Q&A

Cisco Data Center Solutions for Application Networking Services

Q. What are the Cisco® Data Center Solutions for Application Networking Services?

A. Cisco Data Center Solutions for Application Networking represent the centralized set of solutions focused on helping organizations scale, deliver, and optimize business applications and their infrastructure. By deploying these solutions, customers see dramatic improvements in application performance, quicker time to deployment and operation, and a decrease in the number of resources required to meet the business demands. These benefits are realized without incurring additional expenditures in the form of development, server resources, or bandwidth. Products include:

- (New) **Application infrastructure control module for the Cisco Catalyst® 6500**: Cisco Application Control Engine (ACE)
- (New) Application security software module for the Cisco AVS 3120 Application Velocity System
- **Application load balancing appliances**: Cisco CSS 11500 Series Content Services Switch
- **Application load balancing for the Cisco Catalyst 6500**: Cisco Content Switching Module (CSM) for the Cisco Catalyst 6500
- **Application load balancing and Secure Sockets Layer (SSL) acceleration**: Cisco CSM-S Module for the Cisco Catalyst 6500
- **Global load balancing**: Cisco GSS 4400 Global Site Selector switch
- **Application acceleration and application security**: Cisco AVS 3120 Application Velocity System
- **Application acceleration and application security management**: Cisco AVS 3180 Application Velocity System

Q. How do these solutions relate to Cisco's announcement of a new advanced technology, Cisco Application Networking Services?

A. The launch of these solutions in the data center is the first announcement of new products and enhancements to the Cisco Application Networking Services category. In combination with solutions for the WAN and the branch and the application-oriented networking solutions, Cisco provides customers with the ability to comprehensively deliver their business functions across the network. Application delivery solutions provide scalability, acceleration, and optimization between any client and applications or business functions.

Q. What is new in this announcement?

A. New in the announcement are Cisco Application Control Engine (ACE), a new, high-performing application services module for the Cisco Catalyst 6500, and a software module for the Cisco Application Velocity System AVS 3100, adding significant features and functions for application security.

The ACE is a new services module for the Cisco Catalyst 6500 that provides organizations with new levels of control over the way that they deploy, operate, deliver, secure, and manage their applications and business services across the extended enterprise. It enables greater control over application infrastructure, allowing organizations to deploy and migrate applications more quickly, deliver the highest levels of services to end users, and simplify the overall management and operation of their data centers. The device incorporates role-based access control, a powerful workflow engine, and management tools and application programming interfaces (APIs). With throughput of up to 16 Gbps per module and architectural extensibility to incorporate future functions, the Cisco ACE sets a new performance standard for providing application supporting services in the data center. The Cisco AVS software module adds advanced bidirectional application security functions to the AVS 3100 family. Coupled with the new application security module on the AVS, Cisco ACE provides the application infrastructure control, performance, security and a simplified infrastructure to help IT meet ever-increasing business challenges.

Q. How does the Cisco ACE fit in with the Cisco Data Center Solutions for Application Networking?

A. The Cisco ACE represents the next-generation application services module within the family of application networking solutions. Initially, ACE is targeted at the largest and most demanding data center environments where its performance and functional capabilities are required. As such, customers focusing on more discrete problems or in smaller environments will continue to find great value in the Cisco Content Switching Module (CSM). For customers who desire the appliance form factor, the Cisco Content Services Switch (CSS) line in combination with the Cisco AVS appliances is the leading choice.

Table 1. CSS, CSM and ACE Product Comparison

	Cisco CSS 11501	Cisco CSS 11503	Cisco CSS 11506	Cisco CSM for Catalyst® 6500	Cisco ACE for Catalyst® 6500
					
Form Factor	Standalone fixed	Standalone modular	Standalone modular	Integrated module	Integrated module
Port Density	8 FE Standard 1 GE Option	2 GE Standard Up to 32 FE/6 GE	2 GE Standard Up to 80 FE/12 G	46-528 FE 8-178 GE	46-528 FE 8-178 GE
Site Activity	Low	Medium	High	High	Highest
Hardware Scalability	★	★★	★★	★★★	★★★★
Hardware Redundancy	No	No	Yes	Yes	Yes
Session Redundancy	Yes	Yes	Yes	Yes	Yes
Layer 2–3 Networking	Yes	Yes	Yes	Yes	Yes
Management/Control	Yes	Yes	Yes	Yes	Yes
SSL Acceleration	External	Internal	Internal	Catalyst 6500 SSL Module	Internal
Content Switching	Servers, caches, firewalls, VPN				

POSITIONING

Q. What is the Cisco ACE?

A. The Cisco Application Control Engine, a multifunction module for the Cisco Catalyst 6500, that allows organizations to rapidly deploy, provision, accelerate and manage application deployments. By logically partitioning the infrastructure to minimize physical application silos, providing new standards in performance and security, and integrating multiple functions, Cisco ACE gives IT unprecedented control and delivers new levels of service velocity and high-performance service on behalf of the business.

The Cisco ACE solution provides the following:

- **Application infrastructure control**—Providing IT with a next-generation solution to better control the way they deploy, operate, and manage their application infrastructures with virtual partitioning and role-based access control
- **Application performance**—Providing the highest performance, maximum scalability and best availability for data center application delivery

- **Application security**—Ensuring that critical applications, infrastructures, and data are protected from abuse and misuse
- **Infrastructure simplification**—Minimizing the cost and complexity of the infrastructure and reducing the number of devices and vendors by integrating with the Cisco Catalyst 6500, the industry's leading enterprise-class switch

Unlike application front-end appliances, it is the *only product of its type fully integrated with the network*, delivering the capability to create fully virtualized partitions that allow centralized deployment with decentralized management allowing individual application teams to have full administrative control. Cisco ACE provides all services, from Layer 2 through 7, to be partitioned within a single module with resource guarantees and full role-based access control (RBAC).

Q. What does Cisco mean by Application Infrastructure Control?

A. Given the increasing pressure on the IT organization and the need to move more quickly and collaborate across organization silos, customers require a solution that provides tremendous control of the application infrastructure. Cisco ACE introduces the concept of virtual partitions, where a single physical device can act as up to 250 separately managed and operated logical devices. It can be logically partitioned to support completely separate management contexts using either a GUI-based device manager, powerful command-line interface (CLI), or an Extensible Markup Language (XML)-based application programming interface (API). Resources can be allocated and managed based on business, application, or customer segmentation requirements. Change control (add, delete, or change) can be done on a per-logical/-virtual instance, and RBAC gives even more granular control with the ability to fully delegate administrative responsibility to teams using the services of a single ACE module simultaneously. The combination of virtual partition and RBAC enables simplified workflow by delegation of functional responsibility. Because Cisco ACE provides this layer of logical abstraction, it complements other virtualization and management approaches, including switching and routing (through VLAN and virtual route forwarding [VRF]), storage (through virtual storage-area networks [VSANs]), and application and security services. This operational flexibility enables quick response to business and customer demands—and does so at a lower cost and operational complexity. By ensuring the maximum flexibility of deployment and control, Cisco ACE delivers the highest performance, most scalable and most efficient use of the application infrastructure as a whole.

Q. Why would an organization need Cisco ACE?

A. The Cisco ACE is a new product line from Cisco Systems® that offers the highest level of network and application performance, operational flexibility, security, and application acceleration for enterprise and service provider customers. The Cisco ACE helps customers reduce their operating costs while simultaneously increasing security and improving the end-user application experience. Although all customers considering this function can gain value, ACE is most appropriate for the large organizations that both demand the largest scalability and have the greatest need to rationalize their approach to application deployment.

Q. What is the relationship between the Cisco ACE Services Module and Cisco Application-Oriented Networking (AON)?

A. The Cisco ACE Module is focused on providing applications with a scalable, reliable, secure, and high-performance infrastructure. In combination with the Cisco AVS, Cisco ACE is primarily focused on delivering better end-user response times using the least resources. The Cisco AON technology is primarily designed to support communications between business applications to provide message transformation and switching for distributed applications. The ACE and AON are designed to solve different problems within customer organizations.

Q. How does the Cisco ACE Services Module enhance the service module offerings for the Cisco Catalyst 6500?

A. Cisco ACE represents the next generation of technology currently delivered on the Cisco CSM and Cisco SSL Module (SSLM). Previous service modules focused on a specific data center task and performed these at speeds appropriate for the general customer population. The Cisco ACE Module, by introducing virtual partitions and consolidating multiple services on a single extensible line card, delivers these services at unprecedented throughput, scalability and security that can be used for any IP-based application across the data center.

Q. What market does the Cisco ACE Services Module address?

A. The Cisco ACE Services Module addresses the market commonly referred to as the application delivery space. Today, these functions include server load balancing (SLB) and Layer 4–7 switching, advanced application optimization services, and server off-load functions such as SSL acceleration and TCP resue—all of which and more are supported by the Cisco ACE and its companion solutions such as the Cisco AVS.

Q. How does the Cisco ACE Services Module fit in the Cisco Business Ready Data Center?

A. It fits in the standard Cisco Catalyst 6500 chassis and can be included in a business ready data center as a multifunction device that incorporates a variety of services with new levels of application infrastructure control, acceleration performance, application security and infrastructure simplification. It works hand-in-hand with the new Cisco AVS product for additional Web application acceleration and in-depth application protocol/payload security.

Q. Can I upgrade my existing service module to a Cisco ACE Services Module?

A. No. The Cisco ACE Services Module is a new hardware and software solution. However, existing services modules such as the Cisco CSM can coexist within the same chassis.

Functions

Q. What are the main deployment scenarios for the Cisco ACE?

A. The Cisco ACE Services Module is typically deployed in a data center in front of multiple server farms and in support of many application types. It is typically configured with client VLANs that service internal and external user application requests as well as server VLANs that allow for segregation and protection of server resources.

Q. What are the core features of the Cisco ACE Services Module?

A. The core features of the Cisco ACE Services Module fall into the following categories: application infrastructure control, application performance, application security, and infrastructure simplification. In short, the explanations are as follows:

- Unprecedented control for IT over the deployment and management of application service—By creating virtual partitions and with RBAC, IT can dramatically improve service velocity, reduce management overhead, and simplify workflow. The device includes multiple management interfaces, including an XML API, a management GUI, and a rich command-line interface (CLI).
- Industry-leading performance and scalability of up to 16-Gbps throughput and 345,000 Layer 4 connection setups per second per module to handle very large data files and rich media and large user bases.
- Rich levels of application and network security, including bidirectional support for content inspection, SSL encryption and decryption, and transaction logging for application security forensics.
- Integration of Layer 2 to 7 functions by working with the controller and input/output ports of the market-leading Catalyst 6500 enterprise-class switch in the same chassis and consolidation of multiple services within a single processing path yielding greater traffic efficiency, tighter network design, fewer devices, superior availability and easier management.

The core features represent the following detailed functions:

SLB

- **Predictors**—Round robin, Weighted Round Robin, least connections, IP hash, connection watermarks, and content awareness
- **Health probes**—Layer 3 ping, Layer 4 User Datagram Protocol (UDP) data, HTTP GET, HTTP HEAD, Domain Name System (DNS), point of presence (POP), Internet Mail Access Protocol (IMAP), Telnet, Internet Control Message Protocol (ICMP), TCP, UDP, Echo, Finger, Simple Mail Transfer Protocol (SMTP), RADIUS, Lightweight Directory Access Protocol (LDAP), and HTTP GET over SSL
- TCP connection management (multiple client TCP connections traverse a single-server TCP connection)
- HTTP redirection
- **Persistence**—Cookie, cookie insert, offset and length, and header insert
- **Redundancy**—Active-active, stateful, and active-backup

SSL Off-Load

- SSL decryption
- SSL encryption
- Centralized certificate management
- Back-end SSL
- Export cipher suite
- SSL v2 and v3 and transparent LAN services (TLS) v1.0
- Step-up certificates

Data Center Security

- Protocol inspection and fixup of the most popular data center protocols
- Access control lists (ACLs) with up to 256,000 access control elements to selectively allow traffic between ports
- SYN cookies
- TCP connection state tracking
- Virtual connection state for UDP
- SEQ number randomization
- TCP header validation
- TCP window size checking
- Unicast Reverse Path Forwarding (URPF) checking at session establishment

Q. What are the performance characteristics of the Cisco ACE Services Module?

A. The Cisco ACE Services Module brings the highest performance to the application delivery market: up to 16 Gbps of throughput and sustained rate of 345,000 Layer 4 connection setups per second by a single service module; up to 4 ACE modules can be housed in a single Catalyst 6500 chassis offering maximum scalability. Performance metrics are available in the data sheet and can be found online at http://www.cisco.com/go/ace.

Q. What supervisor engines are compatible with the Cisco ACE Services Module?

A. The Cisco ACE Services Module is initially supported by the Cisco Catalyst 6500 Series Supervisor Engine 720 (with a policy feature card 3A [PFC3A], PFC3B, or PFC3b-XL).

Q. Does the Cisco ACE Services Module run Cisco IOS® Software?

A. No. The Cisco ACE Services Module runs its own operating system. The ACE is a Catalyst 6500 fabric-enabled module.

Q. Can I put the Cisco Catalyst 6500 Series Firewall Services Module, Cisco CSM, Cisco SSLM, and Cisco ACE Services Module together in the chassis?

A. Yes.

Q. Does the Cisco ACE Services Module have any external interfaces?

A. Yes. The Cisco ACE Services Module provides several management interfaces for external control. First, ACE has a relatively standard external console port for administrative access for using a standard CLI. Second, ACE provides an XML API for integration with management tools and to be controlled by specific applications themselves. Finally, there will be a full GUI-based manager that will provide full support for all functions and RBAC. While operational, the Cisco ACE can be sessioned into from the supervisor engine of the Catalyst 6500. The ACE has no data input/output ports.

Q. How many Cisco ACE Services Modules can I put into one Catalyst 6500 chassis?

A. Up to 4 Cisco ACE Services Modules are supported per chassis.

Q. Does the Cisco ACE Services Module support failover?

A. Yes. Failover is supported per virtual partition between application instances using a redundant Cisco ACE Services Module. Stateful redundancy is available for traditional active-standby and active-active configurations. Stateful failover is supported both within the chassis and across chassis between peer ACE modules. In combination with the Cisco Global Site Selector (GSS) 4400, the ACE module can be used for failover scenarios involving remote data centers.

Q. How many virtual partitions are supported by the Cisco ACE Services Module?

A. The Cisco ACE Services Module supports up to 250 virtual partitions.

Q. Does the Cisco ACE Services Module work in any Cisco Catalyst 6500 or Catalyst 7600 Series chassis?

A. Yes. The Cisco ACE Services Module is fabric-enabled and should work in any Cisco Catalyst 6500 or Catalyst 7600 Series chassis form factor. However, at first ship the ACE has only been tested inside the Cisco Catalyst 6500 Series enterprise-class switch.

Q. How much flash and DRAM memory is available on board? Can the DRAM be upgraded?

A. The Cisco ACE Services Module comes with 256 MB of removable flash memory and 3 GB of DRAM. The DRAM is not upgradable.

Q. Is the Cisco ACE Services Module supported in both native Cisco IOS Software and hybrid systems?

A. Yes.

Q. How is geographic diversity supported with a Cisco ACE Services Module for a high-availability data center?

A. Global SLB is offered by the Cisco GSS 4400 Global Site Selector. It can support high availability of Cisco ACE Services Modules that are deployed in separate geographic areas.

COMPONENTS

Q. What are the components of the Cisco ACE Module?

A. In first release, the new Cisco ACE product line is available as a services module for the Cisco Catalyst 6500. The Cisco ACE is a line card for the Cisco Catalyst 6500 and can be used in any Cisco Catalyst 6500 chassis running a Supervisor Engine 720 and Cisco IOS Software Release 12.00(0). The Cisco ACE Module contains no I/O ports and relies on the Cisco Catalyst switch for network connectivity.

CISCO AVS QUESTIONS

Q. What is the new Cisco AVS 6.0 Web Application Firewall feature set and what problem does it solve?

A. Web application security is important because Web applications open a large and potentially dangerous hole in an organization's security fabric. Traditional firewalls protect at the port and source/destination levels, but do very little to identify and protect against dangerous traffic type and content. As a result, hackers are able to target business applications to obtain information or money or to disrupt service.

The new Cisco AVS 3120 Web Application Firewall Module delivers the highest level of attack protection available for Web applications. By scanning all application protocols and content and applying business-specific policies, the AVS can protect the infrastructure and the organization against application-layer attacks such as Structured Query Language (SQL) injection, data theft, parameter tampering, cookie poisoning and much more. It can be deployed easily and rapidly by network security professionals, making the Cisco AVS 3120 an ideal solution for immediate risk remediation for all enterprise applications. With unprecedented application layer visibility, the Cisco AVS 3120 provides real-time threat protection and analysis with no-risk network deployment options.

Q. What are the new features in Cisco AVS 6.0?

A. The new features in Cisco AVS 6.0 software focus on improving the Web application security functions (Table 2).

Table 2. Table 2 New Cisco AVS 6.0 Features

	New Features	Benefits
Improvements to Attack Prevention and Input Validation	• The number of predefined application layer attack rules is increased • Customizable regular expression (regex) for creating rules is exposed in the GUI • Usability on creating rules and setting precedence is improved • Users can now set rules in active or passive mode	• Offers highest level of attack prevention in the industry • Protects Web applications from: – SQL injection – Cross-site scripting – Lightweight Directory Access Protocol (LDAP) injection – Command injection – Buffer Overflows – Malicious Code Injection
Application Learning	• The application learns parameters in real time • The application quickly creates rules base on application knowledge • The application dynamically creates security rules based on logs	• Provides accurate security policy • Prevents parameter tampering • Reduces deployment costs
HTTP Normalization	• The HTTP protocol normalizes all application traffic	• Thwarts encoded and disguised attack techniques • Stops directory traversal and other encoded-related attacks
HTTP Protocol Conformance	• HTTP protocol conformance is enforced	• Stops a broad range of URL-based attacks
Cookie Protection	• Users can encrypt or tamper-proof cookies in real time	• Stops cookie snooping, tampering, and other cookie-based attacks
Application Cloaking	• Application cloaking masks server headers • Application cloaking blocks and customizes error return codes	• Deters application reconnaissance
Request Limits	• Requesting limits enforces URL and header limits.	• Stops buffer overflow attacks
Monitoring and Logging	• All Web attacks are logged through syslog • Logging provides a graphical representation of attacks	• Provides accurate monitoring and forensics
Data-Theft Protection	• Full protection from theft of confidential data such as credit card and social security numbers is provided • Data structures are customizable	• Helps ensure compliance with the tough privacy requirements mandated by regulations such as Health Insurance Portability and Accountability Act of 1996 (HIPAA), Gramm-Leach-Bliley, and CA SB-1386
Out-of-Band Monitoring	• This out-of-band deployment architecture transmits no traffic into the network, introduces no points of attack for hackers, and adds no delay to traffic on the network	• Offers risk-free and low-cost deployment • Provides insight into application layer attacks with minimal management requirements

Q. How is the Cisco AVS Web Application Firewall different from an intrusion prevention system (IPS)?

A. IPSs are solid solutions for protecting against attacks targeted at known vulnerabilities in major platforms such as Windows, Solaris, Apache, or Microsoft Internet Information Services (IIS). Cisco AVS excels at protecting against attacks targeted at business applications or Websites. These applications might be software vendor-built applications or in-house custom applications. Security patches and signatures are typically not available for these types of applications, and building these levels of security into each application would be nearly impossible.

Q. How is the Cisco AVS Web Application Firewall different from a network firewall?

A. The Cisco AVS 3120 and network firewalls such as the Cisco PIX® Firewall and Cisco ASA 5500 Series Adaptive Security Appliances are complementary products. The Cisco AVS Web Application Firewall secures Web-based applications; network firewalls excel at securing networks; and the Cisco AVS provides defense in depth for Web applications.

Network firewalls enforce policy on networks, IP addresses, and ports; they have a broad set of application layer features for many different protocols. The firewall can and will be deployed in many locations, including branch, network edge, enterprise edge, etc. The Cisco AVS enforces policy on HTTP data such as URLs, headers, and parameters. The Cisco AVS is deployed only in the data center in front of Web applications.

Q. Can you tell me about the various Cisco AVS 3100 Series Application Velocity System appliances?

A. Cisco originally shipped the Cisco AVS 3110 Application Velocity System. The Cisco AVS 3110 appliance product was the result of the Cisco Systems acquisition of Fineground Networks. The latest version of software supporting that appliance was Fineground Version 5.0 software. This appliance-based product had “Fineground Networks” logos, documentation splash screens, colors, etc.

The Cisco AVS 3120 and AVS 3180 are appliances built by Cisco with Cisco logos, documentation splash screens, colors, etc. These appliances replace the Cisco AVS 3110 appliance.

The Cisco AVS 3120 is an inline appliance for improving Web application performance and providing Web application security. The Cisco AVS 3180 Management Station is an optional appliance-based management console for configuring and managing Cisco AVS 3120 appliances. The Cisco AVS 3180 is also required if customers require the Cisco AVS AppScope Monitor performance monitoring capability. The Cisco AVS 3120 has an embedded device manager and does not require the Cisco AVS 3180 for configuration.

Q. Which appliances support Cisco AVS 6.0 versions of software?

A. Cisco AVS 6.0 software is not supported on the Cisco AVS 3110 hardware. Customers must upgrade to the Cisco AVS 3120 hardware to run Cisco AVS 6.0 software.

The optional Cisco AVS 3180 Management Station must be upgraded to Cisco AVS 6.0 Management Station software to manage a Cisco AVS 3120 appliance with Cisco AVS 6.0 software. A Cisco AVS 3180 Management Station with Cisco AVS 6.0 Management Station software requires that all Cisco AVS 3120 hardware run Cisco AVS 6.0 software. A mixed environment of Cisco AVS 5.0 and AVS 6.0 software cannot be managed with a Cisco AVS 3180. A Cisco AVS 3180 Management Station with Cisco AVS 6.0 software will not manage a Cisco AVS 3110 with any version of software.

Q. Is the current Cisco AVS 5.0 AppScreen Web Application Firewall function still available in Cisco AVS Version 6.0 software?

A. Yes, the AppScreen feature set is still available with the Cisco AVS 6.0 software. AppScreen and the new Web application security features are different software modules, and they provide some similar feature sets. It is expected that AppScreen features will be removed from the software in the next major release of AVS software, as people begin to understand the replacement-configurable parameters within the new Web application security module.

Q. What are the deployment modes for Cisco AVS 6.0?

A. Cisco AVS 6.0 has three deployment modes: out-of-band monitoring, inline transparent mode, and gateway mode. Gateway mode requires the same network configuration as Cisco AVS 5.0 software, and deploys essentially as a reverse proxy in front of the applications. Both the acceleration and the Web application security feature sets can run simultaneously in this mode. Inline transparent and out-of-band monitoring are applicable only for the new Web application firewall features. Inline transparent mode enables the Cisco AVS to deploy in line with no changes to other network configurations such as default gateways. Both inline transparent mode and gateway mode can be deployed using Cisco CSS or CSM load balancing for availability and scalability. Out-of-band monitoring mode deploys off a span port on a switch. The span port replicates all Web traffic to and from the application and forwards it to the Cisco AVS. This deployment option is risk-free. However, this mode logs and alerts only on potential attacks, and it does not block traffic if an attack is detected.

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 Website at 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

Printed in the USA C67-342680-00 04/06