

# Cisco Application-Oriented Networking

## Product Overview

The Cisco® Application-Oriented Networking (AON) platform is the primary technology foundation for a new class of Cisco Systems® 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 multienterprise security, real-time visibility, event-driven messaging, optimized delivery, and other core integration and deployment services.

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 an unsurpassed level of immediate and deep insight for real-time business decision making.

Cisco AON complements existing networking and application technologies by providing a set of enhanced security, visibility messaging, and optimization services that help both IT and business users obtain a greater degree of awareness regarding the essential business information flowing within the network. These services help to:

- **Enforce consistent security policies** for 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, offloading, message caching, and compression services

Cisco AON provides this enhanced and adaptive level of application intelligence by working primarily at the message level rather than at the packet level. Typically, Cisco AON inspects the full message, including the “payload” as well as all headers. It also understands and enhances the delivery of popular application-level protocols such as Hypertext Transfer Protocol (HTTP), Java Messaging Service (JMS), and other accepted standards.

Until now, core messaging and other baseline application services have typically been developed using application software and custom-developed code, which is expensive to build and difficult to maintain. Instead, by employing a pervasive, intelligent network to provide these capabilities, significant business gains can be realized 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 (refer to individual form-factor data sheets for additional information):

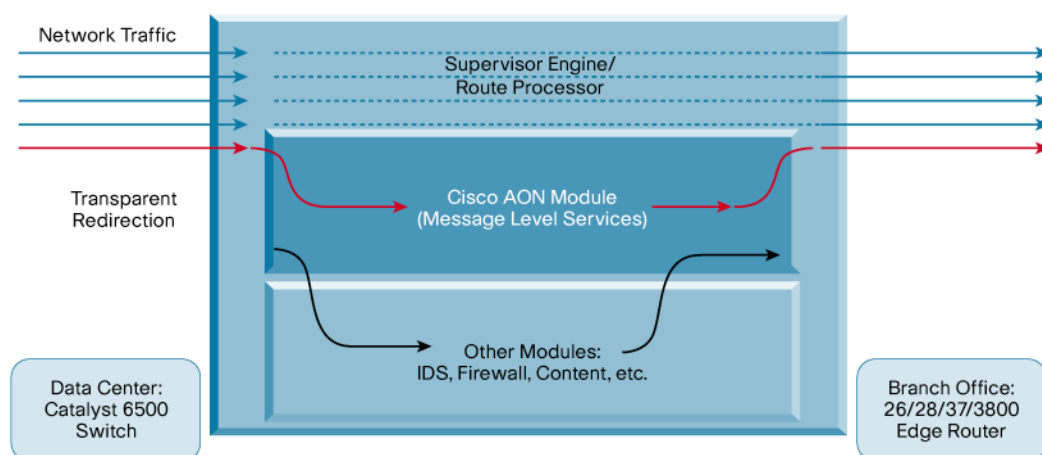
- Cisco Catalyst® 6500 Series AON module, which is deployed primarily in the enterprise core or data centers
- Cisco 2600, 2800, 3700, and 3800 series AON module, which is deployed primarily at the branch office

Cisco AON also comes in an appliance form factor, that extends the AON Product family:

- The Cisco 8340 Series AON Appliance offers both the concentrated single-source performance and ease-of-use of a standalone appliance as well as the value-add of being a network embedded device.

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. AON policies can then be applied to these messages and forwarded to the destination application. Additionally, Cisco AON can be explicitly addressed if required.

**Figure 1.** Traffic Re-Direction to AON



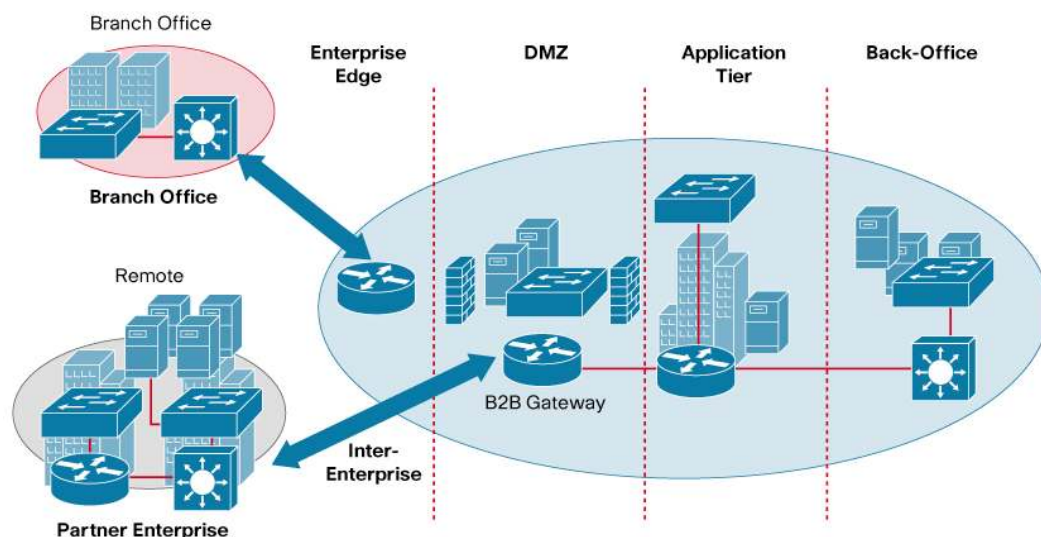
The following tools are available to configure and manage these devices:

- **Cisco AON Development Studio (ADS)**—Cisco AON ADS is used to create message plans, which represent a set of operations (bladelets) to be applied to application messages.
- **Cisco AON Management Console (AMC)**—Cisco AON AMC provides centralized control for configuration, certificate management, and lifecycle management of a distributed AON network.

## Usage Scenarios

The Cisco AON platform helps enable a wide range of different usage scenarios across a customer application network. Following are summaries of some of the usage scenarios in which Cisco AON is typically deployed.

**Figure 2.** High-Level Network Architecture



- **Cisco AON in the remote office or business-to-business (B2B) spoke**—At a remote office or B2B spoke, Cisco AON devices can be deployed as an infrastructure consolidation device. A single AON 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. Additionally, Cisco AON AMC provides centralized management of a distributed branch-office deployment of application policies.
- **Cisco AON at the enterprise edge**—At the enterprise edge, Cisco AON can act as an application-security gateway or a B2B gateway. As an application security gateway, it can intercept and analyze traffic in message formats such as Extensible Markup Language (XML). As a B2B gateway, Cisco AON helps enable a transparent interface with trading partners by providing security, protocol bridging, and message validation and transformation services.
- **Cisco AON at the enterprise core**—In the enterprise core, Cisco AON provides transparent interapplication communication and application delivery; it provides a network-embedded communication bridge between protocols and applications. Cisco AON optimizes application delivery by helping applications offload infrastructure functions such as message-level load balancing to the network where they can scale effectively.

## 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, etc.). 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**—After principal credentials are obtained through message inspection, Cisco AON can determine which level of access the originator of the message should have to the

services it is attempting to invoke. Specific 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.

- **Non-repudiation and data integrity**—Cisco AON can digitally sign entire messages or individual message elements at any given AON device. Specific 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 (an entire message, the message body, individual elements, and their contents). Specific 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**—The key management functions provided by the Cisco AON Management Console (AMC) allows users to register, configure, bind, and provision keys and certificates from the Cisco AON AMC server to the AON device. Specific capabilities include: generate, register, and obtain Class 2 and Secure Sockets Layer (SSL) certificates using Verisign Class 3 Certificate Service; fetch, upload, and import SSL certificates; import PKCS#12 certificates; and import keys from Java keystores.
- **Transport-layer security**—Cisco AON supports transport-layer security mechanisms such as SSL 3.0 and Transparent LAN Services (TLS) 1.0.

### Visibility

Because Cisco AON can act as a network interception point for application message traffic, each node can be configured to act as a sensor that can capture, process, and log highly granular information about application messages. This in-flight capability helps Cisco AON provide an event-capture fabric for application messages. The user can specify through the Cisco AON ADS the types of messages AON should capture for visibility. Cisco AON can inspect the messages and apply these rules at the message-content level.

- **Out-of-band message processing through promiscuous mode**—Cisco AON provides an industry-first capability to receive and process messages without introducing latency in the flow of inline network traffic, helping enable out-of-band monitoring and analysis. For example, FIX and HTTP sessions are received out of band, assembled to recreate the original message, and then appended with relevant metadata such as timestamps and relevant TCP headers. These messages can then be used to analyze a variety of possible scenarios such as transaction monitoring, intrusion detection, insider threats, FIX monitoring, etc. Additionally, service-level agreement (SLA) customers can take advantage of the extensibility framework to tap and frame their proprietary message formats.
- **Logging**—Cisco AON provides the ability to log messages to external systems for future analysis by third-party applications or tools.
- **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**—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, a message can be sent to operations personnel to take corrective action.

## Intelligent Message Routing

Given its central role as an intermediary in highly heterogeneous application environments, it is essential for Cisco AON to flexibly adapt to different types of enterprise information, business policies, and endpoints. Cisco AON operates at the application-message level, thus allowing a higher degree of flexibility in message

- **Application Quality of service (AppQoS)**—Cisco AON offers an industry-first AppQoS feature that helps 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 over price quotes, and enforce that priority end to end, across the application infrastructure and the network. The priorities set at application and transaction levels 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 end result for the business is better alignment of IT infrastructure usage with a higher degree of automatic SLA enforcement, even in times of severe network congestion.
- **Protocol support**—To integrate easily into existing environments, Cisco AON understands various application access methods and provides adapters for today's most commonly used protocols, HTTP, HTTPS, Tibco Element Management Solution (EMS), WebSphere MQ, and WebSphere JMS. Additionally, a custom adapter software development kit (SDK) is available for creation of new adapters to any environment. Most of the 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; an example is the node receiving an application message through WebSphere MQ and sending the same message to another application as a HTTP post. Cisco AON supports protocol translation between any combination of the supported protocols, for instance between HTTP(S) and a Tibco message queue.
- **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 the built-in XSLT-based transformation engine using XSLT style sheets written or procured by the customer, allowing any combination of transformations from XML to other XML or non-XML formats, or conversely. 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 an application message, Cisco AON can act as a proxy that provides an abstraction layer for endpoint applications and apply policies across all these services without the endpoints being aware of the intermediary. This powerful capability allows centralized configuration and control with consistent, distributed enforcement everywhere in the network—a particularly relevant capability given today's highly distributed service-oriented applications.
  - *Content-based routing*—Messages can be routed to an appropriate destination by matching content elements against pre-established policy rules. Cisco AON examines message types or fields (for example, part number, account type, employee location, zip code, etc.) and sets the destination based on rules that specify the routing decision (for

example, based on source or destination URL), protocol header (for example, HTTP or JMS), content inspection of XML paths (XPath) (value of a PO), or other states resulting from a previous operation.

- *Load balancing*—Based on configurable policies and rules, Cisco AON can load balance across multiple endpoints using a variety of 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).
- *Message distribution*—Cisco AON also 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.
- *Reliable messaging*—Cisco AON provides a reliable delivery semantic across multiple protocols. Reliable delivery semantics include: Exactly Once Delivery (for queue-based or other reliable protocols) and At Least Once Delivery.

### Application Optimization

Cisco AON takes advantage of a combination of technologies to enhance message-handling performance and provide superior levels of application availability. It should be noted that in a typical scenario only a fraction of the network traffic flow is selected for attention by AON and redirected through the Cisco AON service module or network nodule, so the vast majority of network traffic passes through as usual. For those packets processed by the 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 (CBR) and XML schema validation. In addition, customers can plug in custom functions that take advantage of the optimized execution path to meet their high-performance needs.
- **Hardware acceleration**—For some performance-intensive operations such as security and XML operations, 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 network bandwidth usage. Either XML and non-XML 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, load balancing, and scalability**—As described in the “Intelligent Message Routing” section, Cisco AON can sit in front of an application cluster to provide high-availability and load-balancing services to the applications.

### Extensibility

Built on an open, extensible architecture, Cisco AON includes a set of application programming interfaces (APIs) to add new adapters and bladelets. It provides an interface to develop extensions to the base AON platform using languages such as Java, C, or other languages.

- 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 architected for high performance and scalability to address the needs of the most demanding applications. It accomplishes this through:

- **Hardware-based acceleration**—By offloading compute-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.

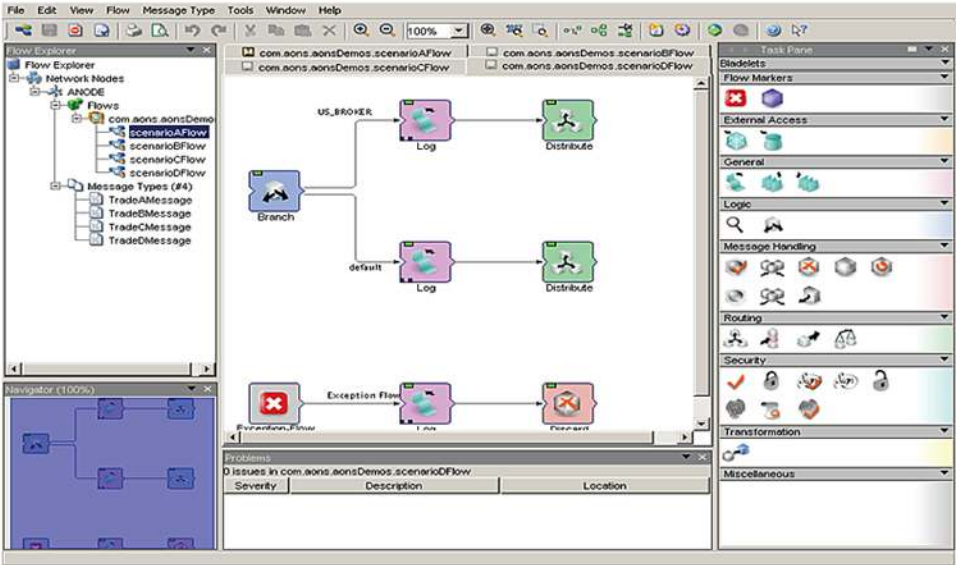
### Cisco AON Design, Configuration, and Management

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 AON ADS**—Cisco AON ADS is a Windows-based tool for developers to configure how application messages are handled at runtime.
  - Easy drag and drop GUI environment
  - Set of preconfigured functions or bladelets (described in the features section previously) that can be used to create message plans
  - One-button synchronization of message plans with the Cisco AON AMC
  - An SDK for creation of custom bladelets and an ADK for creation of custom adapters

**Figure 3.** ADS Design-Time View





- **Cisco AON AMC**—Cisco AON AMC is a Linux-based Web application with full role-based access control for centralized management of the AON system. It helps ensure consistent and up-to-date configurations across all the Cisco AON devices (nodes) in a distributed infrastructure. Cisco AON AMC functions include support for:
  - Configuring and managing 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

Figure 4. AMC Console View

The screenshot shows the AONS Management Console web application running in a Microsoft Internet Explorer browser. The address bar shows the URL: `https://localhost:7010/amc/Monitor_All.do?actionNum=0&selectedSubMenu=submenu.ViewEvents&nodeType=network`. The application has a navigation bar with tabs: Network, Policies, Keystores, Deploy, Monitor (selected), and Admin. The main content area is titled 'Network Nodes: View Events' and displays a table of network nodes.

#	Name	Owner ID	Admin State	Description
1	Node1	Node1	Unregistered	
2	node2	node2	Unregistered	
3	Node3	Node3	Unregistered	

Below the table, there is a pagination control showing 'Rows/Page 10', 'Page 1', and a 'Go' button. There are also 'View Events' and 'Clear Events' buttons.

Table 1. ADS System Requirements



Feature	Description
<b>Disk Space</b>	Cisco AON ADS: 40 Gb minimum
<b>Hardware</b>	Single processor, Pentium III or later
<b>Memory</b>	Cisco AON ADS: 512 MB minimum (1 GB recommended)
<b>Software</b>	Cisco AON ADS: Microsoft Windows 2000 or Windows XP

**Table 2.** AMC System Requirements

Feature	Description
<b>Disk Space</b>	Cisco AON AMC: 20 Gb minimum
<b>Hardware</b>	Single processor, Pentium III or later
<b>Memory</b>	Cisco AON AMC: 512 MB minimum
<b>Software</b>	Cisco AON AMC: RedHat Linux (RHEL) AS or ES 3.0 or later

**Table 3.** AON Supported Standards

Feature	Description
<b>Transport Protocols</b>	HTTP, HTTPS, JMS, Tibco EMS, and WebSphere MQ
<b>Database</b>	Oracle 9i (9.2) and Sybase 12.5.1
<b>Security</b>	DES, 3DES, AES, RSAv1.5, SHA-1, PKCS#12, SSL3.0, and TLS 1.0
<b>Management</b>	Simple Network Management Protocol Version 2 (SNMPv2) and command-line interface (CLI)
<b>XML Processing</b>	XML encryption, XML digital signatures, schema validation, XSLT 1.0, SOAP 1.1, 1.2, and XPath 1.0

## 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 helps ensure a quality, reliable implementation. For more information about Cisco services, refer to [Cisco Technical Support Services](#) or [Cisco Advanced Services](#).

## Summary

As the flagship for a new technology paradigm, Cisco Application-Oriented Networking (AON) provides the foundation for a new class of Cisco products. Cisco AON provides an essential point of convergence to unite networks with applications based on today's highly distributed, service-oriented, and older architectures. It embeds a new class of application intelligence into the network to better meet the underlying needs of applications for security, visibility, event-driven messaging, optimized delivery, and other core integration and deployment services.

Cisco AON complements existing networking technologies by providing a greater degree of awareness about the information flowing through the network, helping customers route information between disparate applications, enforce security policies, optimize the flow of application traffic, and provide improved visibility of information. Cisco AON provides this enhanced level of application intelligence within the network by understanding more about the content and context of the information flow at the application message level rather than the packet level.

Cisco AON is an important component of the Cisco Intelligent Information Network (IIN) vision and strategy. Cisco IIN provides the foundation for building network infrastructure that meets a company's most strategic business objectives aligned with industry trends such as virtualized computing and service-oriented architectures. As the point where networks and applications converge, Cisco AON points the way to a new era of business relevance for the network—as a strategic enabler and accelerator of today's distributed, service-oriented, and traditional business applications and processes. The results are rapid time to market, readily extensible collaboration, and on-demand computing—together producing sustainable competitive advantage.

### 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](http://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](http://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](http://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](http://www.cisco.com/go/offices).

©2006 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, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, 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, Fast Step, Follow Me Browsing, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, Packet, PIX, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StackWise, 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. (0609R)