet or several centimeters.

- **Guest access**—Customers can keep their wireless networks secure while providing customers, vendors, and partners with controlled access to their wired and wireless LANs. Guest access increases company productivity, facilitates real-time collaboration, and helps companies be more competitive in today's anywhere, anytime, business climate.
- **Wireless IDS/IPS**—The RF environment can be kept secure by monitoring the RF and generating alerts for rogue devices or other potential security threats. The Cisco Unified Wireless Network supports robust IPS/IDS with the Cisco Secure Wireless Solution. This solution is an integrated architecture that builds on the fundamentals of the Cisco Self-Defending Network to offer confidential communications, policy control, and comprehensive threat defense within a wireless context.

Organizations are encouraged to deploy wireless LAN mobility services to increase employee productivity and efficiency, gain a competitive advantage, and provide network users with a new level of freedom and flexibility. Cisco will continue to develop new mobility services to empower organizations with mobility solutions that solve business challenges, keep businesses competitive, and support anywhere, anytime connectivity.

#### **Step 5. Unified Wired and Wireless Security**

Organizations are encouraged to migrate to the Cisco Unified Wireless Network and implement the Cisco Secure Wireless Solution to deliver unified wired and wireless security services to control and contain wireless threats, enforce security policy compliance, and safeguard information.

The Cisco Secure Wireless Solution is a comprehensive security framework that combines confidential communications for information in transit, policy control for a variety of users and deployment scenarios, and a robust threat defense capability to protect information and systems from wireless threats. It delivers a comprehensive architecture that integrates the inherent security capabilities of the Cisco Unified Wireless Network with relevant security solutions, including the Cisco Network Admission Control (NAC) Appliance, the Cisco ASA 5500 Series Firewall with Cisco Intrusion Protection System (IPS) software, and the Cisco Security Agent, as well as many other components.

By implementing the Cisco Secure Wireless Solution, organizations can integrate with the Cisco Self-Defending Network to limit damage from emerging security threats such as viruses, worms, and spy ware. Security policy compliance on all wireless devices seeking to access network computing resources can be enforced by integrating with Network Admission Control (NAC). Additionally, a single authentication framework across multiple device types can be implemented to protect network endpoint devices and enforce security policies across the wired and wireless network with the Cisco Secure Services Client.

#### **Cisco Aironet Deployment Scenarios**

All Cisco Aironet deployment scenarios- standalone access points only; standalone access points plus CiscoWorks WLSE; or standalone access points plus CiscoWorks WLSE plus a Cisco Wireless Domain Services (WDS) device—can be migrated to the Cisco Unified Wireless Network.

Simply follow the five steps outlined in this document to migrate your legacy WLAN to the Cisco Unified Wireless Network.

### Migration Incentive Programs

Cisco is offering several incentives and promotions to assist organizations in transitioning to the Cisco Unified Wireless Network and upgrading to 802.11n. Demonstration units, trade-in credits, and quick start programs may be available. Please ask your Cisco account manager for a list of current programs and incentives.

### Cisco Wireless LAN Services

To assist you with your migration, Cisco and our Wireless LAN Specialized Partners offer a broad portfolio of end-to-end services based on proven methodologies for planning, designing, implementing, operating, and optimizing the performance of a variety of secure voice and data wireless network solutions, technologies, and strategies. Cisco Wireless LAN Specialized Partners bring application expertise to help deliver a secure enterprise mobility solution with a low total cost of ownership. For more information about Cisco services, refer to Cisco Technical Support Services or Cisco Advanced Services.

### Summary

Cisco customers are encouraged to migrate to the Cisco Unified Wireless Network to enjoy the advanced features of this innovative solution. Customers that migrate to the Cisco Unified Wireless Network will immediately experience numerous benefits, including ease of management, scalability, advanced feature velocity, high performance, lowered total cost of ownership, and mobility services such as voice services, guest access, location services, and enhanced security.

Cisco will help to ensure customer investment protection for the Cisco Unified Wireless Network through field firmware upgrades, software upgrades, and careful attention to future hardware requirements. Customers can feel confident that with Cisco, their WLAN investments are protected both today and tomorrow.

### For More Information

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

For more information about the Cisco Unified Wireless Network, please visit:

<http://www.cisco.com/go/unifiedwireless>



Americas Headquarters  
Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
[www.cisco.com](http://www.cisco.com)  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 527-0889

Asia Pacific Headquarters  
Cisco Systems, Inc.  
155 Robinson Road  
#29-01 Capital Tower  
Singapore 068912  
[www.cisco.com](http://www.cisco.com)  
Tel: +65 6317 7777  
Fax: +65 6317 7799

Europe Headquarters  
Cisco Systems International BV  
Hearstbergpark  
Hearstbergweg 13-19  
1101 CH Amsterdam  
The Netherlands  
[www.europe.cisco.com](http://www.europe.cisco.com)  
Tel: +31 20 60 020 0/91  
Fax: +31 20 657 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

©2007 Cisco Systems, Inc. All rights reserved. CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, AirNet, BPK, Catalyst, CCD, CCDA, CCDP, CCIE, CCR, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fax, Step, Follow Me Browsing, FormShare, Go to Drive, HomeLink, Internet Quotient, IOS, IPPhone, IPTV, IQ Expertise, the IQ logo, IQ Not Roadside Scorecard, iQuickStudy, iSignStream, iInlays, MeetingPlace, MGX, Networking Academy, Network Registrar, Packet, PIX, ProConnect, ScriptShare, SMARTnet, SsookWise, The Fastest Way to Increase Your Internet Quotient, and TransPath 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. (9705R)