Cisco ACE Application Control Engine Module for Cisco Catalyst 6500 Series Switches and Cisco 7600 Series Routers

Product Overview

The Cisco® ACE Application Control Engine Module for the Cisco Catalyst® 6500 Series Switches and Cisco 7600 Series Routers represents the next generation of application switches for increasing availability, acceleration, and security of data center applications.

The Cisco ACE Module allows enterprises to accomplish four primary IT objectives for application delivery:

- Increase application availability
- Accelerate application performance
- Secure the data center and critical business applications
- Facilitate data center consolidation through the use of fewer servers, load balancers, and firewalls.

The Cisco ACE Module (Figure 1) achieves these goals through a broad set of intelligent Layer 4 load-balancing and Layer 7 content-switching technologies integrated with leading-edge acceleration and security capabilities. A crucial design element of Cisco ACE, and a differentiator between the Cisco solution and other solutions in the marketplace, is its ability to use virtualized architecture and role-based administration capabilities that streamline and reduce the cost of operations involved in deploying, scaling, accelerating, and protecting applications.

The Cisco ACE Module provides best-in-industry scalability and throughput for managing application traffic, up to 16 Gbps in a single module; up to four modules can be run in a single Cisco Catalyst 6500 Series chassis, upgradeable through software licenses or new module additions, thus providing IT with long-term investment protection and scalability.

Additionally, through its unique virtualization capabilities, Cisco ACE enables IT to provision and deliver a broad range of multiple applications from a single Cisco ACE Module, bringing increased scalability for application provisioning to the data center.

To increase application availability, the Cisco ACE Module uses best-in-class application switching algorithms coupled with highly available system software and hardware.

The Cisco ACE Module greatly improves server efficiency through highly flexible application traffic management as well as the offloading of CPU-intensive tasks such as SSL encryption and decryption processing and TCP session management.

Cisco ACE is designed to serve as the last line of defense for servers and applications in data centers. The Cisco ACE Module performs deep packet inspection and blocks malicious attacks. Highly scalable integrated security enables IT professionals to comprehensively secure high-value applications in the data center and facilitates consolidation in the data center.

By combining high-performance application delivery with a comprehensive set of state-of-the-art application delivery features, the Cisco ACE Module enhances IT efficiency and reduces the total cost of ownership (TCO). IT efficiency is increased through the use of innovative features such as virtual devices, role-based administration, instant application isolation, and single-view provisioning. Improved TCO is accomplished by consolidating most Layer 4 through 7 requirements into a complete and reliable application delivery platform.

Figure 1. Cisco ACE Module for Cisco Catalyst 6500 Series Switches and Cisco 7600 Series Routers

Features and Benefits

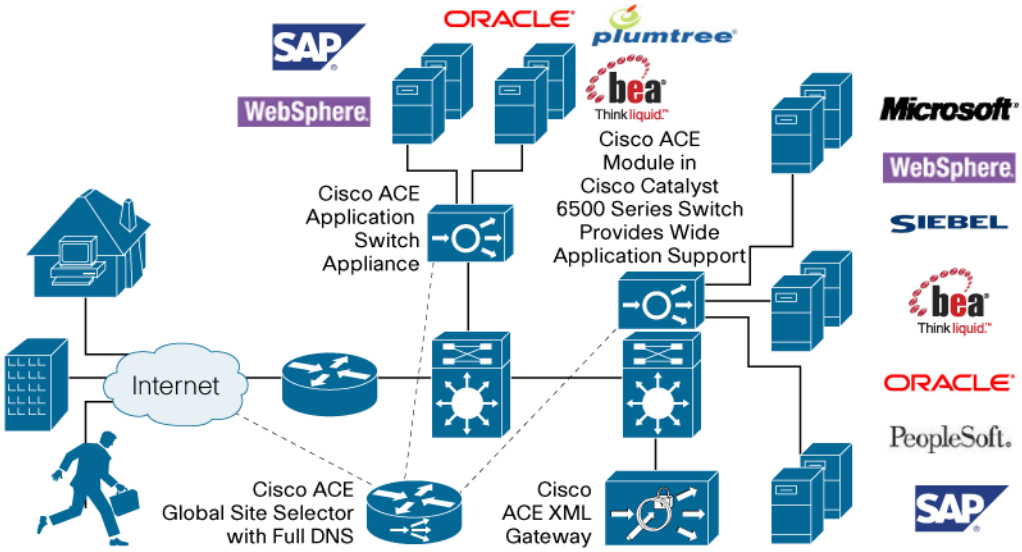
Table 1 summarizes the features and benefits that the Cisco ACE Module provides.

Table 1. Features and Benefits

Features	Benefits
Available	
Application switching	The Cisco ACE Module represents the next generation of application switches, delivering tightly integrated, essential application service functions in a single powerful system. It provides load-balancing and content switching functions with granular traffic control based on customizable Layer 4 through 7 rules. • Intelligent device load balancing: Cisco ACE provides support for Domain Name System (DNS), cache, transparent caches, firewalls, intrusion detection system (IDS), intrusion prevention system (IPS), VPNs, and SSL VPN. • Generic protocol parsing (GPP): Cisco ACE has native understanding of the following protocols: HTTP, FTP, DNS, Internet Control Message Protocol (ICMP), Session Initiation Protocol (SIP), Real-Time Streaming Protocol (RTSP), Extended RTSP, RADIUS, and Microsoft Remote Desktop Protocol (RDP). • Cisco ACE's GPP feature enables you to configure application switching and persistence policies based on any information in traffic payload for custom and packaged applications without requiring any programming. • The Cisco ACE performs payload parsing through hardware using a powerful regular-expression engine to obtain high performance, unlike other software-based solutions. • HTTP header manipulation: Cisco ACE supports the capability to modify, insert, or delete HTTP headers in both client requests and server responses. • Partial server farm failover: Cisco ACE provides the capability to determine which server farm (primary or backup) receives new traffic based on the number of available real servers (rservers.). • TCP dump: Cisco ACE can capture real-time packet information for the network traffic that passes through the Cisco ACE Module, for enhanced troubleshooting. • Source Network Address Translation (NAT) for virtual IP: Source NAT for virtual IP allows you to include a virtual IP address in the NAT pool for dynamic NAT and Port Address Translation (PAT), saving real-world IP addresses on the client-side network. • Source NAT for server farm: Source NAT can back up to a server farm multiple hops away during the failure of a primary server farm, resulting in continuous application availability even during a primary server farm failure. • Flexible network deployment: The Cisco ACE Module uses internal VLAN interfaces. VLANs can be assigned from the supervisor engine to the Cisco ACE. Corresponding VLAN interfaces then can be configured on the Cisco ACE as either routed or bridged. The Cisco ACE Module can be configured in the following modes: ◦ Routed mode: Cisco ACE can be configured to route the traffic when the client-side and server-side VLANs are on different subnets. ◦ Bridge mode: Cisco ACE can be configured to bridge traffic when the client-side and server-side VLANs are on the same subnets. ◦ Asymmetric server normalization (ASN): Cisco ACE can load balance an initial request from the client to a real server; however, the server directly responds to the client, bypassing Cisco ACE.
Predictors	Cisco ACE performs a series of checks and calculations to determine the server that can best service each client request depending on the load-balancing algorithm or predictor. Cisco ACE uses the following predictors to select the best server to satisfy a client request: adaptive response, least loaded, least bandwidth, least connections, round-robin, hash address, hash cookie, hash header, and hash URL.

Features	Benefits
Server health monitoring	To instruct Cisco ACE to check the health of servers and server farms, you can configure health probes (sometimes referred to as keepalives). The following probes are supported: ICMP, TCP, UDP, ECHO {tcp | udp}, Finger, HTTP, HTTPS, FTP, Telnet, DNS, Simple Mail Transfer Protocol (SMTP), Internet Mail Access Protocol (IMAP), Post Office Protocol (POP), RADIUS, scripted, Keepalive Appliance Protocol (KAL-AP), RTSP, SIP, HTTP return-code parsing, and Simple Network Management Protocol (SNMP) probes.
Persistence and stickiness	Cisco ACE provides stickiness that allows the same client to maintain multiple simultaneous or subsequent TCP or IP connections with the same real server for the duration of a session. Cisco ACE supports the following sticky methods: source or destination IP address, cookie, HTTP header, and SSL session ID.
Redundancy	The Cisco ACE Module offers three types of high availability: • Interchassis: A Cisco ACE Module in one Cisco Catalyst 6500 Series or Cisco 7600 Series device is protected by a Cisco ACE Module in a peer Cisco Catalyst 6500 Series or Cisco 7600 Series device. • Intrachassis: A Cisco ACE Module in a Cisco Catalyst 6500 Series or Cisco 7600 Series device is protected by another Cisco ACE Module in the same Cisco Catalyst 6500 Series or Cisco 7600 Series device. • Inter–virtual devices: A Cisco ACE Module supports high availability between virtual devices configured across two modules to allow specific devices to fail over without affecting the other devices and applications on a given module. Cisco ACE integrated with the Cisco Global Site Selector (GSS) can provide a multiple–data center failover system.
Fast	
User Datagram Protocol (UDP) booster	Cisco ACE can boost performance of UDP-based applications such as DNS load balancing to millions of requests per second.
UDP fast aging	Cisco ACE can provide very high scalability in terms of number of clients serviced for applications requiring a single response per request.
SSL acceleration	• The Cisco ACE solution integrates SSL acceleration technology, which offloads the encryption and decryption of SSL traffic from external devices (servers, appliances, etc.), thereby allowing the Cisco ACE to look more deeply into encrypted data and apply security and application switching policies. This enables the Cisco ACE to make more intelligent policy decisions and also helps ensure that your application-delivery platform complies with internal and external regulations. • With reencryption capabilities, Cisco ACE's SSL acceleration feature helps ensure end-to-end encryption of sensitive data while providing the capability to apply intelligent policies. ◦ SSL features supported: SSL termination and initiation, SSL Version 3.0, Transport Layer Security (TLS) Version 1.0, back-end SSL, exportable Rivest, Shamir, and Adelman (RSA) cipher suites, session ID stickiness, SSL URL rewrite (HTTP header rewrite), session ID reuse, client authentication, HTTP header insert of client and server certificate fields and SSL session parameters, HTTP Redirect on client authentication failure, strong RSA cipher suites, and Advanced Encryption Standard (AES) cipher suites. ◦ SSL accelerated protocols: HTTPS, Secure IMAP (IMAPS), Secure Lightweight Directory Access Protocol (LDAPS), Secure Network News Transfer Protocol (NNTPS), Secure POP Version 3 (POP3S), and Secure Telnet (STELNET) ◦ SSL accelerated ciphers: rsa-with-rc4-128-md5, rsa-with-rc4-128-sha, rsa-with-des-cbc-sha, rsa-with-3des-ede-cbc-sha, rsa-export-with-rc4-40-md5, rsa-export-with-des40-cbc-sha, rsa-export1024-with-rc4-56-md5, sa-export1024-with-des-cbc-sha, rsa-export1024-with-rc4-56-sha rsa-with-aes-128-cbc-sha, and rsa-with-aes-256-cbc-sha ◦ Public key exchange algorithm: RSA 512-bit, 768-bit, 1024-bit, 1536-bit, and 2048-bit ◦ Digital certificates: All major digital certificates from certificate authorities, including the following: VeriSign, Entrust, Netscape iPlanet, Windows 2000 Certificate Server, Thawte, Equifax, and Genuity ◦ Sample SSL key and certificate pair
TCP offloading	TCP offloading directs traffic in the most efficient manner by analyzing and directing incoming traffic at the request level. TCP offloading breaks the dependency between application requests and the transport layer. It multiplexes and demultiplexes application-level requests onto persistent connections to back-end servers. It keeps client and server TCP connections alive independent of each other and reuses TCP connections, enabling granular application layer policy and offloading TCP processing from web servers, saving CPU cycles.

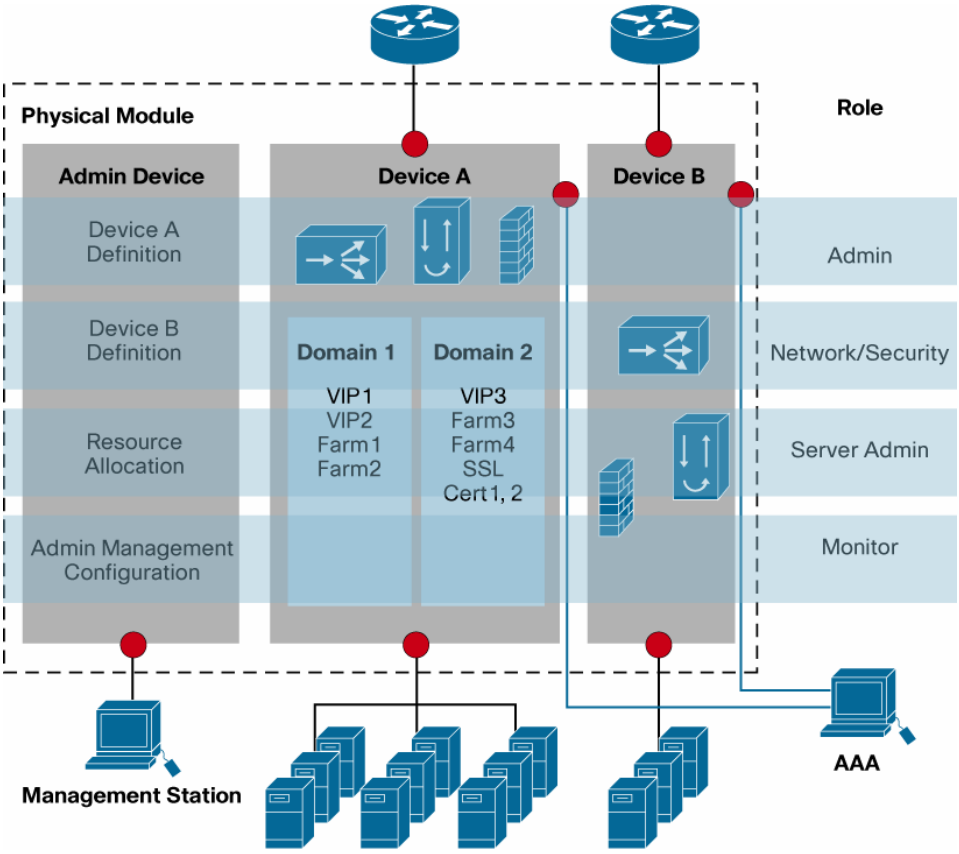
Figure 2. Cisco ACE Network Integration



Features	Benefits
Secure	
Data center security	The Cisco ACE Module is designed to serve as a last line of defense for servers and applications in data centers. The data center security protects against protocol and denial-of-service (DoS) attacks and encrypts mission-critical content. The Cisco ACE data center security capabilities protect the data center and critical applications from malicious traffic with the following features: • HTTP deep packet inspection: HTTP header, URL, and payload • Bidirectional NAT and PAT • Support for static, dynamic, and policy-based NAT and PAT. • Access control lists (ACLs) to selectively allow traffic between ports • TCP connection state tracking • Virtual connection state for UDP • Sequence number randomization • TCP header validation • TCP window-size checking • Unicast Reverse Path Forwarding (URPF) checking at session establishment • ACL object grouping • TCP SYN cookies, providing distributed DoS (DDoS) protection. • Rate limiting: Cisco ACE rate limiting capabilities can be applied to a set of real servers, virtual servers, or both.
Application security	Integrated hardware-accelerated protocol control offers efficient inspection and filtering of popular data center protocols such as HTTP, RTSP, DNS, FTP, ICMP, SIP, Skinny Client Control Protocol (SCCP), and LDAP.
Virtualized Services	
Virtual devices	Virtual devices provide a way to create resource segmentation and isolation, allowing the Cisco ACE Module to act as if it were several individual virtual modules within a single physical module. Virtual devices enable organizations to provide defined levels of services to up to 250 different business organizations, applications, or customers and partners from a single Cisco ACE Module. • Virtual devices offer complete separation of the following: ◦ Configuration files ◦ Management interfaces ◦ Application rule sets • Virtual devices provide customized, specifically allocated resources per application for the following: ◦ Throughput ◦ Connections per second You can limit and manage the allocation of the following Cisco ACE resources: ACL memory, buffers for syslog messages and TCP out-of-order (OOO) segments, concurrent connections (traffic through the Cisco ACE), management connections (traffic to the Cisco ACE), proxy connections, resource limit (set as a rate per second), regular-expression memory, SSL connections, sticky entries, and static or dynamic NATs (Xlates).

Features	Benefits
Role-based administration (RBA)	The RBA feature allows organizations to specify administrative roles and restrict administrators to specific functions within the module or virtual devices (Figure 3). Because multiple administrators within an organization may want to interact with the Cisco ACE Module at different levels (application administration, server administration, network administration, security administration, etc.), it is important to be able to define these administrator roles, allowing each administrator group to freely perform its tasks while not affecting the other groups. This enables secure delegation of tasks to each group. Cisco ACE provides the following predefined roles that you cannot delete or modify: • Admin: This role gives a user complete access to and control over all the objects in virtual devices. A context administrator can create, configure, and modify any object in that context, including policies, roles, domains, server farms, and real servers. • Network Admin: This role provides complete access to and control over the following features: interfaces, routing, connection parameters, NAT, virtual IP copy configurations, and the **change to** command. • Network-Monitor: This role provides access only to all **show** commands and the **change to** command. If you do not explicitly assign a role to a user with the **username** command, this is the default role. • Security-Admin: This role has complete access to and control over the following security-related features within a context: ACLs; application inspection; connection parameters; interfaces; authentication, authorization, and accounting (AAA); NAT; copy configurations; and the **change to** command. • Server-Appln-Maintenance: This role has complete access to and control over the following features: real servers, server farms, load balancing, copy configurations, and the **change to** command. • Server-Maintenance: This role has access to real-server maintenance, monitoring, and debugging: ◦ Real servers: Modify permission ◦ Server farms: Debug permission ◦ Virtual IPs: Debug permission ◦ Probes: Debug permission ◦ Load balancing: Debug permission ◦ **Change to** command: Create permission • SLB-Admin: This role has complete access to and control over the following Cisco ACE features within a context: real servers, server farms, virtual IPs, probes, load balancing (Layers 3, 4, and 7), NAT, interfaces, copy configurations, and the **change to** command. • SSL-Admin: This role is the administrator for all SSL features: • SSL: Create permission • Public key infrastructure (PKI): Create permission • Interfaces: Modify permission • Copy configurations: Create permission • **Change to** command: Create permission • **Secure Backup** and **Restore** commands, in both admin and user contexts • Third-party management tool support with SNMP MIBs In addition to the preceding default roles, new roles can be created to adapt to different organization structures.

Figure 3. Cisco ACE Virtual Devices and Role-Based Administration



Features	Benefits
Deployment and Management	
Layer 2 to 7 network integration	• As a module for the Cisco Catalyst 6500 Series and Cisco 7600 Series chassis, the Cisco ACE fits easily into any new or existing network to provide a full and rich solution for Layers 2 to 7. ◦ With support for up to 1152 ports and chassis throughput of up to 720 Gbps, the solution easily scales to the requirements of the largest networks, and the integrated solution provides a much-reduced solution footprint. Application and data center high availability is supported by RHI and autostate integration, whereby a Cisco ACE virtual device failover can be forced by physical interfaces in the network going in or out of service. ◦ Dynamic Layer 3 routing virtualization is supported by integration with virtual routing and forwarding (VRF) instances on the multiswitch feature card (MSFC) in the Cisco Catalyst 6500 Series and Cisco 7600 Series. ◦ Secondary IP address support is provided on the VLAN interface.
Function consolidation	• By consolidating the functions of application switching, SSL acceleration, data center security, and more on one device, Cisco ACE achieves significant increases in processing rate, from bits per second (bps) to packets per second (pps), while reducing application latency. With consolidation of functions, a TCP flow is terminated only once instead of at four or more places across the network, saving time, processing power, and memory. • The encryption and decryption, load-balancing decision, security check, and business-policy assignment and validation are all performed at a single point in the network to achieve better application performance and with fewer devices, simpler network designs, and easier management.
Investment protection	• By default, Cisco ACE supports virtualization with one administrative device and five user devices, 4-Gbps module bandwidth, 1000 SSL transactions per second (TPS), and a free promotional security license. • Software license upgrades allow the network to scale without the need for major reinvestment in new equipment: ◦ Throughput: The default module bandwidth of 4 Gbps can be increased to 8 or 16 Gbps on the same module. Bandwidth can be scaled by placing up to four Cisco ACE Modules in a single Cisco Catalyst 6500 Series or Cisco 7600 Series chassis. ◦ Virtual devices: The number of default user devices can be increased from 5 to 20, 50, 100, or 250 virtual devices, through software license upgrades. ◦ SSL TPS: You can increase the number of default 1000 SSL TPS to 5000, 10,000, or 15,000, through software license upgrades. • The Cisco ACE Module also provides two field-upgradeable daughter-card slots, so that the Cisco ACE Module can accommodate future functions and additional scalability, providing long platform life. This flexibility helps ensure that the Cisco ACE Module can grow with an enterprise's requirements for years to come without requiring a full module upgrade and with little or no business disruption.

Features	Benefits
Cisco Application Networking Manager (ANM)	Cisco ANM supports management of virtual devices and hierarchical management domains across multiple Cisco ACE Modules. • This server-based management suite discovers, provisions, and monitors all the virtual devices on multiple Cisco ACE Modules, making deployment completely transparent. • Forms-based configuration complements service activation and suspension capabilities to enable quick implementation of applications. • Configurable role-based access control (RBAC) delegation of tasks allows concurrent operation by multiple administrator groups across many Cisco ACE Modules and virtual devices.

Improved IT Efficiency and Lower TCO

By consolidating application services such as server load balancing, data center security, and SSL acceleration on one device, Cisco ACE improves IT efficiency and lowers your TCO. With the consolidation of crucial application services, a TCP flow is terminated only once instead of at four or more places across the network, saving time, processing power, and memory.

The encryption and decryption, load-balancing decision, data center security, and business-policy assignments and validations are all performed at a single point in the network to achieve better application performance and with fewer devices, stronger security with fewer elements, simpler network designs, and easier management. The Cisco ACE Module is an ideal replacement for traditional point data center solutions, improving IT efficiency and lowering TCO by eliminating multivendor power, space, training, management, troubleshooting, and support contract requirements.

Specifications

Table 2 summarizes the Cisco ACE performance and configuration, and Table 3 summarizes the Cisco ACE specifications.

Table 2. Cisco ACE Module Performance and Configuration

Feature	Maximum Performance and Configuration
Global Parameters	
Throughput	16 Gbps*, 8 Gbps*, and 4 Gbps
Syslogs per second	350,000
Global Configuration	
Total VLANs (client and server)	4000
Probes	ICMP, TCP, UDP, Echo, Finger, DNS, Telnet, FTP, HTTP, HTTPS, SMTP, POP3, IMAP, RTSP, RADIUS, SIP, SNMP, KAL-AP, and TCL Scripts
NAT entries	1 million
Virtual partitions	Up to 250*; 5 virtual partitions (devices) included in base price
SSL Performance	
SSL throughput	3.3 Gbps
SSL TPS	1000 TPS included in base price, and 5000, 10,000, or 15,000 TPS with licensing
Application Switching Performance	
Maximum connections per second	325,000 complete transactions sustained rate
Concurrent connections	4 million
Sticky table entries	4 million

* Requires purchase of an upgrade license

Table 3. Cisco ACE Module Specifications

Feature	Description
Physical Specifications	
Chassis slots required	Occupies 1 slot in the chassis
Dimensions (H x W x D)	1.75 x 15.51 x 16.34 in. (44.45 x 394 x 415 mm)
Weight	11 lb (4.98 kg)
Operating Specifications	
Ambient operating temperature	32 to 104°F (0 to 40°C)
Ambient nonoperating temperature	–40 to 158°F (–40 to 70°C)
Operating relative humidity	10 to 85%
Nonoperating relative humidity	5 to 95%
Operating Altitude	
Certified for operation	0 to 6500 ft (0 to 2000 m)
Designed and tested for operation	–200 to 10000 ft (–60 to 3000 m)
NEBS	• SR-3580-NEBS: Criteria Levels (Level 3 compliant) • GR-63-CORE-NEBS: Physical Protection • GR-1089-CORE-NEBS: EMC and Safety
Emissions	• FCC Part 15 (CFR 47) Class A or B • ICES-003 Class A or B • EN55022 Class A or B • CISPR22 Class A or B • AS/NZS CISPR22 Class A or B • VCCI Class A or B • CISPR24 • EN55024 • EN50082-1 • EN61000-3-2 • EN61000-3-3 • EN61000-6-1
Safety	• UL 60950 • Can/CSA-C22.2 No. 60950 • EN 60950 • IEC 60950 • AS/NZS 60950 TS001

System Requirements

Table 4. Cisco Catalyst 6500 Series and Cisco 7600 Series System Requirements for the Cisco ACE Module

Requirement	Details
Chassis	All Cisco Catalyst 6500 Series and Cisco 7600 Series chassis
Supervisor engines	• Cisco Catalyst 6500 Series Supervisor Engine 720 and Supervisor Engine 720-10GE • Cisco 7600 Series Supervisor Engine 720 and Route Switch Processor 720
Chassis OS	• Cisco Catalyst 6500 Series running Cisco IOS® Software Release 12.2(18)SXF4 or later for Supervisor Engine 720, and 12.2(33)SXH or later for Supervisor Engine 720-10GE • Cisco 7600 Series running Cisco IOS Software Release 12.2(18)SXF4 or later and 12.2(33)SRB or later for Supervisor Engine 720, and 12.2(33)SRC or later for Route Switch Processor 720
Chassis connectivity	Functions as a fabric-enabled line card
Chassis slots required	Occupies 1 slot in the chassis

For More Information

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

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Printed in USA C78-458838-00 07/10