Cisco Application-Oriented Networking 2.4

Product Overview

The Cisco® Application-Oriented Networking (AON) platform is the foundation for a new class of Cisco products that provide an essential point of convergence of intelligent networks with applications based on highly distributed, service-oriented, and older architectures. Cisco AON embeds a new class of application intelligence into the network to better meet the underlying needs of applications for multi-enterprise security, real-time visibility, event-driven messaging, optimized delivery, and other core integration and deployment services.

Features and Benefits

Cisco AON natively understands the content and context of application messages (for example, a purchase order or stock trade), and conducts operations on those messages in flight according to business-driven policies and rules. Cisco AON delivers this breakthrough level of application intelligence to complement and extend Cisco integrated network services technologies, resulting in a new level of immediate and deep insight for real-time business decision making.

Cisco AON complements existing networking and application technologies with enhanced security, visibility, messaging, and optimization services that provide a higher degree of awareness regarding the essential business information flowing in the network. These services help to:

- **Enforce consistent business policies** across information access and exchange
- **Provide visibility of information flow**, including monitoring and metering of information flow for both business and infrastructure purposes
- **Enable disparate applications to communicate** by routing information to the appropriate destination, in the format expected by that destination
- **Enhance application optimization** by providing application-level load-balancing, processing offload, message caching, and compression services

Cisco AON works primarily at the message level rather than the packet level. Typically it inspects the full message, including the payload as well as all headers. It also understands and enhances delivery of application-level protocols such as HTTP and Java Messaging Service (JMS).

Core messaging and other baseline application services have typically been developed using application software and expensive custom code. Instead, Cisco AON uses a pervasive, intelligent network to provide these capabilities, helping realize significant business gains in terms of:

- Embedded awareness that spans applications and computing environments
- Real-time business information that informs and enables rapid yet precise decision making
- Network-guided optimization that boosts application performance and reliability

Cisco AON comes in two form factors that integrate into Cisco switches and routers:

- Cisco Catalyst® 6500 Series AON module, deployed in the enterprise core or data centers
- Cisco 28xx through 38xx Series Integrated Service Router (ISR) AON module, deployed at the branch office

Cisco AON also comes in a new appliance form factor. The Cisco 8340 Series AON Appliance offers the high performance and ease-of-use of a standalone appliance as well as the added value of being a network-embedded device.

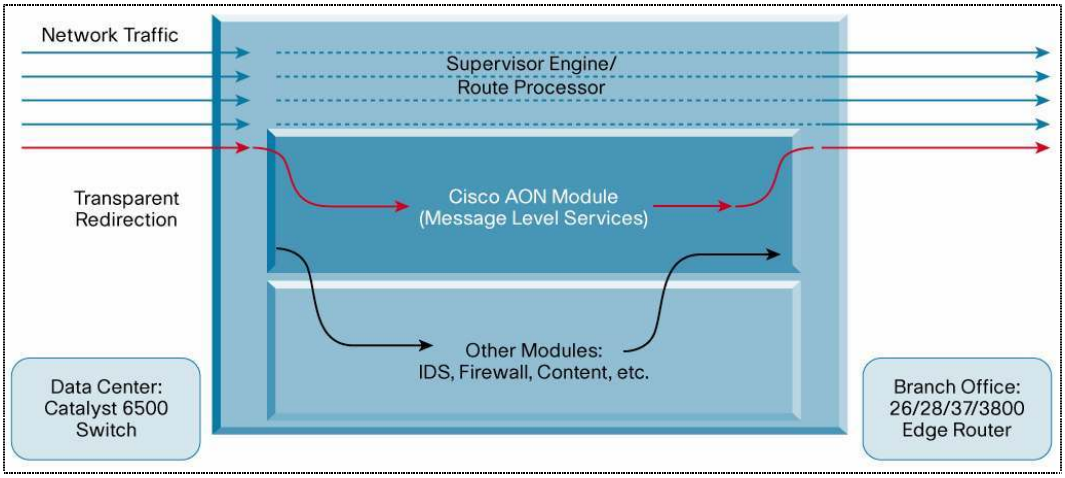
For more detail, refer to data sheets for the individual form factors. See Figure 1.

Figure 1. The Cisco AON Product Family

Cisco AON Operation

The supervisor engine or route processor in the switch or router can transparently redirect application traffic to the Cisco AON module without requiring any changes to the applications themselves (Figure 2). Policies can then be applied to these messages and forwarded to the destination application. Cisco AON also can be explicitly addressed if required.

Figure 2. Traffic Redirection to AON

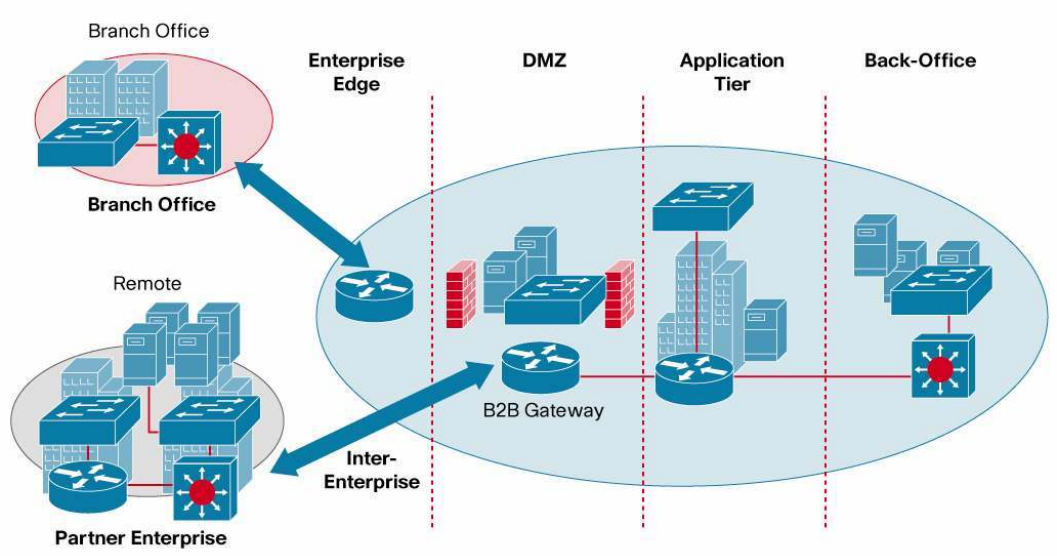


The following tools are available to configure and manage these devices:

- **Cisco AON Development Studio (ADS)** is used to create policy execution plans (PEPs) that represent a set of operations (Bladelets) to apply to application messages.
- **Cisco AON Management Console (AMC)** provides centralized control for configuration, certificate management, and lifecycle management of a distributed AON network.

The Cisco AON platform helps enable a wide range of usage scenarios across an application network (Figure 3). Following are some scenarios in which Cisco AON is typically deployed.

Figure 3. High-Level Network Architecture



- **In the remote office or business-to-business (B2B) spoke:** Cisco AON devices can be deployed for infrastructure consolidation. A single device can provide all the services required by the branch to effectively communicate with the central office. Cisco AON helps enable these services by bridging disparate applications and optimizing network usage at the application level. Cisco AMC provides centralized management for distributed branch-office deployment of application policies.
- **At the enterprise edge:** Cisco AON can act as an application-security gateway or a B2B gateway. As an Extensible Markup Language (XML) trust enforcement point, it provides consistent authentication, authorization, and accounting enforcement across all backend services and applications. As a B2B gateway, Cisco AON helps enable a transparent interface with trading partners by providing trust, protocol bridging, and message validation and transformation services.
- **At the enterprise core:** Cisco AON provides transparent interapplication communication, and it can intercept and analyze traffic in message formats such as XML. It also provides a network-embedded communication bridge between protocols and applications. Cisco AON helps applications offload infrastructure functions such as message-level load balancing to the network, where they can scale effectively.

AON Features

Security

To enforce application security policy within the network, Cisco AON provides a set of services that help enable message-level access and control.

- **Authentication:** Cisco AON can verify the identity of a sender's inbound message-based content (username and password, WS-Security profile, digital certificate, and so on). The solution integrates with security frameworks, such as Kerberos Protocol, and Lightweight Directory Access Protocol (LDAP) servers such as Netegrity SiteMinder, Microsoft Active Directory, OpenLDAP, and SunONE.
- **Authorization:** Cisco AON can determine which level of access the originator of the message should have to the services it is attempting to invoke. Features supported include SAML Authorization Assertion embedded in Simple Object Access Protocol (SOAP), WSS

headers, LDAP group-based authorization, and customer-defined rule-based control policies.

- **Nonrepudiation and data integrity:** Cisco AON can digitally sign message elements or entire messages at any given AON device. Features supported include insertion and verification of XML signatures in WSS headers, detached envelope and enveloping XML signature types, signatures based on private keys, SHA-1 digest computation, and RSA digest encryption.
- **Confidentiality:** Based upon policy, Cisco AON can encrypt and decrypt message elements or entire messages. Features supported include Triple Digital Encryption Standard (3DES) and Advanced Encryption Standard (AES)-128/192/256 symmetric ciphers, RSA symmetric ciphers, destination URL-based keys, and certificates.
- **Centralized key management:** Cisco AMC allows users to register, configure, bind, and provision keys and certificates from the Cisco AMC server to the AON device. Capabilities include generating, registering, and obtaining Class 2 and Secure Sockets Layer (SSL) certificates using Verisign Class 3 Certificate Service; fetching, uploading, and importing SSL certificates; importing PKCS#12 certificates; and importing keys from Java keystores.
- **Transport-layer security:** Cisco AON supports transport-layer security mechanisms such as SSL 3.0.

Visibility

Each Cisco AON node can be configured to act as a sensor that captures, processes, and logs highly granular information about application messages. This capability helps Cisco AON provide an event-capture fabric for specified application messages. Cisco AON can inspect the messages and apply rules at the message-content level.

- **Out-of-band message processing through promiscuous mode:** Cisco AON can receive and process messages without increasing latency in network traffic, helping enable out-of-band monitoring and analysis. For example, Financial Information eXchange (FIX) and HTTP sessions are received out of band, assembled to recreate the messages, then appended with relevant metadata such as time stamps and relevant TCP headers. These messages can be used to analyze scenarios such as transaction monitoring, intrusion detection, insider threats, or FIX monitoring. And service-level agreement (SLA) customers can take advantage of the extensibility framework to tap and frame their proprietary message formats.
- **Logging:** Cisco AON can log messages to external systems for purposes of auditing and compliance or for future analysis.
- **Contextual lookup:** Cisco AON can refer to external systems to obtain contextual information required to analyze the data. For example, it can call out to a customer database to look up customer priority based on a customer ID in the message.
- **Notification and alerting:** Cisco AON can notify or alert other applications in case of an abnormal event. For example, if an SLA time to deliver a message has not been fulfilled, operations personnel can be alerted to take corrective action.

Intelligent Message Routing

Given its role as an intermediary in highly heterogeneous application environments, Cisco AON must flexibly adapt to different types of enterprise information, business policies, and endpoints. Cisco AON operates at the application-message level, allowing a high degree of flexibility:

- **Application quality of service (AppQoS):** The AppQoS feature helps Cisco AON users set application message- and transaction-level priorities and align them with network-level QoS capabilities. For example, an enterprise SAP system can be made to process purchase orders with a higher priority than price quotes and enforce that priority across the application infrastructure and the network. The priorities map to network QoS functions, which in turn direct the priority of message processing both within the AON node and at the transport level in the network. The business result is better alignment of IT infrastructure usage with a higher degree of automatic SLA enforcement, even in times of severe network congestion.
- **Protocol support:** Cisco AON understands various application access methods and provides adapters for most commonly used protocols: HTTP, HTTPS, Tibco EMS, WebSphere JMS & MQ, and BEA JMS. Additionally, a custom adapter software development kit (SDK) is available for creation of new adapters to any environment. Most policies and Bladelets used within Cisco AON understand the semantics of these protocols natively, allowing for higher fidelity and control of the interaction.
- **Protocol switching:** A Cisco AON node can act as a protocol gateway between multiple applications; for example, receiving an application message through WebSphere MQ and sending it to another application as an HTTP post. Cisco AON supports protocol translation between any combination of its supported protocols.
- **Transformation:** The open transformation architecture of Cisco AON supports both XML and non-XML transformation. Cisco AON achieves Extensible Style Language Transformation (XSLT)-based transformation with its XSLT-based transformation engine using XSLT style sheets written or procured by the customer, allowing any combination of transformations between XML and other XML or non-XML formats. External parsers can be plugged in to facilitate reading of the non-XML format and conversion to a format consumable by the engine. In addition, custom transformations can be carried out by adding a third-party Java transformation engine.
- **Service virtualization:** Based on its ability to inspect and understand the content and context of application messages, Cisco AON can act as a proxy that provides an abstraction layer for endpoint applications and applies policies without the endpoints being aware of the intermediary. This powerful capability allows consistent, distributed policy enforcement everywhere in the network—a particularly relevant capability for distributed service-oriented applications. For example, messages can be routed according to their content by matching content elements against policy rules. Cisco AON examines message types or fields (for example, part number, account type, employee location) and sets the destination based on rules, protocol headers, or other states resulting from a previous operation. For another example, Cisco AON can do load balancing across multiple endpoints using algorithms such as Round Robin (equal distribution), Weighted Round Robin (preference for certain endpoints), and Adaptive (essentially a “best-available” service based on captured state of request or response times and latency). As for message distribution, Cisco AON supports “stickiness” to endpoints based on session recognition and management, and message distribution or “fan out” whereby a message is sent to multiple destinations simultaneously.

Application Optimization

Cisco AON takes advantage of a combination of technologies to enhance message-handling performance and improve application availability. In a typical scenario only a fraction of the

network traffic flow is redirected through Cisco AON, so the vast majority of network traffic passes through as usual. For packets processed by Cisco AON, the following features are designed to minimize processing overhead and achieve enterprise-ready levels of throughput and reliability:

- **System optimization:** To speed applications that require high transaction rates, Cisco AON offers performance-optimized message processing and a fast code execution path that is particularly useful in compute-intensive operations such as content-based routing and XML schema validation. In addition, you can plug in custom functions that take advantage of the optimized execution path to meet your high-performance needs.
- **Hardware acceleration:** For some performance-intensive operations such as XML parsing and encryption/decryption, select Cisco AON devices offer hardware-based acceleration.
- **Caching and compression:** Cisco AON can cache the results of previous message inquiries based on the rules defined for a type of request or on indicators set in the response. Caching can be performed for entire messages or for certain elements of a message to reduce application response time and conserve bandwidth. Either XML and non-SML response messages or elements of a message identified and accessed through XPath can be cached. Additionally, Cisco AON can compress messages between nodes. A message policy can be set to compress the data before sending an outbound message, while on the inbound side Cisco AON automatically recognizes the message as compressed and decompresses it before further processing.
- **Availability and load balancing:** As described in the previous section, Cisco AON can sit in front of an application cluster to provide high-availability and load-balancing services to applications.

Extensibility

Built on an open, extensible architecture, Cisco AON includes a set of APIs to add new adapters and Bladelets. It provides an interface to develop extensions to the base AON platform using languages such as Java and C.

- The Adapter Developer Kit (ADK) supports development of plug-in custom adapters to receive and send messages from Cisco AON.
- The Bladelet Developer Kit (BDK) supports development of custom Bladelets in Java and C/C++. This capability is also available in the system optimized code execution path.

Scalability and Performance

Cisco AON is designed for high performance and scalability to address the needs of the most demanding applications. It accomplishes this through:

- **Hardware-based acceleration:** By offloading computation-intensive tasks such as XML processing, cryptographic operations, and regular expression matching to a hardware-based accelerator, Cisco AON can achieve significant performance gains.
- **Virtual cluster:** As application message traffic increases, additional Cisco AON modules can easily be added to the switch or router. Thus Cisco AON can scale horizontally and transparently to match the increased traffic.

Cisco AON Design, Configuration, and Management

Cisco AON operates as a set of distributed application and network services that span business, security, administrative, and network domains. Thus, it is important to provide a set of tools that

effectively and uniformly address different aspects of configurability, manageability, and visibility of the system. Cisco AON tools include Cisco ADS and Cisco AMC.

Cisco AON Development Studio

Cisco ADS is a Windows-based tool for developers to configure how application messages are handled at run time (Figure 4). Its features include:

- Easy drag-and-drop GUI environment
- Set of preconfigured functions or Bladelets that can be used to create message plans
- One-button synchronization of plans with Cisco AMC
- An SDK for creation of custom Bladelets and an ADK for creation of custom adapters

Table 1 below lists system requirements for Cisco ADS.

Cisco AON Management Console

Cisco AMC (Figure 5) is a Linux-based Web application with full role-based access control for centralized management of the Cisco AON system. It helps ensure consistent, up-to-date configurations across all Cisco AON devices in a distributed infrastructure. Functions include:

- Configuring and managing Cisco AON nodes
- Defining and provisioning application policies
- Key and certificate management
- Monitoring of Cisco AON node events and logs to directly interface with the Cisco AON blade operations in a switch or router

Table 2 lists system requirements for Cisco AMC, and Tables 3 and 4 list standards supported by Cisco AON.

Figure 4. Cisco AON Development Studio (ADS) Design-Time View

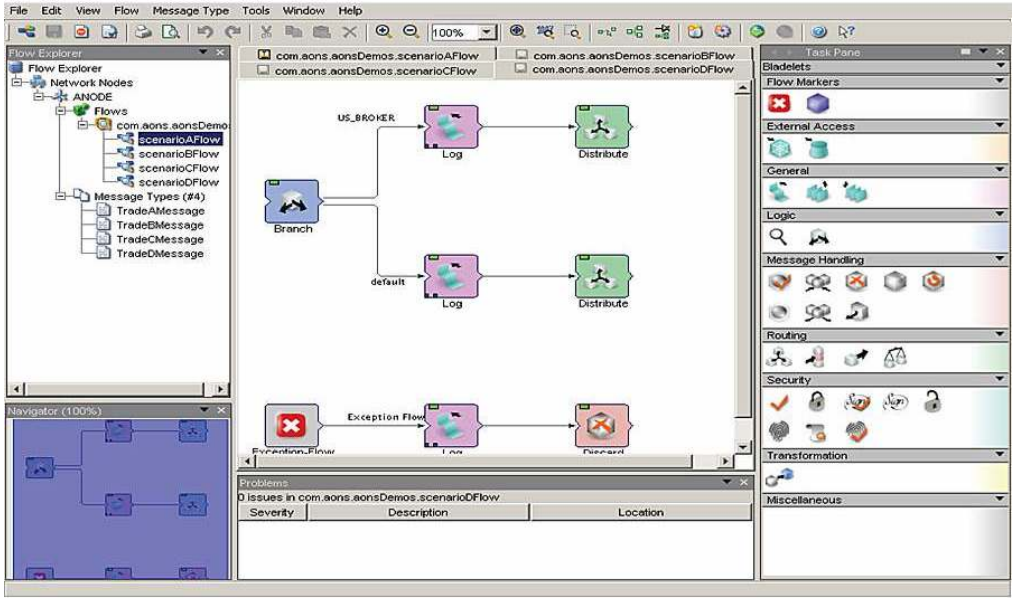


Figure 5. Cisco AON Management Console (AMC) View

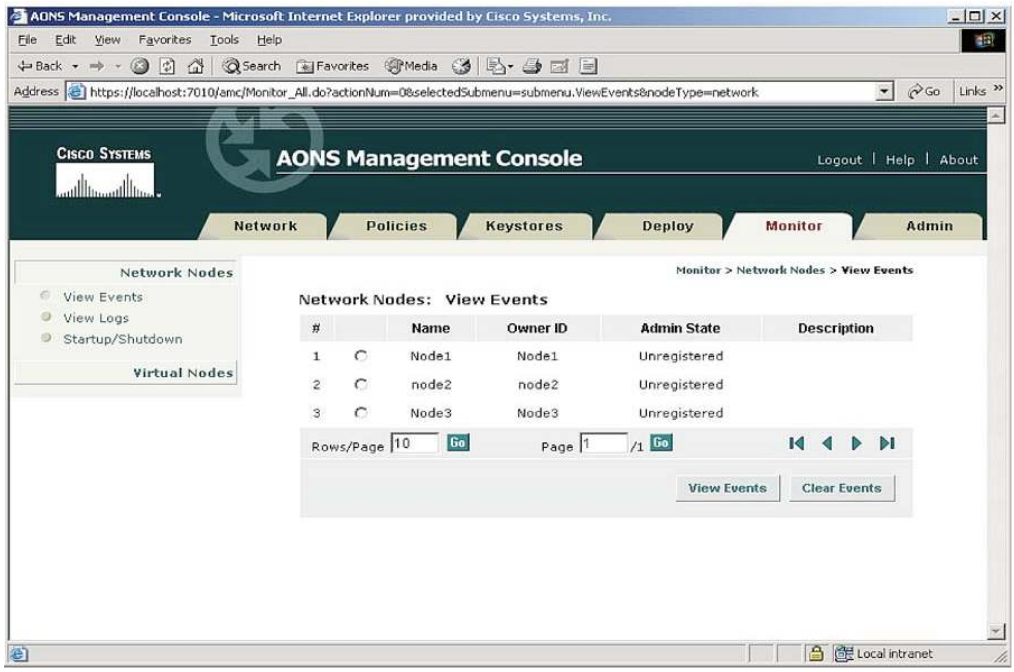


Table 1. Cisco AON Development Studio (ADS) System Requirements

Feature	Requirements
Disk space	40 GB minimum
Hardware	Single processor, Pentium III or later
Memory	512 MB minimum (1 GB recommended)
Software	Microsoft Windows 2000 or Windows XP

Table 2. Cisco AON Management System (AMS) System Requirements

Feature	Requirements
Disk space	20 GB minimum
Hardware	Single processor, Pentium III or later
Memory	512 MB minimum
Software	RedHat Linux (RHEL) AS or ES 3.0 or later

Table 3. Cisco AON Supported Standards

Feature	Requirements
Transport protocols	HTTP, HTTPS, JMS, Tibco EMS, WebSphere MQ,WebLogic JMS, BEA JMS, FTP, SMTP, and UDP
Database	Oracle 9i (9.2) and Sybase 12.5.1
Security	DES, 3DES, AES, RSAv1.5, SHA-1, PKCS#12, SSL3.0, and TLS 1.0
Management	Simple Network Management Protocol V2 (SNMPv2); command-line interface (CLI)
XML	HTTP 1.0, 1.1, HTTPS, SOAP 1.1, SOAP w/ Att, XSLT 1.0, Xpath 1.0, XSD 1.0, 1.1, WS-I, WSDL 1.1

Table 4. Cisco AON Supported Trust Policies Standards

WS-SecurityPolicy specs	Requirements
Integrity Assertions	
SignedParts Assertions	✓- Sign / Verify bladelet
SignedElements Assertions	✓- Sign / Verify bladelet
Confidentiality Assertions	
EncryptedParts Assertion	✓- Encrypt / Decrypt
EncryptedElements Assertion	✓- Encrypt / Decrypt
Token Assertions	
UsernameToken	✓- Authenticate / Authorize
IssuedToken	✓- Authenticate / Authorize
X509Token	✓- Authenticate / Authorize
KerberosToken	/ - Partial / Planning
SpnegoContextToken	✓- Authenticate / Authorize
SecurityContextToken	X - Evaluating
SecureConversationToken	X - Planning
SAMLToken	✓- Authenticate / Authorize
RelToken	/ - Partial / Planning
Transport Security	✓ - Identity bladelet

Ordering Information

To order, call your Cisco account representative.

Service and Support

Cisco offers a wide range of services programs to accelerate customer success. These innovative services programs are delivered through a unique combination of people, processes, tools, and partners, resulting in high levels of customer satisfaction. Cisco services help you protect your network investment, optimize network operations, and prepare your network for new applications to extend network intelligence and the power of your business.

Cisco AON products are bundled with Cisco Advanced Services that will accelerate your time to deployment and help ensure a high-quality, reliable implementation. For more information about Cisco services, refer to Cisco Technical Support Services or Cisco Advanced Services.

For More Information

For more information about the Cisco AON platform, visit http://www.cisco.com/go/aon or contact your local Cisco account representative.

Americas 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: 408 527-0883

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

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 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.**

Printed in USA C78-337845-03 08/07

