

## CISCO INTELLIGENT AIRPORT WIRELESS (WI-FI) NETWORK SOLUTION



### INTRODUCTION

The question for airports today isn't whether to implement a wireless network, but how. Business travelers want Internet access, airport vendors need to communicate with corporate networks, security personnel need a wide variety of network connectivity and communications, and airlines want to exchange information with catering companies, maintenance staff, and baggage handlers. The solution is combining an airport-wide Cisco Systems® wireless infrastructure with service provider partnerships. This combination not only supports the network requirements of the diverse community of airport users but can generate additional revenue for the airport.

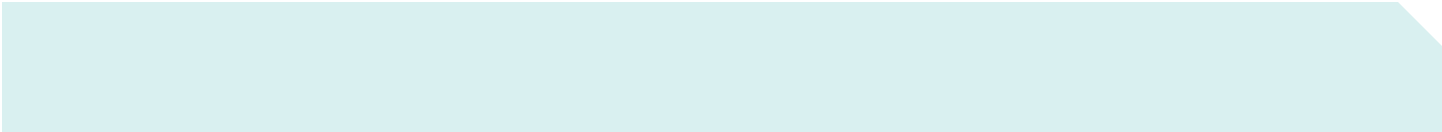
### CISCO INTELLIGENT AIRPORT

To gain the benefits of integrated resources in airports, Cisco Systems® has designed an intelligent information network called the Cisco Intelligent Airport. It has been designed specifically for the unique services and applications of the air transportation industry. Rather than requiring a whole new network build-out, Cisco Intelligent Airport builds upon airports' existing data and voice network investments and support a cost-effective migration to a common, intelligent information infrastructure. Based on open standards, Cisco Intelligent Airport solution securely connects airport, airline, and other tenant operations to provide a cohesive, resilient, and responsive airport operating environment that enables flexible airport operations, improved physical and network security and enhanced passenger services, including public wireless Internet access.

### WIRELESS NETWORKS ARE ESSENTIAL FOR TODAY'S AIRPORTS

Air travel has always involved waiting in airports, and today's tight security measures mean even longer delays. For the business travelers who represent an estimated two-thirds of airline revenues, those delays are expensive as well as inconvenient. According to IDC, 63 percent of business travelers believe that extended travel time makes them less effective while on the job.

While airport delays may be unavoidable, lost productivity is not. More and more, employers are providing tools such as wireless-enabled laptops, personal digital assistants (PDAs), and VPN access to corporate networks to help employees work more efficiently at home and on the road. Corporate travelers now take more than 280 million business trips each year, and Cahners In-Stat estimates that 80 percent of all business travelers use VPN technology.



Business travelers equipped with these tools want to use the time they spend in airports as productively as possible. An airport that provides high-speed Internet access through a wireless LAN (WLAN) can transform boarding gates, lounges, and food courts into practical, value-added working environments for business travelers. In hub airports where passengers may spend several hours waiting for a connecting flight, this offering is particularly attractive. As more mobile professionals and their employers consider public access Internet capability when choosing airlines and transit routes, the investment in wireless Internet access can translate into higher customer volumes.

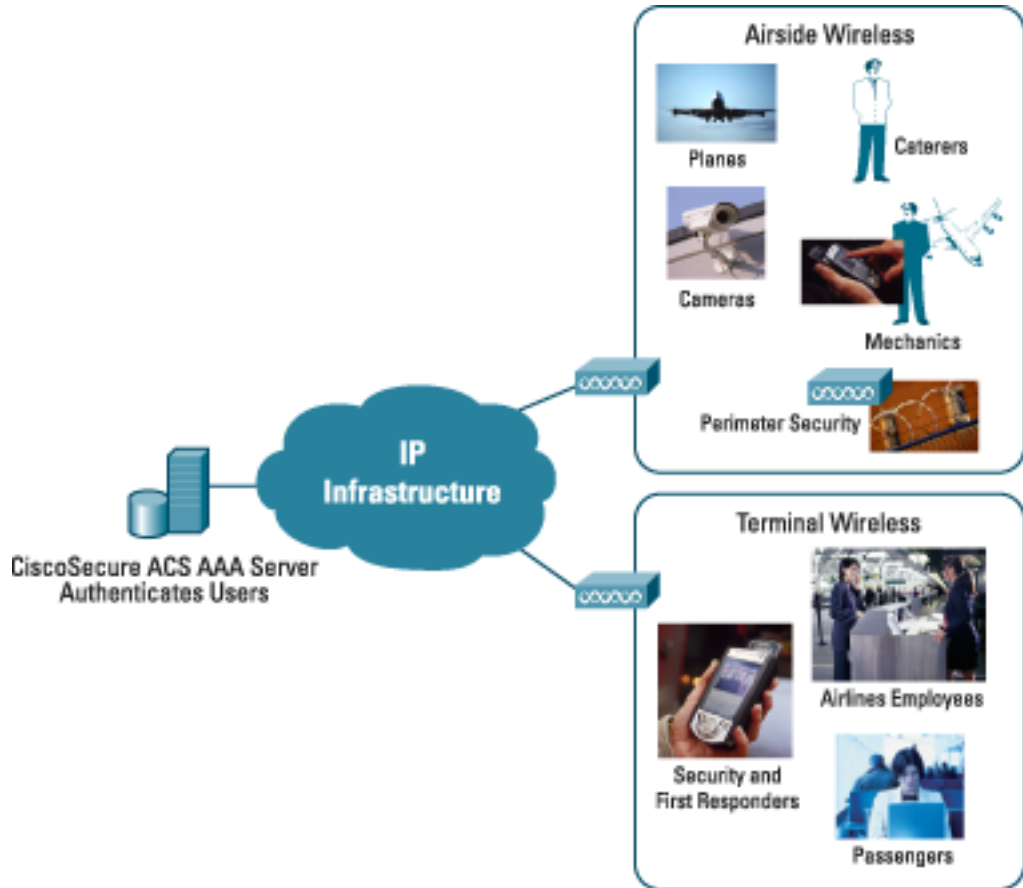
Recognizing this trend, operators of airports and other venues that cater to mobile professionals are increasingly deploying Internet connectivity solutions. In-Stat/MDR estimates that Internet hotspots are now available at 12,000 airports, hotels, and other public venues worldwide, which represents a fivefold increase in the last two years alone. In-Stat/MDR predicts that the number of worldwide Internet hotspots will reach nearly 56,000 by 2004, and grow to more than 113,000 by 2006. And public access is just one application of a WLAN infrastructure.

In addition to providing wireless Internet access capability to travelers, this infrastructure can also support private access applications for the airport community. For the private use community, fee-based airside services can include high-speed access to corporate networks for caterers, mechanics, and flight crews to improve operational efficiency and reduce airplane ground time. Baseline network access services can be provided to airlines and other tenants as part of the lease agreement, with an additional charge for applications or services that require higher levels of network bandwidth. These applications can in turn provide additional revenue streams.

In 2000, the Airport Council International (ACI) World Assembly passed a resolution recommending that airport operators provide and manage an exclusive common infrastructure for wireless technology. A network foundation built on Cisco® products and a Cisco advanced security framework can meet these needs by providing secure and open access within a single infrastructure.

Linking all airport locations and network resources under a common infrastructure offers airports many benefits, including improved manageability, reduced total cost of ownership, and better operational efficiency. An integrated infrastructure designed for converged networking can also support voice, data, and video applications, further helping to reduce costs. Finally, an integrated network infrastructure that supports wireless network access can create new revenue opportunities for the airports themselves.

**Figure 1**  
Wireless Airport Deployment Options



### **SERVICE PROVIDER PARTNERSHIP GENERATES REVENUE FOR AIRPORTS**

There are three business models under which an airport and a service provider can work together to provide public WLAN access services:

- **Wholesale Model:** The airport owns the network infrastructure and resells bandwidth to one or more service providers.

An infrastructure that is owned by the airport can generate revenue through fees paid by service providers on the public access side, as well as by airlines at terminals or contracting companies working for the airlines on the private and secured access side. In the case of a service provider, fees can be assessed based on the number of subscribers accessing the network, bandwidth used, or time spent on the network. Or, service providers can pay a fixed rate to the airport for unlimited bandwidth use, in which case usage need not be tracked once the subscriber is authenticated by the network. Here, the airport becomes an equal access provider (a vendor that provides multiple WLAN service providers with wholesale access to a WLAN infrastructure).

Owning the infrastructure also gives airports the flexibility to implement local services, such as baggage reconciliation or voice over wireless LAN for airlines, tenants, and airport employees.

- **Managed Model:** A single service provider provisions and operates the wireless network for the airport.

The benefit of this model to the airport operator is freedom from wireless network installation, maintenance, and operational concerns, as the capital expenditures (CapEx) are borne by the service provider.

- **Hybrid Model:** An equal access provider provisions and operates the network and resells the bandwidth to a variety of mobile, wireless, and wired line service providers (xSP).

In this model, the airport builds a strong service-level agreement with an equal access provider to help ensure continued high-quality wireless access and free itself from network management and operational responsibility. Local services are a natural outgrowth of this model and offer many opportunities for business-relevant applications.

Regardless of whether the network is owned by the airport, a single service provider, or an equal access provider that resells network bandwidth to other service providers, a network infrastructure from Cisco can support the complex needs of airports.

### **CISCO MEETS RIGOROUS AIRPORT REQUIREMENTS**

To help ensure the success of the wireless network infrastructure and maximize the related revenues, simply providing network access points is not enough. Connectivity solutions must deliver the performance, reliability, and security to support business-class network applications. Airports have specific landside and airside challenges that network providers must address to meet these requirements. The Cisco Intelligent Airport has been developed to address these challenges and provide an integrated architecture for voice, video and data communications. Public and private wireless networks are critical components of this and are key enablers of new services and applications.

For private use applications, the sheer size of many airports is a factor. The network provider must implement a comprehensive site survey to help ensure that there are no “dead spots” (areas where wireless coverage is not available), and that coverage is maintained when roaming between access points. The Cisco Structured Wireless-Aware Network (SWAN) solution and Cisco Advanced Services for Wireless provide engineers, tools, and automated features that help manage site surveys as well as manage and secure the WLAN.

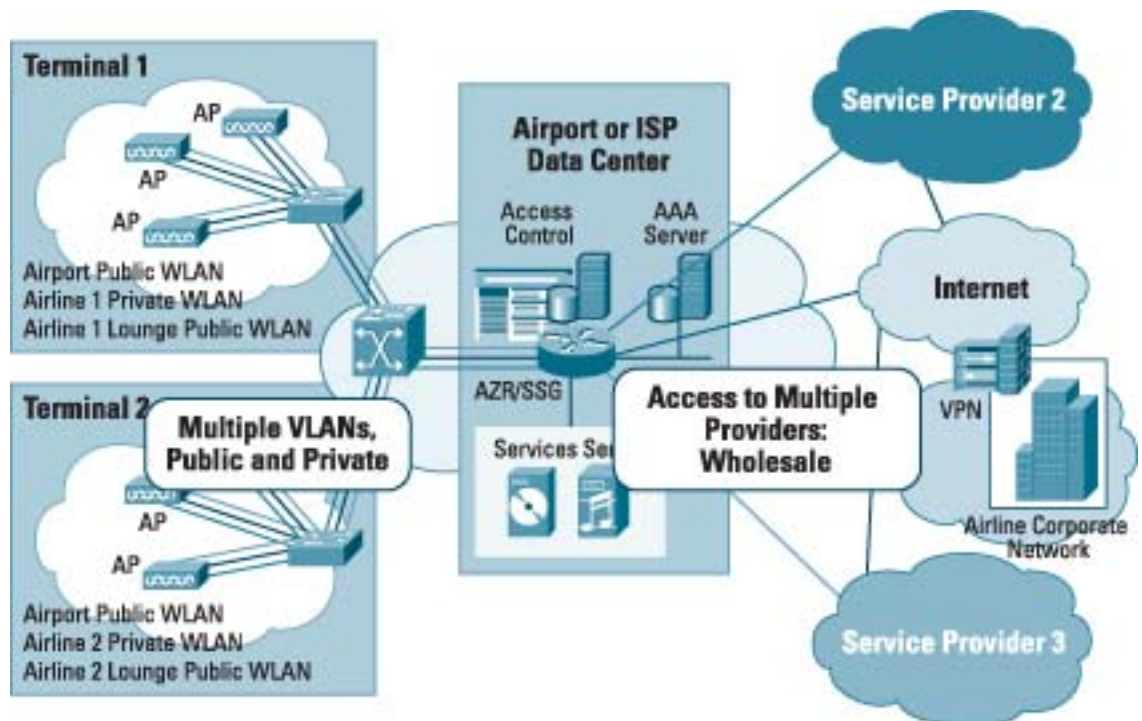
The heterogeneous nature of the population using an airport network is also a factor. For example, even among the seemingly common group of people maintaining a single airplane, there may be 10 different companies handling the variety of tasks involved. And each company requires secure access to its own network within the airport infrastructure.

Baggage reconciliation is an example of a private network application where the wireless component adds extensive value to airport operations. This application can associate potentially dangerous baggage with its owner, and send a picture of the owner to customs agents. Baggage that has been scanned and is known to contain suspicious items is tagged, and that tag triggers a digital camera to take a photo when the owner removes the baggage from the conveyor. The image of the owner is immediately sent to customs agents’ PDAs via the wireless LAN, so that they will know which passengers to separate from the line passing through customs.

Cisco offers the ideal network infrastructure to meet the wireless coverage and security challenges of airports. With a Cisco foundation of intelligent core network routing and switching technologies, airports can deliver the business-class speed, functionality, and quality of service (QoS) necessary to support the full range of internal and passenger-facing applications. Cisco wireless and mobility solutions are robust enough to support voice and video traffic, and wirelessly extend airport applications to mobile security, maintenance, and operations staff.

Figure 2 shows how a Cisco infrastructure addresses the diverse needs of an airport wireless network. Access to multiple service providers supports an airport-owned infrastructure model, and multiple virtual LANs (VLANs) support the security and flexibility needs of public and private access users.

**Figure 2**  
Airport Wireless Network Architecture



The following Cisco products and capabilities provide the flexibility, performance, and security that airports require for a wireless network infrastructure:

- **Cisco Mobile Exchange:** Multiservice and multiservice provider context management.
- **VLANs:** Secure private and public differentiated access management.
- **QoS:** Prioritized streams and services.
- **Cisco Structured Wireless-Aware Network (SWAN):** Simple and accelerated deployment, network management, and security.
- **Cisco Aironet® Wireless Access Points:** 802.11 radio access.

**Cisco Mobile Exchange**—The Cisco Mobile Exchange portfolio is a powerful, services-based architecture for public wireless LAN (PWLAN) operators. Private and institutional operators use the Cisco Service Selection Gateway (SSG), Cisco Subscriber Edge Services Manager (SESM), and Cisco Access Registrar to offer customizable on-demand services, branded Web portals, and service-based authorization and accounting services to subscribers.

Cisco Mobile Exchange offers the ability to manage brand, locations, and services management in a very flexible way. For instance, Cisco Mobile Exchange allows airline lounges to provide distinct branding, helping to downplay the fact that all lounges actually share the same infrastructure. Cisco Mobile Exchange also offers the flexibility to welcome all users individually, regardless of their computer configuration (such as proxy server, DNS settings, or IP address).

**VLANs**—VLANs let devices communicate with each other as if they were physically attached to the same LAN segment, regardless of their location throughout the airport. This allows the network administrator to assign users who require access to the same sensitive information to a common VLAN that is separate and secure from the general user community.

Cisco offers wireless VLAN support so that airports can use a single wireless access point to securely service different customer groups, including airlines, concessionaires, and passengers. This lets the airport IT staff identify and separate internal users from public users, as well as separate different groups within the private user community. This is a critical capability for airport wireless LANs, regardless of whether the airport is using a service provider-owned or airport-owned infrastructure model. In the airport-owned model where service providers purchase network resources from the airport, each service provider can have a dedicated VLAN.

**QoS**—QoS is the capability of a network to prioritize service appropriately for selected traffic. This capability helps ensure that mission-critical and time-sensitive applications receive the bandwidth that they need to perform well, and that other applications also receive fair treatment.

Cisco QoS capabilities enable network administrators to control network resource priority allocation to support specific applications and VLANs. For example, top priority can be assigned to an application that sends video images from security cameras to external security organizations during an airport security event. QoS also gives service providers the ability to offer service-level guarantees to support specific application requirements and specific classes of users.

**Cisco SWAN**—Airport WLANs need to be easy to secure, deploy, and manage. The powerful advantage of airport WLANs could be reduced if the WLAN is improperly installed, secured, or managed. Cisco SWAN provides superior wireless security, management, deployment, and mobility by integrating and extending wireless awareness into every element of the network infrastructure. Cisco SWAN places wireless functionality and management at the right places across the network.

Cisco SWAN extends to the wireless LAN the same level of security, scalability, reliability, ease of deployment, and management that customers have come to expect in their wired LANs. This solution provides a single, integrated scheme for wired and wireless management. This is especially important to airports because of their large size and complex security issues. Cisco SWAN provides:

- *Rogue access point detection*—Network security is maintained via rogue (unauthorized) access point detection and an intrusion detection system (IDS). Having the ability to detect rogue access points is critical to maintaining a secure WLAN. Rogue access points installed by employees or intruders create security breaches that put the entire network at risk. With Cisco SWAN, the process of detecting rogue access points is automated. IT managers can easily and automatically detect, locate, and disable rogue access points.
- *Assisted site surveys*—WLAN deployments are simplified via assisted site surveys, access point auto-configurations, and automated re-site surveys. Site surveys are a “best practice” during deployment, and they should be performed regularly thereafter to address changes that occur dynamically in the environment. Cisco SWAN supports effective site surveys and re-site surveys using airport IT personnel without the need to hire outside vendors.

- *Interference detection*—Radio interference that is affecting network performance is automatically detected and reported. Interference detection and location are critical to maintaining a reliable WLAN.
- *Automated WLAN management*—WLAN management and operations are automated via scheduled configuration changes and monitoring. A wide range of repetitive time-consuming tasks are automated to simplify the management and security of the WLAN, resulting in enhanced productivity for network administrators—and cost savings for the airport.
- *Fast secure roaming*—WLAN client devices can roam securely from one access point to another without any perceptible delay during reassociation with fast secure roaming. This feature supports latency-sensitive applications such as wireless voice over IP (VoIP) without dropping connections during roaming. This is a valuable feature for internal airport communications since it allows phone calls over the WLAN without incurring cell phone charges.
- *Self-healing WLANs*—Cisco Aironet access points automatically adjust their cell coverage areas to compensate for an adjacent disabled or failed access point. The self-healing process provides contiguous coverage to maximize the available coverage of the WLAN.

Cisco SWAN provides network managers with the tools they need to secure, control, and manage the airport wireless LAN.

**Cisco Aironet Series wireless access points**—The Cisco Aironet Series of wireless LAN solutions provides IEEE 802.11a/b/g wireless devices, including access points, wireless LAN client adapters, bridges, antennas, and accessories. These products easily integrate into an existing network as a wireless overlay for in-building and building-to-building wireless LAN solutions or as a stand-alone network for new deployments.

The Cisco Aironet Series is a key component of Cisco SWAN. Cisco SWAN is capable of managing any number of Cisco Aironet access points, from just a few to hundreds of thousands.

## **SECURITY**

Airport security conjures up images of metal detectors and x-ray machines, but securing the airport network infrastructure is just as important as physical security measures and can add value to physical security systems. Cisco is the industry leader in deploying secure wireless networking, which encompasses authentication, encryption, and network reliability.

## **CISCO SUPPORTS WLAN SECURITY SOLUTIONS FOR BOTH PRIVATE AND PUBLIC NETWORK ACCESS**

### **Private Network Access**

Private network access within the airport user community can be supported by the Cisco Wireless Security Suite included with Cisco Aironet and Cisco Compatible Extensions wireless products. The Cisco Wireless Security Suite supports strong mutual authentication and dynamic encryption providing enterprise-class security. It also provides full support for the Wi-Fi Alliance security standard Wi-Fi Protected Access (WPA).

### **Public Network Access**

Cisco accomplishes public access security through a different approach that supports open standards, requires no specialized client devices, and supports all Wi-Fi certified client devices including Cisco Aironet, Cisco Compatible Extensions, and other manufacturers' client devices. User access is controlled through a variety of authentication schemes involving user names, passwords, credit card numbers, and other means of identification such as Extensible Authentication Protocol/Subscriber Identity Module (EAP/SIM).

### **Cisco Compatible Extensions**

With the Cisco Compatible Extensions program, WLAN device suppliers license Cisco technology innovations, design their products to meet Cisco specifications, and undergo extensive third-party testing. Participation in this program helps ensure that innovative features pioneered by Cisco are available in virtually all client equipment that uses wireless LAN-enabled silicon, including laptop computers and PDAs.

Cisco has worked closely with many semiconductor design firms, including Intel, Advanced Micro Devices, Texas Instruments, and others to support an array of features in Cisco Compatible Extensions products. The program also helps ensure that Cisco wireless security features are readily available in products from many industry-leading wireless device vendors, including IBM, Hewlett-Packard, Dell, and others (see [http://www.cisco.com/en/US/partners/pr46/pr147/partners\\_pgm\\_concept\\_home.html](http://www.cisco.com/en/US/partners/pr46/pr147/partners_pgm_concept_home.html) for a current list of partners). All wireless devices built under the program are IEEE 802.11 compliant and Wi-Fi certified to ensure compatibility with other Wi-Fi certified products.

### **Advanced Security Features**

Cisco also provides security features that prevent an authorized user's wireless connection from being "hijacked" by an unauthorized user. These measures protect the service provider against intruders attempting to use network resources without paying for them and ensure that users are not billed in error for access extended to other parties. A Cisco SWAN IDS also helps keep the network secure by easily and automatically detecting, locating, and disabling rogue access points.

With a secure, converged network infrastructure, the operational efficiency and benefits of physical security systems can also be enhanced. Innovative security systems, such as explosive detection systems (EDS), biometrics, and digital video surveillance, can be linked with the airport network infrastructure to facilitate emergency response communications. By network enabling these systems and carrying information over a common, standards-based wired and wireless communications infrastructure, airports can correlate security information in real time and base decision making on a more complete intelligence picture. Activating cameras when an alarm is tripped, for example, can provide first responders with real-time video of security threats on a portable device.

### **CISCO ADVANCED SERVICES COMPLEMENT CISCO PRODUCTS, TECHNOLOGIES, AND SOLUTIONS**

To help airports incorporate wireless solutions into their network architecture and meet their business objectives, Cisco Advanced Services for WLANs, PWLANs, and mobile wireless offer expert advice and services to support the network as airports plan, design, implement, operate, and optimize wireless solutions. Cisco wireless consultants and engineers are experienced in all phases of deploying large network infrastructures. They hold CCIE® and other IT industry certifications and have a broad range of experience running network operations for many global Fortune 500 companies. Equipped with specialized tools and knowledge of the latest wireless technology, Cisco Advanced Services engineering teams understand customers' wireless business objectives and can assist with the planning, design, implementation, operation, and optimization of airport wireless solutions.

## AIRPORTS REAP MULTIPLE BENEFITS FROM CISCO SOLUTIONS

Airports that use Cisco wireless and mobility solutions to provide public and private network access can be assured that the network infrastructure will meet the rigorous demands of this industry. Whether the airport elects to own the network infrastructure and partner with multiple service providers or offer wireless access through a provider-owned network, a Cisco wireless network infrastructure provides many benefits:

- *More efficient airport operations*—Supporting private use airport applications with a wireless LAN helps airport staff work more productively.
- *Improved passenger satisfaction*—Providing travelers with high-speed Internet and company intranet access enables airports to become an integral part of the mobile professional's life away from the office.
- *Increased passenger loyalty*—Adopting Cisco wireless and mobility solutions helps airports differentiate themselves as technology and customer service leaders.
- *Web-enabled marketing*—Customer-facing access solutions provide airport retailers with a powerful new channel for marketing and promotional activities. Airport operators can customize hotspot home pages to include information, promotions, and special offers from airport retailers, restaurants, and other partners.

With a Cisco wireless intelligent information solution, Cisco offers the reliability, security, and flexibility that airport operators expect from an information network.



**Corporate Headquarters**  
Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
www.cisco.com  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 526-4100

**European Headquarters**  
Cisco Systems International BV  
Haarlerbergpark  
Haarlerbergweg 13-19  
1101 CH Amsterdam  
The Netherlands  
www-europe.cisco.com  
Tel: 31 0 20 357 1000  
Fax: 31 0 20 357 1100

**Americas Headquarters**  
Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
www.cisco.com  
Tel: 408 526-7660  
Fax: 408 527-0883

**Asia Pacific Headquarters**  
Cisco Systems, Inc.  
168 Robinson Road  
#28-01 Capital Tower  
Singapore 068912  
www.cisco.com  
Tel: +65 6317 7777  
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the **Cisco 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 Arrow logo, 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, EtherFast, EtherSwitch, Fast Step, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, Registrar, ScriptShare, SlideCast, SMARTnet, StrataView Plus, 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) 203228\_ETMG\_JS\_04.04