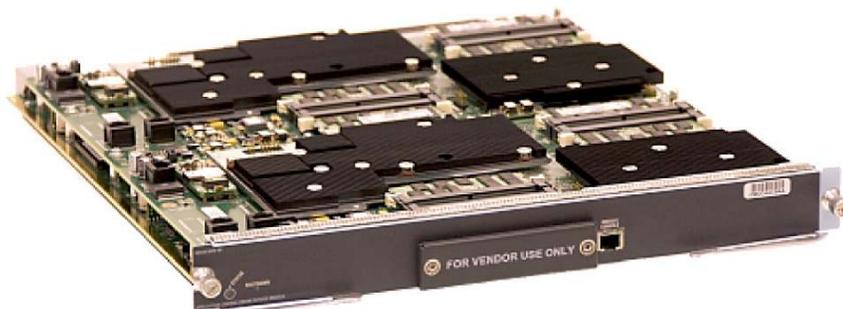


Cisco ACE30 Application Control Engine Module

Product Overview

The Cisco® ACE30 Application Control Engine Module (Figure 1) belongs to the Cisco ACE family of application switches, which deliver availability, security, and consolidation of data center applications. The Cisco ACE product family consists of the Cisco ACE30 Module for the Cisco Catalyst® 6500 Series Switches and the Cisco 7600 Series Routers, Cisco ACE 4710 Appliance, Cisco Global Site Selector (GSS) Appliance, and Cisco Application Networking Manager (ANM) management software.

Figure 1. Cisco ACE30 Module



The Cisco ACE30 allows enterprises to accomplish these important IT objectives for application delivery:

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

The Cisco ACE30 achieves these goals through a broad set of intelligent Layer 4 load-balancing and Layer 7 content-switching technologies that work with IPv4 and IPv6 traffic and are integrated with the latest virtualization and security capabilities. It supports translation between IPv4 and IPv6 traffic, enabling migration to IPv6 and allowing deployments in mixed networks.

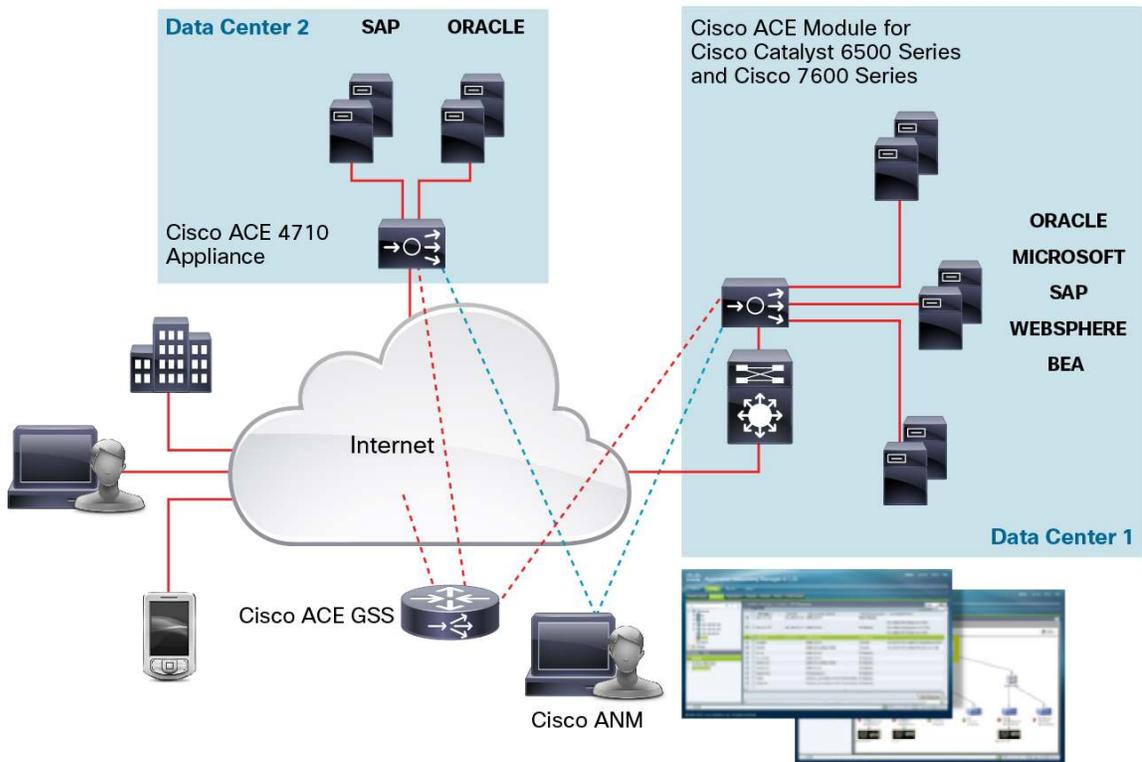
The Cisco ACE30 provides flexibility in managing application traffic, scaling up to 16 Gbps in a single-slot module form factor, upgradeable through software licenses, thus providing IT with long-term investment protection and scalability.

Additionally, through virtualization and role-based access control (RBAC) capabilities, the Cisco ACE30 enables IT to provision and deliver a broad range of applications from a single Cisco ACE module, bringing increased scalability for application provisioning to the data center. This capability helps streamline and reduce the cost of operations involved in implementing, scaling, accelerating, and protecting applications.

The Cisco ACE30 greatly improves server efficiency through highly flexible application traffic management and the offloading of CPU-intensive tasks such as SSL encryption and decryption processing, HTTP compression, and TCP session management.

The Cisco ACE platform is designed to serve as a last line of defense for servers and applications in data centers. An integrated firewall enables IT professionals to comprehensively secure high-value applications in the data center and facilitates data center consolidation (Figure 2).

Figure 2. Cisco ACE Network Integration



By combining high application performance with a comprehensive set of state-of-the-art application delivery features, the Cisco ACE30 promotes greater IT efficiency and reduces the total cost of ownership (TCO).

Features and Benefits

Table 1 summarizes the features and benefits of the Cisco ACE30.

Table 1. Features and Benefits

Feature	Benefit
Availability	
Application switching	<p>The Cisco ACE30 provides load-balancing and content-switching functions with granular traffic control based on customizable Layer 4 through 7 rules with support for both IPv4 and IPv6 addresses, VIPs, and server farms.</p> <p>Cisco ACE can natively load-balance the following protocols in an IPv4 environment: HTTP/HTTPS, FTP, Domain Name System (DNS), Internet Control Message Protocol (ICMP), Session Initiation Protocol (SIP), Real-Time Streaming Protocol (RTSP), Extended RTSP, Lightweight Directory Access Protocol (LDAP), RADIUS, Skinny Client Control Protocol (SCCP) and Microsoft Remote Desktop Protocol (RDP). In an IPv6 environment, it can natively load-balance HTTP, HTTPS, and SSL protocols. It has generic protocol parsing capabilities that enable the configuration of application switching and persistence policies based on any information in the traffic payload for custom and packaged applications without requiring any programming.</p> <p>The Cisco ACE30 supports translation and load balancing between IPv4 and IPv6 networks and provides flexibility to customers in planning their IPv6 migrations.</p>

Feature	Benefit
Predictors	Predictors or load-balancing algorithms enable the Cisco ACE30 to select the best server to satisfy a client request.
Persistence and stickiness	Stickiness 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.
Redundancy	Stateful failover capabilities help ensure resilient network protection for enterprise network environments. The Cisco ACE30 integrates with Cisco GSS to provide a multiple data center scaling and failover system.
Server health monitoring	The Cisco ACE30 checks the health of application servers and server farms through configuration of health probes.
Performance	
Compression	The Cisco ACE30 delivers up to 6-Gbps hardware-accelerated data compression and provides fast application performance for application users.
SSL acceleration	The Cisco ACE30 integrates SSL acceleration technology, which offloads the encryption and decryption of SSL traffic from external devices (servers, appliances, etc.), thereby allowing Cisco ACE to look more deeply into encrypted data and apply security and application switching policies and help ensure compliance with internal and external regulations.
TCP offload	The Cisco ACE30 directs website traffic in the most efficient manner by analyzing and directing incoming traffic at the request level. These capabilities enable highly specific application-layer policy and offload TCP processing from the web servers, saving CPU cycles.
Security	
Data center security	The Cisco ACE30 protects the data center and critical applications from protocol and denial-of-service (DoS) attacks and encrypts mission-critical content.
Application security	The Cisco ACE30 provides deep protocol inspection capabilities, which enables IT professionals to comprehensively secure high-value applications in the data center. It secures mission-critical applications and protects against identity theft, data theft, application disruption, and fraud and defends web-based applications and transactions against targeted attacks by professional hackers.
Virtualized Services	
Virtual contexts	Virtual contexts provide a means for creating resource segmentation and isolation, allowing the Cisco ACE30 to act as if it were several individual virtual appliances within a single physical appliance. Virtual contexts enable organizations to provide defined levels of service to up to 250 business departments, applications, or customers and partners from a single Cisco ACE appliance.
Role-based access control (RBAC)	RBAC allows organizations to specify administrative roles and restrict administrators to specific functions within the appliance or virtual contexts, allowing each administrator group to freely perform its tasks without affecting the other groups.
Deployment and Management	
Function consolidation	Through consolidation of application switching, SSL acceleration, data center security, and other functions on one device, the Cisco ACE30 helps achieve better application performance, with fewer devices, simpler network designs, and easier management.
Investment protection	By default, the Cisco ACE30 supports virtualization with one administrator context and 250 user contexts, 30,000 SSL transactions per second (TPS), and up to 6 Gbps of compression. The default throughput can be increased to up to 16 Gbps without the need for new equipment, through software license upgrades.
Cisco ANM	Cisco ANM supports the management of virtual contexts and hierarchical management domains across multiple Cisco ACE30 modules. This server-based management suite discovers, provisions, monitors, and reports across many virtual contexts on multiple Cisco ACE30 Modules, making deployment transparent.

Product Specifications

Table 2 presents the performance specifications for the Cisco ACE30.

Table 2. Product Performance Specifications

Feature	Maximum Performance and Configuration
Throughput	4, 8, or 16 Gbps
Compression throughput	4 or 6 Gbps (using GZIP or Deflate)
Virtual contexts	250
SSL throughput	6 Gbps
SSL TPS	Up to 30,000 TPS using 1024-bit keys

Feature	Maximum Performance and Configuration
Maximum number of Layer 4 connections per second	500,000 complete transactions sustained rate
Maximum number of Layer 7 connections per second	200,000 complete transactions sustained rate
Concurrent connections	4 million

Table 3 presents the product specifications for the Cisco ACE30.

Table 3. Product 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 2000m)
Designed and tested for operation	-200 to 10000 ft (-60 to 3000m)
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 lists system requirements for the Cisco Catalyst 6500 Series Switches used with the Cisco ACE30, and Table 5 lists requirements for the Cisco 7600 Series Routers.

Table 4. Cisco Catalyst 6500 Series System Requirements for the Cisco ACE30 Module

Requirement	Details
Chassis	Cisco Catalyst 6503E, 6504E, 6506E, 6509E, 6509-V-E, 6513, or 6513E Switch
Supervisor engine	Cisco Catalyst Sup720-3B, Sup720-3BXL, Sup720-10G-3C, Sup720-10G-3CXL, Sup2T-10G, or Sup2T-10G-XL
Chassis OS	Cisco Catalyst 6500 Series running Cisco IOS® Software Release 12.2(33)SX14 (or later depending on supervisor)
Chassis connectivity	Functions as a fabric-enabled line card
Chassis slots required	Occupies 1 slot in the chassis

Table 5. Cisco 7600 Series System Requirements for the Cisco ACE30 Module

Requirement	Details
Chassis	Cisco 7603, 7604, 7609, 7613, 7603-S, 7604-S, 7606-S, or 7609-S Router
Supervisor engine	Cisco Catalyst Sup720-3B, Sup720-3BXL, RSP720-3C-GE, RSP720-3CXL-GE, RSP720-3C-10GE, or RSP720-3CXL-10GE
Chassis OS	Cisco 7600 Series running Cisco IOS Software Release 15.0(1)S (or later)
Chassis connectivity	Functions as a fabric-enabled line card
Chassis slots required	Occupies 1 slot in the chassis

Ordering Information

Table 6 lists part numbers for ordering the Cisco ACE30 Module.

Table 6. Ordering Information

Product Number	Product Description
ACE30-MOD-K9=	Application Control Engine 30 Hardware
SC6K-A41-ACE	ACE A4(1) SW for ACE30 Module
SC6K-A51-ACE	ACE SW (5.1) for ACE30 Module
ACE30-BASE-04-K9	ACE30 Module with 4G, 1G Comp, 1K SSL TPS and 5VC
ACE30-MOD-04-K9	ACE30 Module with 4G, 4G Comp, 30K SSL TPS and 250VC
ACE30-MOD-08-K9	ACE30 Module with 8G, 6G Comp, 30K SSL TPS and 250VC
ACE30-MOD-16-K9	ACE30 Module with 16G, 6G Comp, 30K SSL TPS and 250VC

Additional Information

For more information about the Cisco ACE product family, please visit the following sites or contact your local account representative:

- Cisco ACE Modules: <http://www.cisco.com/go/ace>
- Cisco ACE 4710 Appliance: <http://www.cisco.com/go/ace>
- Cisco GSS Appliance: <http://www.cisco.com/go/gss>
- Cisco ANM management software: <http://www.cisco.com/go/anm>



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

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.

 Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third party trademarks mentioned 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. (1110R)