

Application Delivery with Cisco ACE Application Control Engine



June 2007

Introduction

Application front ends (AFEs) are data center appliances that are used to facilitate access to network applications for both local and remote users. These types of devices are also referred to as application switches or application delivery controllers (ADCs).

The basic idea behind AFEs can be traced back to the IBM mainframe computing model of the 1960s and 1970s, where front-end processors (FEPs) helped optimize the utilization of mainframe computers by offloading communications-intensive processing. In the current environment, there are many examples of communications-intensive processing that are best removed from servers and performed on devices that are designed especially for those tasks. For example, Extensible Markup Language (XML) is estimated to be 15 percent of current network traffic and is expected to grow to 50 percent of network traffic over the next few years. An XML message is usually a high-value transaction, such as a purchase order. These messages are also complex and are usually 3 to 10 times larger than an equivalent binary message.

In its current incarnation, the AFE can combine a number of functions, including the following:

- Server load balancing (SLB), to maximize the scalability and availability of an application
- Layer 4 to 7 switching, to direct application queries to the most appropriate server
- Firewall functions, to help ensure the integrity of the company's data and provide application-specific security
- Off-loading of computationally intensive tasks, such as the processing of Secure Sockets Layer (SSL) traffic
- XML application and Web services switching, acceleration, and securing

In conducting a broad market survey of enterprise requirements for WAN optimization and application acceleration¹, Ashton, Metzler & Associates has developed a set of evaluation criteria that can assist IT organizations in the selection of AFE solutions. For example, the criteria can be used as the basis for an initial screening of vendor solutions to arrive at a short list of vendors whose solutions can be examined more carefully before a purchase decision is made. Another possible use of the criteria is as an aid in developing a more detailed RFP to given to vendors on the short list.

The remainder of this document provides a brief discussion of the evaluation criteria together with an evaluation of how the Cisco® AFE solution meets these criteria. The Cisco AFE solution consists of the Cisco ACE Application Control Engine Modules for Cisco Catalyst® 6500 Series Switches or Cisco 7600 Series Routers and the Cisco ACE Global Site Selector (GSS). Throughout this document the Cisco solution will be referred to either as ACE or as Cisco's ACE. The evaluation of Cisco ACE is based primarily on an examination of documents posted at the Cisco Website. Therefore, this evaluation provides an example of the sort of preliminary analysis that would typically be performed to arrive at a short list of potential solutions.

¹ Application Delivery Handbook, www.kubernan.com

Evaluation Criteria

The AFE evaluation criteria are listed in Table 1. Note that this list is intended as a fairly complete compilation of possible criteria. As a result, a given organization or enterprise may apply only a subset of these criteria for a given purchase decision. In addition, individual organizations will ascribe different weights to each of the criteria because of differences in data center architecture, security requirements, network design, and application mix. As shown in the table, assigning weights to the criteria and relative scores for each solution provides a simple methodology for comparing alternative solutions.

IT organizations can use many techniques to complete Table 1 and use it to compare alternative solutions. For example, the weights can range from 10 to 50 points, with 10 points meaning not important, 30 points meaning average importance, and 50 points meaning critically important. The score for each criteria can range from 1 to 5, with 1 meaning fails to meet minimum needs, 3 meaning acceptable, and 5 meaning significantly exceeds requirements.

As an example, consider solution A. For this solution, the weighted score for each criterion (W_iA_i) is found by multiplying the weight (W_i) of each criterion by the score of each criterion (A_i). The weighted scores for all criteria are then summed ($\sum W_iA_i$) to get the total score for the solution. This process can then be repeated for additional solutions, and the total scores of the solutions can be compared.

Table 1 Criteria for Evaluating AFEs

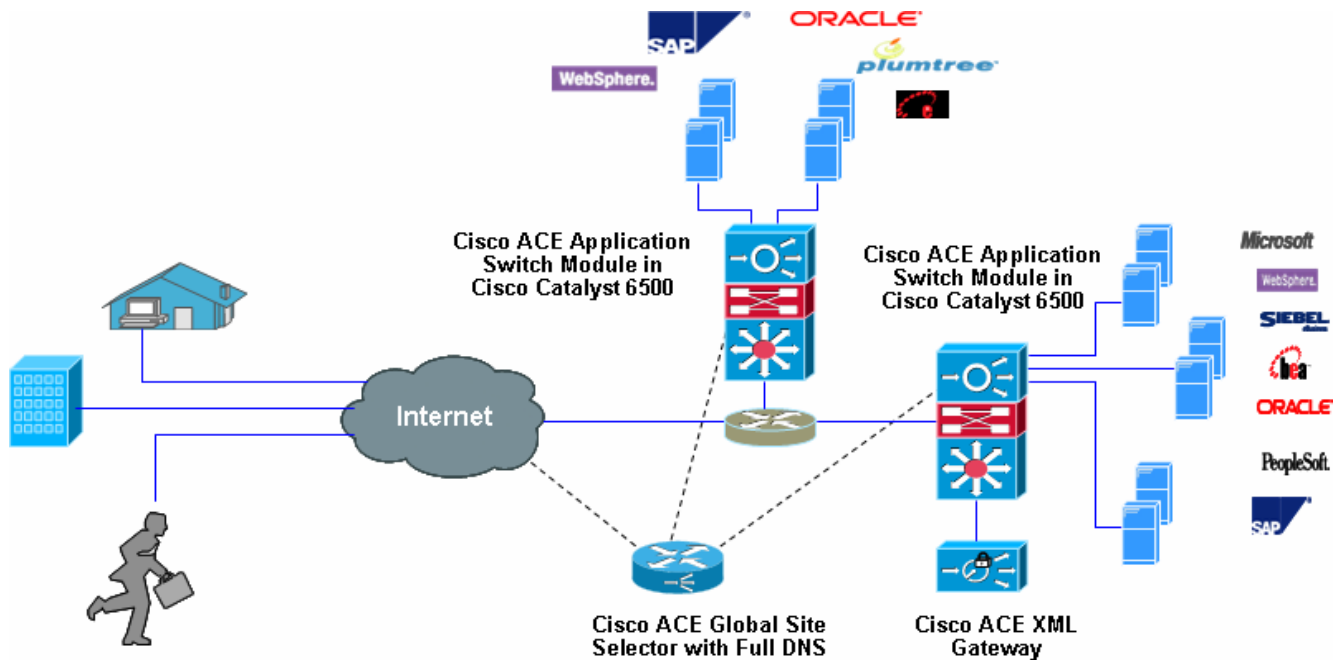
Criterion	Weight (W_i)	Score for Solution A (A_i)	Score for Solution B (B_i)
Performance			
Transparency and integration			
Scalability			
Solution architecture			
Functional integration			
Virtualization			
Security			
Application availability			
Cost effectiveness			
Ease of deployment and management			
Total score		$\sum W_iA_i$	$\sum W_iB_i$

Cisco ACE

As shown in Figure 1, Cisco ACE is a family of application delivery products and consists of Cisco ACE Modules installed in Cisco Catalyst 6500 Series Switches or Cisco 7600 Series Routers in data centers. The Cisco GSS can redirect users requests to help ensure business

continuity and the availability of enterprise application resources even in the event of a catastrophic failure that takes an entire data center offline. The Cisco ACE XML Gateway can switch, accelerate, and secure XML application and Web services. Although the figure shows only user access to the data center over the Internet, the solution also provides benefits for users located on the same campus or site LAN as the data center.

Figure 1 Cisco ACE Solution for Application Delivery



Evaluating the Cisco ACE Family

This section evaluates Cisco ACE family based on the criteria presented in Table 1. These evaluation criteria are not mutually exclusive. For example, the cost effectiveness, security, and ease of deployment of Cisco ACE result in part from the solution’s support of virtualization.

Performance

Description of the Criteria

Performance is an important criterion for any piece of networking equipment. Performance, however, is particularly important for a device such as an AFE because data centers are central points of aggregation. Thus, the AFE needs to be able to support the extremely high volumes of traffic transmitted to and from servers in data centers.

A simple definition of performance is the number of bits per second that a device can support. Although bits per second is extremely important, in the case of AFEs other important measures of performance include the number of Layer 4 connections that can be supported and the number of Layer 4 setups and teardowns that can be supported.

Third-party tests of a solution can be helpful. You must be sure, however, to quantify the performance gains that the solution will provide in the particular application environment in which it will be installed. As part of this quantification, you must determine whether the performance of the solution degrades as additional functions within the solution are activated or when changes are made to the application mix within the data center.

Evaluation of Cisco ACE

According to Cisco, the Cisco ACE Module is capable of processing application traffic at up to 16 Gbps in a single module and 64 Gbps in a switch chassis with four modules. The module also supports a sustained rate of up to 348,000 Layer 4 connection setups and teardowns per second. These numbers represent some of the highest performance rates currently available in the marketplace.

Transparency and Integration

Description of the Criteria

Transparency is an important criterion for any piece of networking equipment. However, unlike branch office optimization solutions that are proprietary, AFEs are standards based and so tend to be more transparent than other classes of networking equipment.

You must be able to deploy an AFE solution and not break anything such as routing, security, or quality of service (QoS). The solution should also be as transparent as possible relative to both the existing server configurations and the existing security domains. In addition, the solution should not make troubleshooting more difficult.

The AFE also must easily integrate with other components of the data center, such as the firewalls, and with other appliances that may be deployed to provide application services. In some data centers, it may be important to integrate the Layer 2 and 3 access switches with the AFE and firewalls so that all application intelligence, application acceleration, application security, and server offloading are applied at a single point in the data center network.

Evaluation of Cisco ACE

Cisco ACE is an asymmetrical solution, which means that it is fully transparent from the perspective of the local and remote client systems as well as the server and applications. Cisco states that as a standards-based technology, Cisco ACE can be integrated with standards-compliant solutions from other vendors for functions such as firewalling and SSL processing offloading.

With its presence in the enterprise networking market, Cisco is in a unique position to help ensure that its solutions integrate with the existing networking infrastructure. Hence, it is not surprising that Cisco states that the Cisco ACE Module also integrates transparently with other types of service modules within Cisco switches and with other Cisco network elements. In particular, Cisco ACE complements the Cisco branch-office optimization solution, providing a

complete end-to-end solution for performance-optimized remote and local access to centralized enterprise applications and data storage resources.

In testing products such as an AFE, IT organizations typically test performance criteria such as the ones previously mentioned. IT organizations should also test the transparency of these solutions.

Scalability

Description of the Criteria

To be highly scalable, an AFE solution must provide a range of products that span the performance and cost requirements of a variety of data center environments. Performance requirements for accessing data center applications and data resources are usually characterized in terms of both the aggregate throughput of the AFE and the number of simultaneous application sessions that can be supported. A related consideration is how device performance is affected as additional functions are enabled.

Evaluation of Cisco ACE

The current Cisco ACE solution is based on a single Cisco ACE Module for Cisco switches. Scalability is achieved in two ways:

- The module is offered with tiered performance levels that are linked to the software license purchased in conjunction with the hardware. For example, the Cisco ACE Module has software licenses that provide three levels of performance with 4, 8, or 16 Gbps of throughput.
- Up to four Cisco ACE Modules can be installed in a Cisco switch, allowing higher levels of maximum throughput as well as redundancy to support higher availability.

The performance options are summarized in Table 2.

Table 2 Performance Options

Configuration	Throughput (Gbps)	Maximum Layer 4 Setups and Teardowns per Second
4 Cisco ACE Modules with 16-Gbps license	64	1,392,000
3 Cisco ACE Modules with 16-Gbps license	48	1,044,000
2 Cisco ACE Modules with 16-Gbps license	32	696,000
Cisco ACE Modules with 16-Gbps license	16	348,000
Cisco ACE Modules with 8-Gbps license	8	348,000
Cisco ACE Modules with 4-Gbps license	4	348,000

Most companies start with a limited deployment of this technology and then expand it over time, so the capability of the Cisco solution to grow incrementally to 64 Gbps is a major strength of the solution.

Solution Architecture

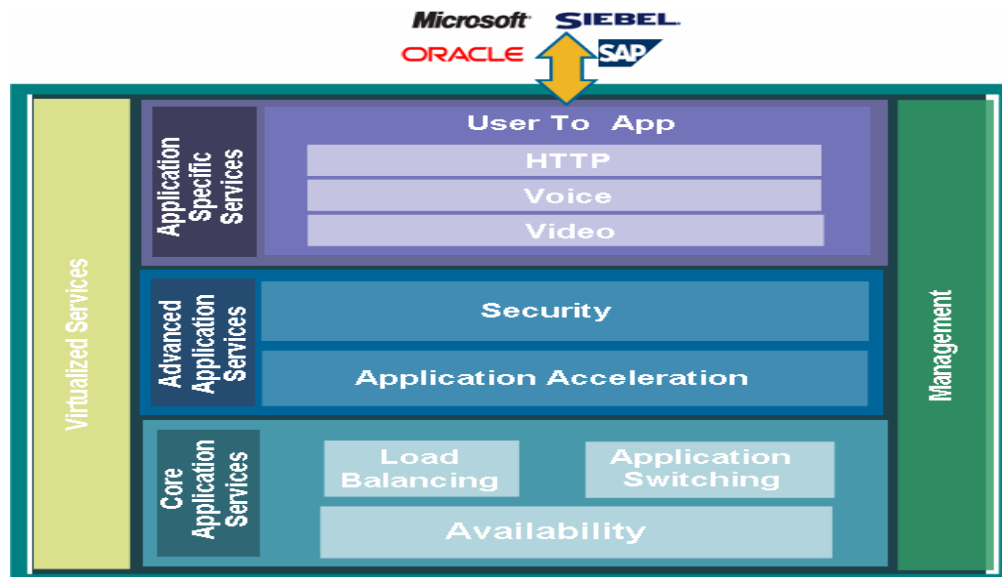
Description of the Criteria

Together, the scalability and the solution architecture define the capability of the solution to support a range of implementations and to extend to support additional functions. In particular, if the organization intends the AFE to be able to support additional optimization functions over time, you must determine whether the hardware and software architecture can support new functions without an unacceptable loss of performance and without unacceptable downtime.

Evaluation of Cisco ACE

The Cisco ACE layered architecture is shown in Figure 2. This figure shows how the application interface is layered on a virtualized layer of application services over an application switching foundation. The Cisco ACE Module has provisions for two daughter cards that can be used to provide hardware support for additional functions that may be added in the future.

Figure 2: Cisco ACE Architecture



Another crucial component of an AFE's architecture is the way the AFE supports scalability. Cisco supports scalability with software license upgrades. This architecture tends to reduce the need for new hardware and hence minimizes the application downtime and degradation associated with hardware-centric capacity upgrades.

As is described later in this document, the Cisco ACE architecture supports virtualization. As a result, Cisco ACE can deliver services such as server load balancing, acceleration, and security

across any application or department on a virtual device basis. For example, an IT department can allocate a virtual device for each line of business. Virtualization can substantially reduce capital, cooling, rack space, and power requirements in the data center and enable an organization to better scale its data center resources.

Functional Integration

Description of the Criteria

Many data center environments have plans in place to reduce overall complexity by consolidating both the servers and the network infrastructure. An AFE solution can contribute significantly to network consolidation by supporting a wide range of application-aware functions that transcend basic server load balancing and content switching. Extensive functional integration reduces the complexity of the network by minimizing the number of separate devices and user interfaces that data center managers and administrators must navigate. Reduced complexity generally translates to lower total cost of ownership (TCO) and higher availability.

Evaluation of Cisco ACE

The Cisco ACE solution integrates the full range of Cisco application delivery technologies, including Layer 4 and 7 load balancing and content switching, application security, server offload for SSL, and TCP processing, as well as an expanded set of asymmetrical (server-side only) application acceleration capabilities. Other, more specialized functions, such as XML processing offloading, are provided by the Cisco ACE XML Gateway standalone appliance. Cisco ACE Modules in Cisco Catalyst switches provide yet another dimension of functional integration and network consolidation.

Virtualization

Description of the Criteria

Virtualization is becoming a primary technology for achieving data center consolidation and its related benefits. For example, server virtualization supports data center consolidation by allowing a number of applications running on separate virtual machines to share a single physical server. Prior to virtualization, a common practice was to run only one application per server to maximize operating system stability. This approach was expensive in that it required additional pieces of hardware, and it also increased the need for space and power, further increasing costs.

AFEs can also be virtualized by partitioning a single physical AFE into a number of logical AFEs or AFE contexts. Each logical AFE can be configured individually to meet the server load balancing, acceleration, and security requirements of a single application or a cluster of applications. Therefore, each virtualized AFE can consolidate the functions of a number of physical AFEs dedicated to the support of single applications. Virtualization adds significantly to the flexibility of the data center by allowing applications to be easily moved from one physical server to another. For example, with a virtual AFE mapped to a virtual machine, the AFE does not need to be reconfigured when an application is moved or automatically fails over

to a new physical machine. Benefits of virtualization include reduced TCO through consolidation of AFE physical devices, higher availability in the event of failover, and associated savings in management costs and power and cooling costs.

Evaluation of Cisco ACE

The Cisco ACE product family has a virtualized architecture that enables IT managers to configure up to 250 virtual AFE devices on a single physical Cisco ACE Module. This architecture allows IT organizations to provide customized application delivery functions for different applications or departments or to accommodate other requirements. This approach results in fewer devices to install and manage to meet the needs of diverse applications. Each virtual AFE can be given an allocation of the physical AFE's resources, such as bandwidth, number of active connections, connection setup and teardowns per second, number of Network Address Translation (NAT) translations, and memory.

The Cisco role-based administration (RBA) feature allows organizations to specify administrative roles and restrict administrators to specific functions within the device or its virtual partitions. Cisco ACE virtualization also allows different administrative domains within the overall IT structure to maintain independent, decentralized administrative control over their application environments.

Cisco provided third-party test results that show the potential benefits of AFE virtualization in savings for power and cooling. For a sample configuration of 25 virtual AFEs, compared to the same number of standalone AFEs the tests show savings in excess of US\$100,000 per year in power and cooling costs.

Some solutions currently available in the marketplace limit their support of virtualization to access-control capabilities and do not offer true device and service-level virtualization. Although this approach is helpful, to get the real benefits of virtualization, the implementation should be at the device level, to allow all aspects of the physical device to be virtualized. Ashton, Metzler & Associates is not aware of any AFE other than Cisco ACE that has a truly virtualized architecture.

Security

Description of the Criteria

The solution must be compatible the current security environment, while also allowing the configuration of application-specific security features that complement general-purpose security measures, such as firewalls and intrusion detection system (IDS) and intrusion prevention system (IPS) appliances. In addition, the solution itself must not create any additional security vulnerabilities.

Evaluation of Cisco ACE

The Cisco ACE solution is designed to serve as an additional layer of security for servers and applications in a multilayered security model. Cisco ACE virtualization maximizes the isolation

between application environments, preventing attacks on one application from affecting other applications supported by the same AFE device. Cisco ACE also supports SSL encryption and standard network security features such as NAT and Port Address Translation (PAT).

Cisco ACE supports stateful firewall access control lists (ACL)s in conjunction with application and protocol inspection engines that use the Layer 4 to 7 packet inspection capabilities of content switching. For example, Cisco ACE performs HTTP deep packet inspection of the header, URLs, and payload. Cisco ACE also performs protocol compliance inspection, filtering, and fixup for data center protocols such as Real-Time Streaming Protocol (RTSP), Domain Name System (DNS), FTP, and Internet Control Message Protocol (ICMP). These capabilities allow the Cisco ACE to provide IDS- and IPS-type protection from protocol attacks and denial-of-service (DoS) attacks, plus an additional level of protection against day-zero attacks.

Security remains a priority concern for nearly all IT organizations. An important feature of Cisco ACE is that it blocks anomalous signatures in network traffic targeted at server software that might otherwise result in DoS. In this way, Cisco ACE protects against identity theft, data theft, application disruption, and fraud.

This integrated firewall capability minimizes the space, capital expense, management, and possible performance implications associated with having to install a separate security device between data center switches and servers to manage user access and to identify and control malware. Building layers of security protection into all key network junctures is a security best practice that Cisco recommends.

As XML traffic increases in data centers, an application switching solution must also provide XML security. The Cisco ACE XML Gateway appliance secures XML applications, Web-services, and intra-application communications.

Application Availability

Description of the Criteria

The availability of enterprise applications is typically a very high priority. Because the AFE is in line with the Web servers and other application servers, a traditional approach to defining application availability is that the AFE must be capable of supporting redundant, high-availability configurations that feature automated failover among the redundant devices, a traditional approach to application availability. Although this type of support clearly is important, application availability has other dimensions. For example, as previously mentioned, an architecture that enables scalability through the use of software license upgrades tends to minimize the application downtime associated with hardware-centric capacity upgrades.

Evaluation of Cisco ACE

Cisco ACE supports stateful failover between redundant service modules with full replication of connection state. Two basic redundancy configurations are supported:

- Primary and secondary Cisco ACE Modules can be installed in the same Cisco switch.

- Where dual redundant data center access switches are in the path to the servers, Cisco ACE redundancy is achieved with a Cisco ACE Module installed in each switch.

In either configuration, Cisco ACE allows a virtual partition on one module to be configured to fail over to a backup virtual partition on the secondary module without affecting the other virtual partitions serving other applications.

With either the Cisco ACE appliances or modules, the redundant pair of devices can support either active-passive or active-active redundancy. In active-active mode, both Cisco ACE devices work simultaneously and provide backup for each other while supporting stateful failover.

Cisco ACE helps ensure application availability by protecting the application from server failure. This function is provided by an extensive set of application health probes that help ensure that traffic is forwarded to a server that is functioning normally and has the resources to satisfy client requests.

As mentioned earlier, the Cisco GSS appliance provides a failover system among multiple data centers. This capability helps ensure business continuity in the event of catastrophic failure of a data center site. In addition, the Cisco ACE architecture enables scalability through the use of software license upgrades. In many cases, this capability eliminates the long delay associated with the need to purchase and install new hardware to support growth. As a result, organizations circumvent the application downtime and degradation associated with hardware-centric capacity upgrades.

Cost Effectiveness

Description of the Criteria

Cost effectiveness is related to scalability. In particular, you must understand what the initial solution costs. You should also understand how the cost of the solution changes as the scope and scale of the deployment expands.

Evaluation of Cisco ACE

The cost effectiveness of the Cisco ACE solution is greatly enhanced by its virtualization capabilities, which affect both capital expenditures (CapEx), such as hardware and software purchases, and operating expenses (OpEx), such as rack space, power, cooling, and ongoing management costs for applications. For example, Cisco ACE virtualization reduces the number of individual application switches needed in consolidated data centers, which typically have space limitations. Operating with fewer physical devices reduces capital costs, and having fewer devices in the data center frees rack space and reduces power and cooling requirements. Cisco states that Cisco ACE equipment can reduce the provisioning time required for new applications by up to 70 percent as well as lower ongoing management time and TCO. Cisco ACE licensing is also intended to allow IT managers to select and pay for only the level of capability that they require for a specific data center solution. The following list shows the

granularity of the performance levels and functions that characterizes the Cisco ACE scalable licensing model for the Cisco ACE Module:

- Cisco ACE Module: Includes 1000 transactions per second (TPS) SSL and five virtual partitions (default)
- Cisco ACE 4-Gbps throughput license: Mandatory
- Cisco ACE 8-Gbps throughput license: Optional
- Cisco ACE 16-Gbps throughput license: Optional
- Cisco ACE upgrade license from 4 to 8 Gbps: Optional
- Cisco ACE upgrade license from 8 to 16 Gbps: Optional
- Cisco ACE 5000 SSL TPS license, upgradeable to 10,000 and 15,000: Optional
- Cisco ACE 20 virtual contexts license: Optional
- Cisco ACE 50 virtual contexts license: Optional
- Cisco ACE 100 virtual contexts license: Optional
- Cisco ACE 250 virtual contexts license: Optional
- Cisco ACE upgrade license from 20 to 50 virtual contexts: Optional
- Cisco ACE upgrade license from 50 to 100 virtual contexts: Optional
- Cisco ACE upgrade license from 100 to 250 virtual contexts: Optional
- Cisco ACE security feature set license: Optional

Ease of Deployment and Management

Description of the Criteria

As with any component of the network or the data center, an AFE solution should be relatively easy to deploy and manage. It should also enable new applications to be relatively easily deployed and managed, and so ease of configuration management is a particularly important consideration when the data center supports a wide diversity of applications. As is the case with a number of the criteria in Table 1, ease of deployment and management should be tested by IT organizations as part of their evaluation of AFEs.

Evaluation of Cisco ACE

Cisco ACE facilitates ease of deployment and management through device virtualization, RBA, and software configuration rollback. Virtualization has already been discussed. The RBA feature allows organizations to specify administrative roles and control administrator access to specific functions within the module or virtual partitions. As a result, Cisco ACE offers centralized control together with decentralized configuration management using template-based or customizable user permissions for each virtual partition. Template-based configuration and auditing complement service activation and suspension capabilities to facilitate provisioning of new applications.

RBA reduces application deployment times by allowing a single device to support multiple applications and application instances that can be used in parallel by multiple departmental stakeholders. This architecture also reduces TCO by simplifying application provisioning and ongoing management for IT teams, enabling multiple departments or stakeholders to

independently manage appropriate, role-assigned tasks. Cisco states that these capabilities reduce the time to provision a new application by 70 percent.

Using software configuration rollback, the IT administrator can roll back any virtual device to a previous configuration. This capability also allows the IT administrator to easily save an instance of an application in service from one virtual device and gracefully reuse it as new instances of existing applications are deployed in other virtual devices, all without affecting any other applications serviced by the device.

Summary

As shown in market research that Ashton, Metzler & Associates recently published², the deployment of AFEs should increase significantly in the near future. Given the critical nature of AFEs, IT organizations that are evaluating this class of products need to use a structured process. As part of that process, IT organizations should develop a set of decision criteria similar to the set displayed in Table 1.

The criteria displayed in Table 1 were used to analyze Cisco ACE. This analysis showed that Cisco ACE has a number of strengths, including the following:

- **Performance:** Cisco ACE is one of the best performing AFEs available in the marketplace. It can process application traffic at up to 64 Gbps, and it can support more than a million Layer 4 setups and teardowns per second.
- **Virtualization:** Cisco ACE supports up to 250 virtual AFE devices on a single physical Cisco ACE Module. This level of virtualization lowers TCO because it results in fewer devices to install and manage. Virtualization also results in higher availability because with a virtual AFE mapped to a virtual machine, the AFE does not need to be reconfigured when an application is moved or automatically fails over to a new physical machine. Ashton, Metzler & Associates is not aware of any other AFE that has a virtualized architecture.
- **Transparency and integration:** With its presence in the enterprise networking market, Cisco is in a unique position to help ensure that its solutions do not break anything such as routing, security, or QoS. Cisco is also in a unique position to help ensure that the Cisco ACE integrates with the existing networking infrastructure.
- **Scalability and architecture:** Cisco provides the capability to expand the Cisco ACE incrementally to support 64 Gbps. Cisco provides this scalability through software license upgrades. This architecture tends to reduce the need for new hardware and hence minimizes the application downtime and degradation associated with hardware-centric capacity upgrades.
- **Security:** Security remains a crucial concern for nearly all IT organizations. All Cisco ACE models contain integrated firewall capabilities. The Cisco ACE Data Center Firewall feature performs both Layer 3 access-control filtering and Layer 7 deep packet inspection (DPI) to identify anomalous signatures that could cause DoS. The Cisco ACE Application Firewall feature prevents day-zero attacks by identifying and blocking suspicious traffic for which there is no known malicious signature already identified and stored in a database to match. Cisco ACE also secures XML applications, Web-services, and intra-application communications.

² Application Delivery Handbook, p. 29, www.kubernan.com