

Cisco Application Control Engine Module

The Cisco® Application Control Engine (ACE) family for the Cisco Catalyst® 6500 delivers the highest level of application infrastructure control, application performance, application security and infrastructure simplification.

The Cisco ACE family provides application and network operations management with new levels of control over the way they deploy, operate, deliver, secure and manage their applications and business services across the extended enterprise (Figure 1). The Cisco ACE helps enable greater control over the application infrastructure, allowing organizations to quickly deploy and migrate applications, delivering the highest levels of services to the end user while simplifying the overall management and operation of a data center. By combining the highest application performance with application security and infrastructure simplification, the Cisco ACE solution helps organizations reduce overall operating expenses (OpEx) and capital expenditures (CapEx).

Figure 1. Cisco ACE Module



The Cisco ACE provides the following features, functions and benefits:

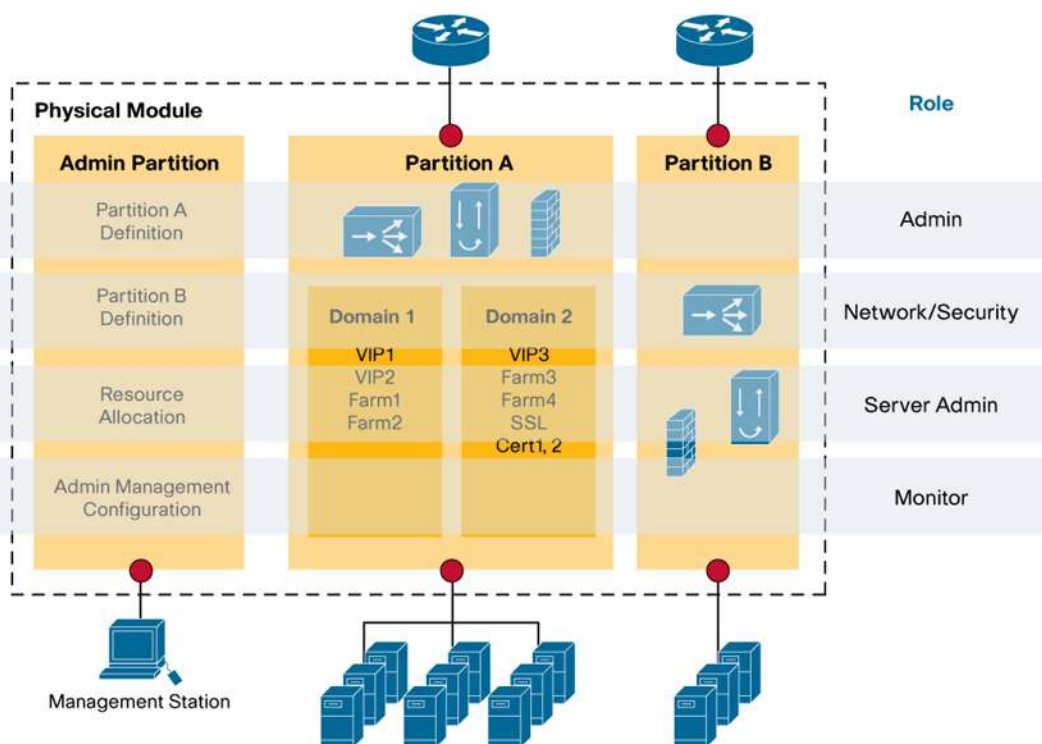
- **Application infrastructure control**—Virtual partitioning provides a way to create resource segmentation and isolation, allowing the Cisco ACE to act like it is several individual virtual modules within a single physical module. With this solution, organizations can provide a defined level of service to up to 250 different business organizations, applications, or customers and partners from a single Cisco ACE module. Virtual partitions adapt the application infrastructure to business operations with fewer devices and superior control.

Moreover, each virtual partition includes hierarchical management domains, helping ensure guaranteed performance levels of applications while maximizing use of available resources in the ACE module.

The Cisco ACE offers centralized control with decentralized management using template-based or customizable user permissions for each virtual partition. The Role-Based Access Control (RBAC) feature allows organizations to specify administrative roles and restrict administrators to specific functions within the module or virtual partitions. Because multiple administrators within an organization may want to interact with the Cisco ACE module at different levels (for example, 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.

With application infrastructure control, The Cisco ACE vastly improves overall workflow and empowers you to provide rapid response to application demands. (Figure 2).

Figure 2. Cisco ACE Virtual Partitioning and RBAC



- **Application performance**—The Cisco ACE provides the highest level of application delivery in the industry. With up to 16 Gbps of throughput capacity and 345,000 sustained connections per second per ACE module, the Cisco ACE is ready to handle large data files, rich-media applications and a large user base with ease. The ACE family of modules offers up to 16 Gbps of scalable throughput with pay-as-you-grow licensing and no need for a complete system upgrade to add additional capacity. The ACE is architected for add-on services and scalability extensions in the future. In fact, with up to four modules in a single Cisco Catalyst 6500 chassis, the ACE offers the highest scalability in the industry.

The Cisco ACE also offers multitiered redundancy, availability and scalability for maximum protection for your critical business. It is the only product in the industry that offers three types of high availability:

- **Inter-chassis:** An ACE in one Cisco Catalyst 6500 is protected by an ACE in a peer Cisco Catalyst 6500.
- **Intra-chassis:** An ACE in a Cisco Catalyst 6500 is protected by another ACE in the same Cisco Catalyst 6500 (the Cisco Catalyst 6500 has solid redundancy built in).
- **Inter-partition:** Cisco ACE supports high availability between virtual partitions configured across two modules to allow specific partitions to fail over without affecting the other partitions and applications on a given module

All these availability modes provide rapid, stateful application redundancy with replication of connection state and sticky tables.

- **Application security**—The Cisco Self-Defending Network promises customers peace of mind by offering defense at multiple levels. The Cisco ACE in conjunction with the Cisco AVS 3100 Series Application Velocity System provides the richest solution for application security.

The Cisco ACE protects the data center and critical applications from malicious traffic with the following features:

- HTTP deep packet inspection—HTTP header, URL, and payload
- Bidirectional Network Address Translation (NAT) and Port Address Translation (PAT)
- Support for static, dynamic and policy-based NAT/PAT
- Access control lists (ACLs) to selectively allow traffic between ports
- TCP connection state tracking
- Virtual connection state for User Datagram Protocol (UDP)
- Sequence number randomization
- TCP header validation
- TCP window size checking
- Unicast Reverse Path Forwarding (URPF) checking at session establishment

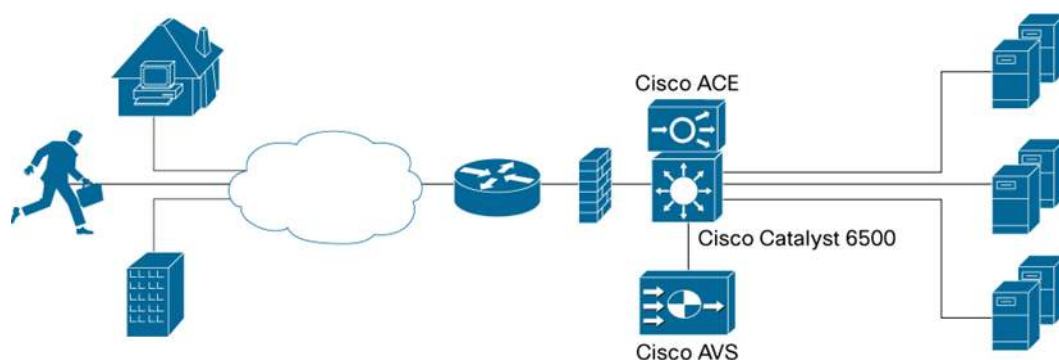
Integrated hardware-accelerated protocol control—a first in the application delivery space—offers efficient inspection, filtering, and fix-up of popular data center protocols such as HTTP, Real-Time Streaming Protocol (RTSP), Domain Name System (DNS), FTP, and Internet Control Message Protocol (ICMP).

Large, scaleable ACLs with up to 256,000 elements permit both front-end scalability (number of users/client applications) and back-end scalability (number of servers/server farms) the applications are destined to. Similarly, high performance and scalable NAT transactions with up to 1,000,000 entries allow consolidation of many large data centers and faster application roll-out. Again, virtual partitions help keep all overlapping IP subnets separate, without a need for costly network redesigns, reconfigurations, or additional devices to protect your data center.

The Cisco ACE also supports checks for protocol compliance, as well as transaction logging and reporting for security forensics.

- **Infrastructure simplification**—Layer 2 to 7 network integration—As a module for the Cisco Catalyst 6500 chassis, the Cisco ACE fits easily into any new or existing network to provide a full and rich solution for Layers 2 to 7 (Figure 3). 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 Route Health Injection (RHI) and auto-state integration, where an ACE virtual partition failover can be forced by physical interfaces in the network going up or down. Dynamic Layer 3 routing virtualization is supported by integration with virtual route forwarding (VRF) instances on the multiswitch feature card (MSFC) in the Cisco Catalyst 6500.

Figure 3. Cisco Application Control Engine Network Integration



- **Functional consolidation**—By consolidating the functions of content switching, Secure Sockets Layer (SSL) acceleration, data center security and more on one device, the Cisco ACE derives significant multipliers from bps to 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, in turn saving time, processing power, and memory. The encryption and decryption, load-balancing decision, security check, and business policy assignments and validations are all done at a single point in the network to achieve better application performance and with fewer devices, simpler network designs, and easier management.
- **Cisco Application Networking Manager (ANM)**—The Cisco ANM supports the management of virtual partitions and hierarchical management domains across multiple ACE modules. This server-based management suite discovers, provisions, monitors and reports across many virtual partitions on multiple ACE modules, making deployment completely transparent. Template-based configuration and auditing complement service activation/suspension capabilities to enable quick implementation of applications. Configurable RBAC delegation of tasks with a matching service API allows concurrent operation by multiple administrator groups across many ACE modules and virtual partitions. Expected availability Q3CY06.
- **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 deeper into encrypted data and apply security and content switching policies. This setup not only allows the Cisco ACE to make more intelligent policy decisions but also helps ensure your application-delivery platform adheres to internal and external regulatory compliance. With re-encryption capabilities, the Cisco ACE solution helps ensure end-to-end encryption of sensitive data while still providing the ability to apply intelligent policies.
- **Transaction visibility**—With the ability to deliver industry-leading syslog rates up to 350,000 per second, the Cisco ACE solution makes it possible to log a large number of connection setups and tear-downs, providing transaction-level visibility, without affecting data traffic performance.
- **Future-proof solution**—With two field-upgradable daughter-card slots, the Cisco ACE module can accommodate future functions and additional scalability. This flexibility assures that the Cisco ACE solution can grow with requirements for years to come without requiring a full module upgrade and with little or no business disruption.

Table 1. Cisco ACE Maximum Performance and Configuration Summary

Feature	Maximum Performance/Configuration
Global Parameters	
Throughput	16 Gbps ¹ , 8 Gbps ¹ and 4 Gbps
Packets per Second	6.5 million
Syslogs per Second	350,000
Global Configuration	
Total VLANs (Client/Server)	4000
Probes	4000 ICMP, TCP, UDP, Echo, Finger, DNS, Telnet, FTP, HTTP, HTTPS, SMTP, POP3, IMAP, RADIUS, and Scripted
ACL Items	Up to 256,000 access control elements
NAT Entries	1 million
Virtual Partitions	250 ¹ , 5 virtual partitions included in base price
SSL Performance	
SSL Throughput	4 Gbps
SSL TPS	1000 TPS included in base price and 5000 TPS, 10,000 TPS or 15,000 TPS with licensing
Content Switching Performance	
Maximum Connections per Second	348,000 complete transactions sustained rate
Concurrent Connections	4 million
Content Switching Configuration	
Virtual Servers	4,096
Server Farms	16,000
Real Servers	16,000
Sticky Table Entries	4 million

Table 2. 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)
Operational Specifications	
Ambient Operating Temperature	0 to 40°C (32 to 104°F)
Ambient Nonoperating Temperature	-40 to 70°C (-40 to 158°F)
Operating Relative Humidity	10 to 85%
Nonoperating Relative Humidity	5 to 95%
Operating Altitude	
Certified for Operation	0 to 2000 m (0 to 6500 ft)
Designed and Tested for Operation	-60 to 3000 m (-200 to 10000 ft)

¹ Requires purchase of an upgrade license

Feature	Description
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

Table 3. Cisco Catalyst 6500 Series Switch Requirements

Requirement	Details
Chassis	All Cisco Catalyst 6500 chassis
Supervisor Engines	Cisco Catalyst 6500 Series Supervisor Engine 720, 720-3B, and 720-3BXL
Chassis OS	Switches running Cisco IOS® Software
Chassis Connectivity	Functions as a fabric-enabled line card
Chassis Slots Required	Occupies 1 slot in the chassis

Table 4. Product Part Numbers

Product Description	Part Number
Cisco ACE Service Module—Includes 1000 SSL TPS and 5 Virtual Partitions	ACE10-6500-K9
Cisco ACE 4-Gbps Throughput License	ACE-04G-LIC
Cisco ACE 8-Gbps Throughput License	ACE-08G-LIC
Cisco ACE Upgrade License from 4 Gbps to 8 Gbps	ACE-UPG1-LIC=
Cisco ACE 5,000 SSL Transactions per Second License	ACE-SSL-05K-K9
Cisco ACE 10,000 SSL Transactions per Second License	ACE-SSL-10K-K9
Cisco ACE 15,000 SSL Transactions per Second License	ACE-SSL-15K-K9
Cisco ACE Upgrade license from 5,000 to 10,000 SSL Transactions per Second License	ACE-SSL-UP1-K9=
Cisco ACE Upgrade license from 10,000 to 15,000 SSL Transactions per Second License	ACE-SSL-UP2-K9=
Cisco ACE 20 Virtual Contexts License	ACE-VIRT-020
Cisco ACE 50 Virtual Contexts License	ACE-VIRT-050
Cisco ACE 100 Virtual Contexts License	ACE-VIRT-100
Cisco ACE 250 Virtual Contexts License	ACE-VIRT-250
Cisco ACE Upgrade License from 20 to 50 Virtual Contexts	ACE-VIRT-UP1
Cisco ACE Upgrade License from 50 to 100 Virtual Contexts	ACE-VIRT-UP2
Cisco ACE Upgrade License from 100 to 250 Virtual Contexts	ACE-VIRT-UP3
Cisco ACE Security Feature Set License	ACE-SEC-LIC-K9
Cisco ACE 6504 Bundle with 4Gbps Throughput License	WS-C6504-E-ACE-K9 ²
Cisco ACE 6509 Bundle with 8Gbps Throughput License	WS-C6509-E-ACE-K9 ²

² Cisco ACE bundles do not include I/O modules so that the customer can order the module of their choice.



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: 408 527-0688

Asia Pacific Headquarters
 Cisco Systems, Inc.
 16B Robinson Road
 #29-01 Capital Tower
 Singapore 068912
www.cisco.com
 Tel: +65 6317 7777
 Fax: +65 6317 7768

Europe Headquarters
 Cisco Systems International BV
 Heesterbergpark
 Heesterbergweg 13-19
 1101 CH Amsterdam
 The Netherlands
www-europe.cisco.com
 Tel: +31 0 20 620 0791
 Fax: +31 0 20 557 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.

©2007 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 Intranet 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, IPona, IPTV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, Packet, PIX, ProConnect, RateMUX, ScriptShare, SliceCast, SMARTnet, StackWise, The Festos, 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. (8761R)