Tel: +44 (0)1279 408 777
Email: sales@gocomsys.com
Website: www.gocomsys.com

Refurbished CISCO RBA Datasheet

CISCO > INTERFACES-MODULES

Cisco Services Modules

Features and 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.
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.
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.

Cisco ACE Module Performance and Configuration

Global Parameters

Throughput	16 Gbps*, 8 Gbps*, and 4 Gbps

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

SSL Performance

SSL throughput	3.3 Gbps

Application Switching Performance

Maximum connections per second	325,000 complete transactions sustained rate
Concurrent connections	4 million
Sticky table entries	4 million

Cisco ACE Module Specifications

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)

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%

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

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

The next steps...

ORDER NOW

VIEW ONLINE

Tel: +44 (0)1279 408 777

Email: sales@gocomsys.com

Website: www.gocomsys.com