What's New in Cisco ACE Application Control Engine Module for the Cisco Catalyst 6500 and Cisco 7600 Series—Software Release 2.1.0

PB458841

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 maximizing availability, acceleration, and security of data center applications. The Cisco ACE Module allows enterprises and service providers to accomplish four primary IT objectives for application delivery:

- Maximize 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.

Cisco ACE Module Software Release 2.1.0 highlights includes the following:

Available

- Dedicated multimedia support increases server capacity by 38%.
- Application switching based on actual application health.
- GSS can now leverage ACE intelligence for global load balancing.

Fast

- 10X increase in DNS balancing speed by re-using flow setups.
- Faster recovery of UDP resources improves Layer 4 performance.
- Intelligent re-use of session information delivers faster SSL.

Secure

- Stop DOS attacks by intelligent tagging of malicious traffic.
- Mitigate server resource attacks by fine tuning incoming traffic rates.
- Eliminate attacks against payload information through deep inspection.

Table 1. New Features in Cisco ACE Module Software Release 2.1.0

Available	Description	Benefit
Generic Protocol Parsing (GPP)	ACE has native understanding of the following protocols: HTTP, FTP, DNS, ICMP, SIP, RTSP, Extended RTSP, Radius and RDP. However, data center owners may have to deal with many other applications –custom applications, legacy applications, packaged applications, etc. 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 via hardware using a powerful regular expression engine to obtain maximum performance unlike other software-based solutions.	ACE can switch custom and packaged applications without any programming.
HTTP Header Manipulation	Cisco ACE supports the ability to insert, delete or rewrite HTTP headers in both client requests and server responses. HTTP Header Insertion ACE provides an ability to insert HTTP header in request, response or both. Consider an example when ACE uses source NAT to translate the clients IP address, often the servers need a way to identify that client. To identify a client whose source IP address has been NAT'ed, you can instruct the ACE to insert a generic header and string value of source IP address before the request is sent to the server.	Increased client visibility for applications to perform logging and auditing.
	HTTP Header Rewrite ACE provides an ability to rewrite HTTP header in request, response or both. Consider an example where a client wants to connect to a secured Web application. In this scenario, client sends a HTTPS request to the application. An external application switch terminates the SSL connection and sends clear text to the application. Since the application is unaware that incoming client HTTPS request was terminated on the application switch, the application may redirect the client to a non secured HTTP URL rather than to the secured HTTPS URL. To solve this problem, Cisco ACE application switch modifies the redirected URL from HTTP to HTTPS in the "Location" header before sending the response to the client.	Secure delivery of SSL content back to the client
	Delete HTTP Header HTTP header deletion can be used to strip sensitive HTTP headers from server responses. For example, by default many web servers include the information about the web server such as version, O/S in HTTP response header. This information could potentially be used to generate malicious attacks. In this example, Cisco ACE can automatically delete such headers, thus hiding the server type and version from clients.	Secured Web applications
Partial Server-Farm Failover	Currently, if a backup server-farm is configured, the primary server-farm would failover to the backup only when all the real servers in that server-farm go down. Partial Server-farm Failover feature allows the user to specify a minimum percentage (eg. X%) of real servers to be active in the farm before the primary server-farm fails over to the backup server-farm. When the primary server-farm fails over to the backup, all currently established connections will continue to exist on the primary server-farm. All new requests are routed to the backup server-farm. For the primary server-farm to return to service, a minimum percentage (eg. Y% > X%) of real servers should be active.	Cisco ACE provides capability to manage which server farm (primary or backup) receives new traffic based on the number of available Real Servers (RServers).
TCP Dump	ACE can capture real-time packet information for the network traffic that passes through the ACE. The ACE buffers the captured packets, and you can copy the buffered contents to a file in flash memory on the ACE or export to Ethereal.	Enhanced Troubleshooting

Available	Description	Benefit
Source NAT for VIP	Source NAT for VIP allows to include a Virtual IP (VIP) address in the network address translation (NAT) pool for dynamic NAT and PAT This feature can be used to Source-NAT Real Server-originated connections (bound to the client) using the VIP address.	Save real world IP addresses on the client-side network
Source NAT for Sever Farm	Enables source NAT to a backup Server Farm multiple hops away during the failure of a primary ServerFarm ACE can apply dynamic NAT for both primary and backup Server Farms, for multiple outgoing Server VLAN's.	Provides continuous application availability even during the Primary Server Farm failure.
Adaptive Response Predictor	Cisco ACE adds several new intelligent load-balancing predictors. Cisco ACE predictor selects a server based on its response time. Response times are calculated over a user-configured number of samples and supports the following three measurement options: • SYN-to-SYN-ACK: Server response time between SYN sent from ACE to SYN-ACK received from server • SYN-to-Close: Server response time between SYN sent from ACE to FIN/RST received from server. Application Request to Response: Server response time between HTTP request sent from ACE to HTTP response received from server .	ACE switches applications based on real-time server/application performance data measured across a variety of user-configured criteria.
Least-Loaded Predictor	This ACE predictor selects the least-loaded server based on the value of up to 8 SNMP MIB objects defined by the user. These objects can be server resources like CPU utilization, memory resources, disk drive availability, etc. Users can associate weights with each of the measured objects for ultimate granular control in application switching.	
Least-Bandwidth Predictor	This ACE predictor selects the server that processed the least amount of application traffic between ACE and the real servers, in both directions, over a user-configured sampling period and number of samples.	
Keepalive Appliance Protocol (KAL-AP)	Keepalive-Appliance Protocol (KAL-AP) on the ACE application switches allows communication with ACE Global Site Selector (GSS), to report VIP and real Servers availability The above information is used by the Cisco ACE GSS for intelligent global server load balancing (GSLB) across data centers. KAL-AP communication between the ACE GSS can be secured using MD5 encryption.	Global server load-balancing (GSLB) to provide business continuity
Simple Network Management Protocol (SNMP) Probes	The main purpose of an SNMP message is to control (set) or monitor (get) parameters on an SNMP agent, eg. web server. SNMP uses an Object Identifier (OID) to specify the exact parameter to set or get in an SNMP agent. This SNMP-based server load probe allows the user to configure a query consisting of up to eight SMNP object identifiers (OIDs) to probe the server. In addition, the user can associate weights with each of these OIDs. The information retrieved by this probe from the servers is used as input to the Least-loaded predictor described above.	Intelligent server health monitoring using customized probes in an SNMP environment
Scripted Probes	In addition to existing flexibility to author specific Toolkit Command Language (TCL) scripts unique to customer environments for server health monitoring, ACE support is extended to execute ACE CLI commands via TCL Scripts	Intelligent server health monitoring using customized TCL scripts
HTTP Return Code Parsing	This feature enables configuration of a threshold value based on the number of specific HTTP return codes seen in a specified timeframe. When this threshold is reached, the Cisco ACE can automatically remove a server from service. HTTP return code parsing is invaluable in a scenario where it is desirable to remove a server from service if, for example, a page cannot be found (e.g. many HTTP 404 Not Found responses are seen). In this case, traditional TCP-based HTTP server availability probes would indicate the server is available and responding, but would not provide information about whether or the server is able to fulfill requests for content. HTTP return code parsing is needed in this scenario to provide additional server-level information with which to determine server availability.	Enhanced in-band server health monitoring for improved application availability

Available	Description	Benefit
New Protocol Support: Session Initiation Protocol (SIP)	SIP is a peer-to-peer protocol where end-devices (user agent) initiate interactive communications such as Internet multimedia conferences, Internet telephone calls, voice over IP, and multimedia distribution sessions with SIP servers. Cisco ACE supports SIP over TCP and UDP. Load-balancing decision can be based on fields in the SIP header. Session persistence is based on SIP Call ID. Based on the keep-alive response from the SIP servers, ACE can rotate the server in or out of service, and make reliable load-balancing decisions for SIP-based media applications.	Intelligent switching, scalability and high-availability of SIP-based multimedia applications
New Protocol Support: Real-Time Streaming Protocol (RTSP)	RTSP protocol is used for streaming audio and video for applications such as Cisco IP/TV, RealAudio, and RealNetworks. Cisco ACE supports RTSP over TCP. The load-balancing decision can be based on RTSP URL(rtsp://) or fields in the RTSP header. Session Persistence is done using RTSP Session headers. Based on the keep-alive response from application servers running Cisco IP/TV, Real Audio or Real Networks, etc. the ACE can place the servers in or out of service, and make reliable load-balancing decisions of RTSP media applications.	Intelligent switching, scalability and high-availability of RTSP-based streaming audio and video
New Protocol Support: Remote Authentication Dial-In User Service (RADIUS).	RADIUS is an authentication and accounting protocol. Cisco ACE is RADIUS protocol aware and provides ability to load balance and persist based on specific RADIUS protocol information.	Intelligent switching , scalability and high-availability across many Radius servers
New Protocol Support: Microsoft Remote Desktop Protocol (RDP)	Microsoft RDP provides users with remote display and input capabilities over network connections for Windows-based applications running on a terminal server. ACE supports RDP load balancing for Windows–based applications running on terminal servers. Cisco ACE makes the load-balancing decision based on the routing token in the RDP header.	Intelligent switching , scalability and high-availability across many Microsoft terminal servers

Table 2.

Fast	Description	Benefit
UDP Booster	UDP booster feature is used for switching applications that requires very high UDP connection rates, like DNS loadblancing. To achieve such high rates, ACE uses statistical load-balancing instead of traditional algorithmic load-balancing.	Boost performance of UDP-based applications like DNS load balancing to millions of requests per second.
UDP Fast Aging	ACE can provide very high scalability in terms of number of clients serviced for applications requiring a single response per request With UDP Fast Aging ACE closes the UDP connection immediately after the server responds to the client. ACE load balances all new requests to new real servers in the server farm according to the predictor algorithm. All retransmitted UDP requests from clients go to the same real server.	Highly scalable UDP applications that require a single response per request.

Fast	Description	Benefit
Session ID Stickiness	Stickiness or persistence is the mechanism that allows the same client to maintain multiple simultaneous or subsequent connections with the same real server for the duration of a session. When customers visit an e-commerce site and start to add items to their shopping carts, it is important that all the requests from a client get directed to the same server so that all the items are contained in one shopping cart on one server. An instance of a customer's shopping cart is typically local to a particular Web server and is not duplicated across multiple servers. E-commerce applications are not the only types of applications that require stickiness. Any web application that maintains client information and state may require stickiness, such as banking applications or online trading. ACE can stick a client to an appropriate server based on Source and/or destination IP address, Cookies, Hypertext Transfer Protocol (HTTP) header and SSL Session ID. Secure Socket Layer (SSL) ensures the secure transmission of data between a client and a server. The client and server use the SSL handshake protocol to establish an SSL session between the two devices. A new session ID is created every time the client and the SSL server go through a complete negotiation of session parameters, unique to each session. ACE can stick a client to an appropriate server based on SSL Session ID.	Secure session persistence over SSL
Session ID Reuse	Secure Socket Layer (SSL) ensures the secure transmission of data between a client and a server. The client and server use the SSL handshake protocol to establish an SSL session between the two devices. In a standard SSL handshake, a new session ID is created every time the client and the SSL server go through a complete negotiation of session parameters, unique to each session. ACE can accelerate subsequent SSL session setups between the client and the ACE by reusing SSL IDs stored in its session cache from previously negotiated session parameters.	Accelerate SSL client connection setup.
Client Authentication	In a standard SSL implementation a server authenticates itself to clients by sending an X509 certificate (digital identification for authentication). However, there is no similar assurance that the client is who it claims to be. Client authentication feature on ACE, acting as an SSL server, addresses this problem by requiring the client to provide X509 certificate. ACE (server) verifies the following information on the certificate: • A recognized CA issued the certificate. • The valid period of the certificate is still in effect. • The certificate signature is valid and not tampered. • The CA has not revoked the certificate.	Permits only legitimate clients to access servers

Table 3.

Secure	Description	Benefit
Rate Limiting	ACE software release 2.1 adds new rate limiting capabilities: • Connection rate: The number of connections per second received by the ACE destined to a real server • Bandwidth rate: The number of bytes per second applied to the network traffic exchanged between the ACE and a real server, in both directions Rate-limiting based traffic policing is supported at the per virtual server level. Rate- limiting based load-balancing is supported at the per real/rserver level. This features also provides feedback to load-balancing decision; it takes real servers exceeding rate limits out of load-balancing and puts them back into load-balancing when the rate is below the limits. The rate limit parameters can be applied to a set of real servers, virtual servers or both.	Protects Server resources

Secure	Description	Benefit
Access Control List (ACL) with Object Groups	ACLs are used to restrict network access based on a set of filters defined as access-list entries (ACE). An ACL is applied to an interface or globally to all interfaces. ACLs are used to filter interesting traffic and instruct the ACE to either permit or deny the traffic based on the criteria defined in the filter. The filters can be based on criteria such as source address, destination address, protocol, protocol-specific parameters such as ports (for TCP or UDP), etc. ACLs permit/deny access from a client to a server for a specific service. In large configurations there can be multiple combinations of client, server and services resulting in large number of ACL entries. Managing this large number of ACLs can become very challenging. Object-Grouping provides the capability to group client addresses, server addresses and services together in a single ACL entry.	Streamlines configuration of multiple ACL entries.
TCP SYN Cookie—Denial-of-Service (DoS) Protection	A successful TCP three-way handshake (SYN, SYN-ACK, ACK) is required for a client to connect to the server. Occasionally the three-way handshake may not complete. Such occurrences are normal if the frequency is low, however a high volume of such occurrences could signal a hacker trying to attack the server. A TCP SYN cookie is an initial sequence number calculated by the server to a SYN request from a client and inserted in the SYN-ACK response. A TCP SYN flood attack is characterized by large number of SYN requests sent to a server from one or more clients with source IP addresses that are invalid and unreachable, the goal being to overwhelm the target server, consume its resources, and cause it to deny service to legitimate connection requests. SYN Cookie feature on ACE provides a mechanism to authenticate a client thereby preventing SYN floods from a rogue client.	ACE protects itself and servers in the applications from DOS attacks
Multimedia and Voice over IP (VoIP): SIP, and Skinny Client Control Protocol (SCCP)	In addition to existing support for hardware-accelerated application inspection for HTTP, FTP, DNS, ICMP and RTSP protocols. ACE extends this capability to SIP, SCCP and ILS/LDAP.	Secures multimedia and VOIP applications and services
Database and OS Services: Internet Locator Services and Lightweight Directory Access Protocol (ILS/LDAP)	Application protocol inspection helps verify the protocol behavior and identify unwanted or malicious traffic attempting to pass through the ACE.	

Table 4. Cisco Catalyst 6500 and Cisco 7600 Series System Requirements

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

Ordering Information

Table 5. Ordering Information

Part Number	Product Description
WS-C6509E-ACE20-K9**	Cisco ACE20 6509 Bundle with 8 Gbps Throughput License

WS-C6504E-ACE20-K9**	Cisco ACE20 6504 Bundle with 4 Gbps Throughput License
WS-C6509-E-ACE-K9**	Cisco ACE10 6509 Bundle with 8 Gbps Throughput License
WS-C6504-E-ACE-K9**	Cisco ACE10 6504 Bundle with 4 Gbps Throughput License
ACE20-MOD-K9	Cisco ACE20 Service Module for Cisco Catalyst 6500 Series and Cisco 7600 Series: Includes 1000 SSL TPS and 5 Virtual Devices
ACE20-MOD-K9=	Cisco ACE20 Service Module for Cisco Catalyst 6500 Series and Cisco 7600 Series: Includes 1000 SSL TPS and 5 Virtual Devices (spare)
ACE10-6500-K9	Cisco ACE10 Service Module for Cisco Catalyst 6500 Series and Cisco 7600 Series, Includes 1000 SSL TPS and 5 Virtual Devices
ACE10-6500-K9=	Cisco ACE10 Service Module for Cisco Catalyst 6500 Series and Cisco 7600 Series, Includes 1000 SSL TPS and 5 Virtual Devices (spare)
ACE-16G-LIC	16Gbps Throughput License for Cisco ACE20
ACE-08G-LIC	8-Gbps Throughput License for Cisco ACE 10 and Cisco ACE20
ACE-04G-LIC	4-Gbps Throughput License for Cisco ACE10 and Cisco ACE20
ACE-UPG2-LIC=	Upgrade License from 8 Gbps to 16 Gbps for Cisco ACE20
ACE-UPG1-LIC=	Upgrade License from 4 Gbps to 8 Gbps for Cisco ACE10 and Cisco ACE20
ACE-SSL-15K-K9	15,000 SSL Transactions per Second License for Cisco ACE10 and Cisco ACE20
ACE-SSL-10K-K9	10,000 SSL Transactions per Second License for Cisco ACE10 and Cisco ACE20
ACE-SSL-05K-K9	5,000 SSL Transactions per Second License for Cisco ACE10 and Cisco ACE20
ACE-SSL-UP2-K9=	Upgrade license from 10,000 to 15,000 SSL Transactions per Second License for Cisco ACE10 and Cisco ACE20
ACE-SSL-UP1-K9=	Upgrade license from 5,000 to 10,000 SSL Transactions per Second License for Cisco ACE10 and Cisco ACE20
ACE-VIRT-250	250 Virtual Contexts License for Cisco ACE10 and Cisco ACE20
ACE-VIRT-100	100 Virtual Contexts License for Cisco ACE10 and Cisco ACE20
ACE-VIRT-050	50 Virtual Contexts License for Cisco ACE10 and Cisco ACE20
ACE-VIRT-020	20 Virtual Contexts License for Cisco ACE10 and Cisco ACE20
ACE-VIRT-UP3	Upgrade License from 100 to 250 Virtual Contexts for Cisco ACE10 and Cisco ACE20
ACE-VIRT-UP2	Upgrade License from 50 to 100 Virtual Contexts for Cisco ACE10 and Cisco ACE20
ACE-VIRT-UP1	Upgrade License from 20 to 50 Virtual Contexts for Cisco ACE10 and Cisco ACE20

** Cisco ACE Bundles do not include I/O modules so that customer can order I/O modules of their choice.

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

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.

Printed in USA C25-458841-00 03/08

