Cisco ACE 4710 Application Control Engine

Product Overview

The Cisco® ACE 4710 Application Control Engine (Figure 1) represents the next generation of application switches for increasing the availability, acceleration, and security of data center applications.

Figure 1. Cisco ACE 4710 Appliance

The Cisco ACE 4710 allows enterprises to accomplish four primary IT objectives for application delivery:

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

The Cisco ACE 4710 achieves these goals through a broad set of intelligent Layer 4 load-balancing and Layer 7 content-switching technologies integrated with the latest virtualization and security capabilities. The Cisco ACE 4710, through is its use of virtualized architecture and role-based administration, helps streamline and reduce the cost of operations involved in implementing, scaling, accelerating, and protecting applications.

The Cisco ACE 4710 provides scalability and flexibility in managing application traffic, with up to 4 Gbps in a one-rack-unit (1RU) form factor, upgradeable through software licenses, thus providing IT with long-term investment protection and scalability.

To increase application availability, the Cisco ACE 4710 uses best-in-class application switching algorithms coupled with highly available system software and hardware.

Additionally, through its innovative virtualization and role-based access control (RBAC) capabilities, the Cisco ACE 4710 enables IT to provision and deliver a broad range of applications from a single Cisco ACE appliance, bringing increased scalability for application provisioning to the data center.

The Cisco ACE 4710 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. The Cisco ACE appliance performs deep packet inspection and blocks malicious attacks. An integrated firewall enables IT professionals to comprehensively secure high-value applications in the data center and facilitates consolidation in the data center (Figure 2).

Figure 2.   Cisco ACE Network Integration
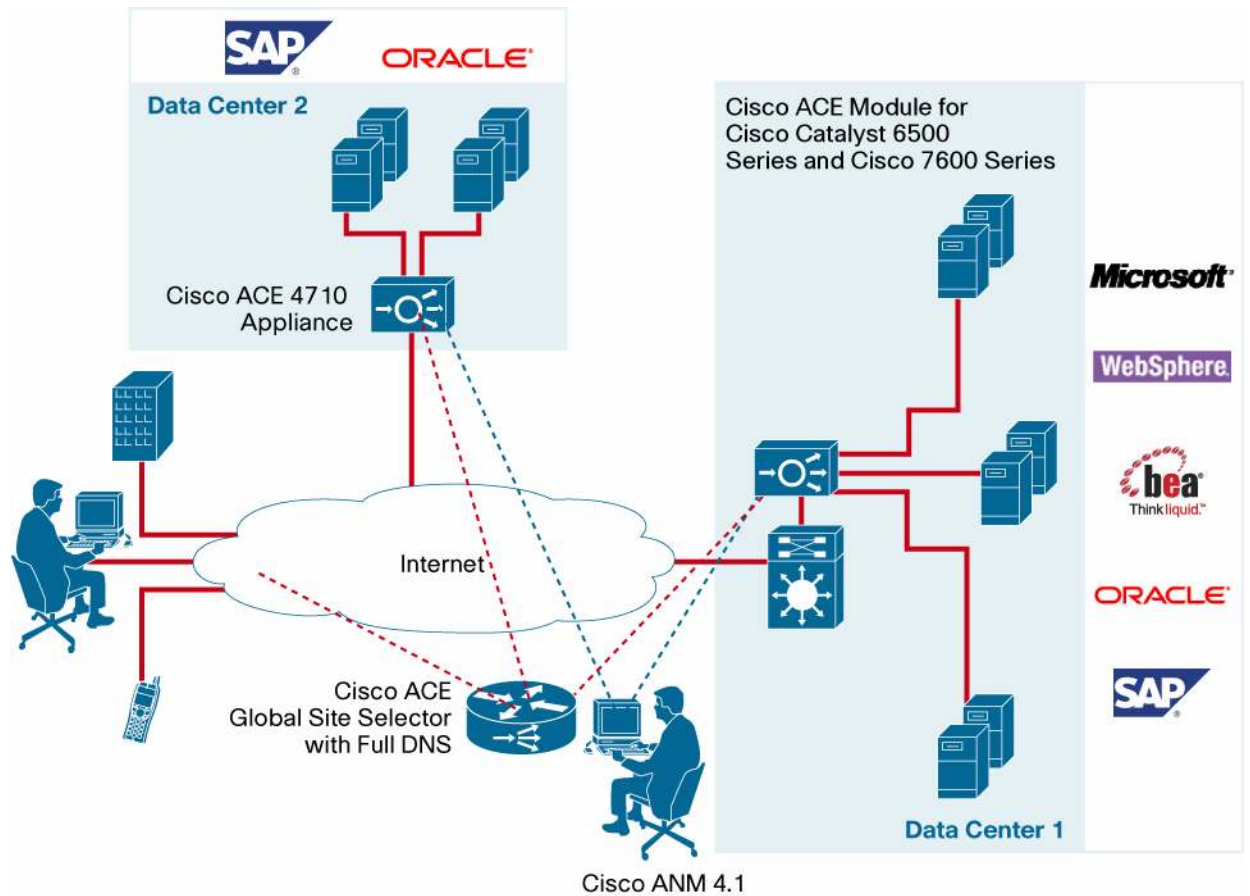
By combining high application performance with a comprehensive set of state-of-the-art application delivery features, the Cisco ACE 4710 promotes greater IT efficiency and reduces the total cost of ownership (TCO).

Features and Benefits

Table 1 summarizes the features and benefits of the Cisco ACE 4710.

Table 1. Features and Benefits

| Feature	Benefit
Availability	
Application Switching	The Cisco ACE 4710 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).
	• The Cisco ACE GPP feature enables you to configure application switching and persistence policies based on any information in the traffic payload for custom and packaged applications without requiring any programming.
	• The Cisco ACE performs payload parsing through hardware using a powerful regular expression (regexp) engine to obtain optimal 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 for enhanced troubleshooting.
	• **Source network address translation (NAT) for virtual IP:** Source NAT for virtual IP allows users to include a virtual IP address in the NAT pool for dynamic NAT and port address translation (PAT), with the result that real-world IP addresses are saved on the client-side network.
	• **Source NAT for server farm:** Source NAT can be provided on a backup server farm multiple hops away during the failure of a primary server farm, resulting in continuous application availability.
	• **Flexible network deployment:** Cisco ACE 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 according to 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
	• Hash URL
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 GPP for session-level persistence such as for the SSL session ID
Redundancy	• Provides system and session redundancy, with the capability to switch over automatically to a redundant Cisco ACE upon system or network failure; failover happens automatically, with no human intervention
	• Provides stateful failover capabilities to help ensure resilient network protection for enterprise network environments
	• Supports active-standby and active-active redundancy topologies with configuration synchronization
	• Enables businesses to perform software maintenance release upgrades on Cisco ACE and servers without affecting network uptime or connections
	• Allows stateful redundancy to be enabled on a per-virtual-device basis, isolating a failure to its specific virtual device; a failover event in one virtual device does not affect operation of other virtual devices
	• Integrates with the Cisco ACE Global Site Selector (GSS) software to provide a multiple data center failover system

Feature	Benefit
Server Health Monitoring	To instruct Cisco ACE to check the health of servers and server farms, the user can configure health probes (sometimes referred to as keepalives). The following probes are supported: - ICMP - TCP - User Datagram Protocol (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 Application Protocol (KAL-AP) - RTSP - SIP - HTTP return-code parsing - Simple Network Management Protocol (SNMP) probes
Performance	
Compression	Cisco ACE delivers powerful 2-Gbps hardware-accelerated data compression and provides faster application performance for application users. Both GZIP and Deflate compression are supported.
SSL Acceleration	Cisco ACE 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 feature enables 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 SSL acceleration 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 algorithms:** RSA 512-bit, 768-bit, 1024-bit, 1536-bit, and 2048-bit **Digital certificates:** All major digital certificates from certificate authorities, including VeriSign, Entrust, Netscape iPlanet, Microsoft Windows 2000 Certificate Server, Thawte, Equifax, and Genuity - Sample SSL key and certificate pair
TCP Offload	Cisco ACE directs website traffic in the most efficient manner by analyzing and directing incoming traffic at the request level. TCP offload breaks the dependency between application requests and the transport layer. It multiplexes and demultiplexes application-level requests onto persistent connections set up to back-end servers. It keeps client and server TCP connections alive, independent of each other, and reuses TCP connections. These capabilities enable granular application-layer policy and offload TCP processing from the web servers, saving CPU cycles.
Application Latency Reduction	- Dramatically improves the end user application experience by reducing latency and the number of roundtrips required for application access - Eliminates unnecessary browser cache validation requests and provides automatic embedded object version management at the server, resulting in significantly improved application response times for application users
Caching	Caching directly offloads server requests for frequently requested static objects such as images and applets. This feature is fully configurable and enhances overall application performance and transaction throughput. Dynamic caching technology further accelerates enterprise application performance and improves server system scalability by enabling the Cisco ACE to fulfill requests for dynamic content. Using this feature, the offload capabilities begin to offload application servers and even core databases. 1.5 GB of RAM is available for caching. The memory ships standard with every appliance.

Feature	Benefit
Security	
Data Center Security	The Cisco ACE 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 capabilities that can be applied to a set of real servers, virtual servers, or both
Application Security	Multicore CPU-accelerated protocol control offers efficient inspection, filtering, and fixing of popular data center protocols such as HTTP, RTSP, DNS, FTP, ICMP, SIP, Skinny Client Control Protocol (SCCP), and LDAP. Cisco ACE 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 Devices	Virtual devices (Figure 3) provide a means for creating resource segmentation and isolation, allowing the Cisco ACE appliance to act as if it were several individual virtual appliances within a single physical appliance. Virtual devices enable organizations to provide defined levels of service to up to 20 business departments, applications, or customers and partners from a single Cisco ACE appliance. Complete separation of the following is provided: - Configuration files - Management interfaces - Application rule sets Customized, guaranteed resources per application for the following are provided: - Throughput - Connections per second Capability to limit and manage the allocation of the following Cisco ACE resources is provided: - 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 (number per second) - Regexp memory - SSL connections - Sticky entries - Static or dynamic network address translations (xlates)

Feature	Benefit

Role-Based Administration (RBA)	RBA (Figure 3) allows organizations to specify administrative roles and restrict administrators to specific functions within the appliance or virtual devices. Because multiple administrators within an organization may want to interact with the Cisco ACE appliance 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.
	
	Cisco ACE provides the following predefined roles that cannot be deleted or modified:
	
	• **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 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 role is used by default.
	
	• **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.

Deployment and Management	
Function Consolidation	Through consolidation of application switching, SSL acceleration, data center security, and other functions on one device, the Cisco ACE derives significant multipliers, 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 assignments and validations are all performed at a single point in the network to achieve better application performance, with fewer devices, simpler network designs, and easier management.
Investment Protection	By default, the Cisco ACE 4710 supports virtualization with one administrator device and five user devices, 1-Gbps bandwidth, 1000 SSL transactions per second (TPS), and 100 Mbps of compression. The solution can be expanded without the need for new equipment, through the following software license upgrades: • **Throughput:** The default throughput of 1 Gbps can be increased to 2 or 4 Gbps. • **Virtual devices:** The number of virtual devices can be increased from 5 to 20 virtual devices. • **SSL TPS:** The SSL TPS value can be increased from 1000 to 5000 or 7500 TPS. • **Compression:** Compression can be increased to 500 Mbps or 1 or 2 Gbps of throughput. • **Application acceleration:** Application acceleration is a licensable option.
Cisco ACE 4710 Device Manager	The Cisco ACE Device Manager, which resides in flash memory on the Cisco ACE appliance, provides a browser-based interface for configuring and managing the Cisco ACE appliance. Its intuitive interface combines easy navigation with point-and-click provisioning of services, reducing the complexity of configuring virtual services and multiple feature sets. Some of the main functions of the Cisco ACE Device Manager are as follows: • Supports end-to-end service provisioning of the Cisco ACE appliance and any associated virtual contexts, including network access, port management, application acceleration and optimization, load balancing, SSL management, resource management, and fault tolerance • Helps you manage Cisco ACE appliance licenses and RBAC • Provides a monitoring interface with a flexible choice of statistics and graphs

Feature	Benefit
Cisco Application Networking Manager (ANM)	Cisco ANM supports the management of virtual devices and hierarchical management domains across multiple Cisco ACE appliances. This server-based management suite discovers, provisions, monitors, and reports across many virtual devices on multiple Cisco ACE appliances, making deployment transparent. Template-based configuration and auditing complement service activation and suspension capabilities to enable quick implementation of applications. Configurable RBA delegation of tasks with a matching service API allows concurrent operation by multiple administrator groups across many Cisco ACE appliances and virtual devices.

Figure 3.   Cisco ACE Virtual Devices and RBA
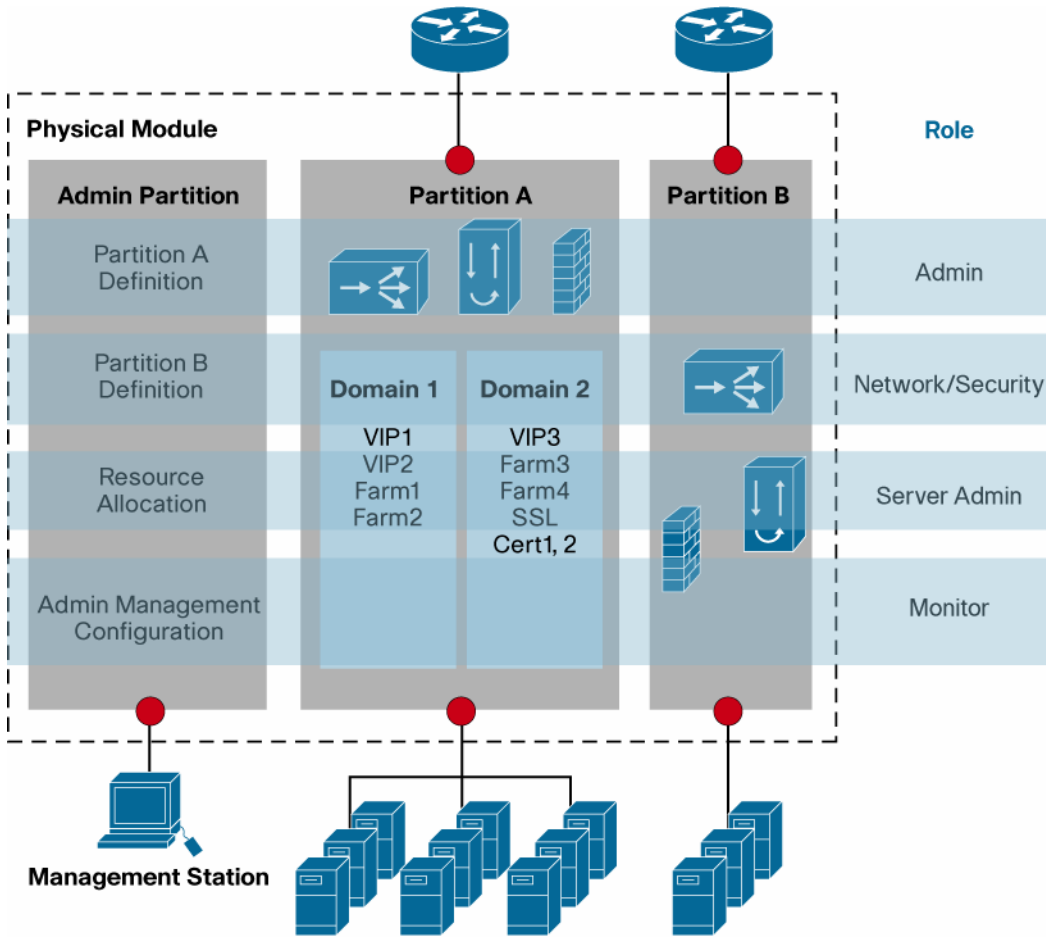
Product Specifications

Table 2 presents the performance specifications for the Cisco ACE 4710.

Table 2.   Product Performance Specifications

Feature	Maximum Performance or Configuration
Global Parameters	
Throughput	1, 2, or 4 Gbps
Compression	500 Mbps, or 1 or 2 Gbps (using GZIP or Deflate)
SSL Performance	
SSL Throughput	1 Gbps
SSL TPS	1000 TPS included in base price; upgradeable to 5000 TPS and 7500 SSL TPS
Application Switching Performance	
Maximum Connections per Second	• 100,000 complete transactions sustained rate (Layer 4) • 30,000 complete transactions sustained rate (Layer 7)
Concurrent Connections	1 million

Table 3 presents the product specifications for the Cisco ACE 4710.

Table 3.   Product Specifications

Item	Specification
Chassis	• 1RU appliance • W x D x H: 16.9 x 20 x 1.67 in. (42.4 x 430 x 509 mm)
Network Ports	4 10/100/1000 Ethernet ports
Management	Embedded browser-based GUI and SNMP
Typical Operating Power	128 watts (W)
Maximum Power	345W
Flash Memory	1 GB
Ambient Temperature	104°F (40°C)
Relative Humidity	80%
Acoustics	< 68 dBA
Certifications	• FCC • CE • VCCI • BSMI BMC • C-tick • BSMI RPC • UL and cUL • CCC • MIC • BSMI Safety Report and BSMI RPC Certificate

Ordering Information

Table 4 lists part numbers for ordering and Table 5 lists service product IDs.

Table 4.   Ordering Information

Part Number	Description
Bundles and Upgrades	
ACE-4710-BAS-2PAK	1G 2 Pack Bundle: Includes two units each of ACE 4710 Hardware, 1 Gbps Throughput, 1000 SSL TPS, 100 Mbps Compression, 5 Virtual Devices, 50 Application Acceleration Connection License, Embedded Device Manager
ACE-4710-1F-K9	1G Bundle: Includes ACE 4710 Hardware, 1 Gbps Throughput, 5,000 SSL TPS, 500 Mbps Compression, 5 Virtual Devices, 50 Application Acceleration Connection License, Embedded Device Manager
ACE-4710-2F-K9	2G Bundle: Includes ACE 4710 Hardware, 2 Gbps Throughput, 7,500 SSL TPS, 1Gbps Compression, 5 Virtual Devices, 50 Application Acceleration Connection License, Embedded Device Manager
ACE-4710-4F-K9	4G Bundle: Includes ACE 4710 Hardware, 4 Gbps Throughput, 7,500 SSL TPS, 2Gbps Compression, 5 Virtual Devices, 50 Application Acceleration Connection License, Embedded Device Manager
ACE-4710-BUN-UP2=	1G Bundle to 2G Bundle Upgrade License: Includes 2-Gbps throughput license, 7500-TPS SSL license, 1-Gbps compression license, 5-virtual devices license, 50 Application acceleration conn. license
ACE-4710-BUN-UP3=	2G Bundle to 4G Bundle Upgrade License: Includes 4-Gbps throughput license, 7500-TPS SSL license, 2-Gbps compression license, 5-virtual devices license, 50 Application acceleration conn. License
Individual Licenses	
ACE-AP-01-LIC	1 Gbps Throughput License
ACE-AP-02-LIC	2 Gbps Throughput License
ACE-AP-04-LIC	4 Gbps Throughput License
ACE-AP-04-UP1=	Throughput upgrade license from 1 Gbps to 4 Gbps
ACE-AP-04-UP2=	Throughput upgrade license from 2 Gbps to 4 Gbps
ACE-AP-SSL-05K-K9	SSL 5,000 TPS License
ACE-AP-SSL-7K-K9	SSL 7,500 TPS License
ACE-AP-VIRT-020	20 Virtual Context License
ACE-AP-C-500-LIC	500 Mbps Compression License
ACE-AP-C-1000-LIC	1 Gbps Compression License
ACE-AP-C-2000-LIC	2 Gbps Compression License
ACE-AP-OPT-LIC-K9	Application Acceleration License
ACE-AP-SSL-UP1-K9=	ACE SSL Upgrade from 5,000 to 7,500 TPS
ACE-AP-C-UP1=	Upgrade Compression From 500 Mbps to 1 Gbps
ACE-AP-C-UP2=	Upgrade Compression From 500 Mbps to 2 Gbps
ACE-AP-C-UP3=	Upgrade Compression From 1 Gbps to 2 Gbps

Table 5.   Service Products

Part Number	Service Product ID	Service Level
ACE-4710-BAS-2PAK	CON-SNT-ACE47PAK	Cisco SMARTnet® Service
ACE-4710-1F-K9	CON-SNT-ACE47101	Cisco SMARTnet®
ACE-4710-2F-K9	CON-SNT-ACE47102	Cisco SMARTnet
ACE-4710-4F-K9	CON-SNT-ACE47104	Cisco SMARTnet
ACE-4710-K9	CON-SNT-ACE4710	Cisco SMARTnet
ACE-4710-BAS-2PAK	CON-SNTE-ACE47PAK	Cisco SMARTnet Enhanced
ACE-4710-1F-K9	CON-SNTE-ACE47101	Cisco SMARTnet Enhanced
ACE-4710-2F-K9	CON-SNTE-ACE47102	Cisco SMARTnet Enhanced
ACE-4710-4F-K9	CON-SNTE-ACE47104	Cisco SMARTnet Enhanced

Part Number	Service Product ID	Service Level
ACE-4710-K9	CON-SNTE-ACE4710	Cisco SMARTnet Enhanced
ACE-4710-BAS-2PAK	CON-SNTP-ACE47PAK	Cisco SMARTnet Premium
ACE-4710-1F-K9	CON-SNTP-ACE47101	Cisco SMARTnet Premium
ACE-4710-2F-K9	CON-SNTP-ACE47102	Cisco SMARTnet Premium
ACE-4710-4F-K9	CON-SNTP-ACE47104	Cisco SMARTnet Premium
ACE-4710-K9	CON-SNTP-ACE4710	Cisco SMARTnet Premium
ACE-4710-BAS-2PAK	CON-S2P-ACE47PAK	Cisco SMARTnet 2-Hour Premium
ACE-4710-1F-K9	CON-S2P-ACE47101	Cisco SMARTnet 2-Hour Premium
ACE-4710-2F-K9	CON-S2P-ACE47102	Cisco SMARTnet 2-Hour Premium
ACE-4710-4F-K9	CON-S2P-ACE47104	Cisco SMARTnet 2-Hour Premium
ACE-4710-K9	CON-S2P-ACE4710	Cisco SMARTnet 2-Hour Premium
ACE-AP-01-LIC	CON-SAU-ACP01GL	Cisco Software Application Support plus Upgrades (SASU)
ACE-AP-02-LIC ACE-AP-02-LIC= ACE-AP-04-LIC=	CON-SAU-ACP02GL	Cisco SASU
ACE-AP-VIRT-020 ACE-AP-VIRT-020=	CON-SAU-ACPVI020	Cisco SASU
ACE-AP-OPT-LIC-K9 ACE-AP-OPT-LIC-K9=	CON-SAU-ACP-OPT	Cisco SASU

For More Information

For more information about the Cisco ACE 4710, visit http://www.cisco.com/go/ace or contact your local account representative.