

# Cisco Application Control Engine: A Technical Overview of Virtual Partitioning

Virtualization of the network is paramount for companies to successfully roll out the applications required for today's business services. The Cisco® ACE Application Control Engine Module provides a robust virtualization solution for Layer 4–7 services to meet the growing needs of today's data center. This paper discusses the benefits of using the virtual partitions of the Cisco ACE to deploy data center solutions.

## Scope

This paper describes the benefits of virtualization, what to consider before implementation, and implementation guidelines. You will learn how to effectively configure the Cisco ACE Application Control Engine Module to help ensure the best service to end users by taking advantage of its scalability, availability, and failover features with the added benefits of virtual partitioning.

## Audience

This document is intended as a technical reference for networking professionals familiar with content switching and network design, who are interested in learning how to implement virtual partitions within the Cisco ACE module.

## Industry Challenges

Traditional data centers consist of Layer 2–3 networking devices as well as Layer 4–7 devices such as load balancers and intra-DMZ firewalls. These devices can be shared or dedicated to operational groups, business units, or application tiers. Deployment practices depend on organizational business structures and the requirements of service and application infrastructures. Data centers tend to develop a variety of deployment and operational inefficiencies as traditional solutions must scale to meet new business requirements:

- New services require new physical deployments, new qualification cycles, and dedicated resources
- New physical deployments entail additional cabling and power requirements
- Deployments are often slowed by complex coordination in workflow
- Additional operational overhead is required to manage and maintain separate physical network devices
- Equipment is often underutilized

## Impact to the Organization

Deploying new services requires either additional equipment provisioning for a dedicated solution, or coordination with one or more internal groups in a shared environment. The latter can lead to delays in deployment and additional risks to production systems. In either scenario, many businesses deploy multiple product solutions, often from multiple vendors. In addition, working with multiple products requires additional time to set up, test, and validate candidate applications prior to production rollout. Delays in this process can easily exceed the cost of the physical components and lead to increased ongoing operational costs.

Other factors that drain IT budgets include:

- Complex design, requiring multiple devices per service
- Highly skilled, costly resources required to manage and maintain application design
- Expensive application infrastructure
- Complex workflow involving multiple groups within the organization
- Delays in reacting to new business requirements
- Stocking spares

Even in environments where the deployment process has matured, there are cost inefficiencies resulting from standard capacity-planning practices. To allow for scalability, network devices are only 60 to 75 percent utilized in ideal scenarios. Taken as a single instance this is a recommended practice; however, as the designs scale and business requirements change on a regular basis, the percentage of unused resources can exceed whole devices. For example if there are four load balancers deployed in the data center, all at the ideal 75 percent utilization, the equivalent of a dedicated load balancer remains unused. By using virtual partitioning, these four load balancers can share the same physical device and the same reserve for future growth.

## Cisco Solution

The Cisco ACE Application Control Engine Module provides a virtualization solution for secure application delivery. Although the module can be used as a traditional single-user device, the real benefits to the data center reside within the module's virtual partitioning. The virtual partitioning provides complete separation of configuration, disk space, and traffic handling. A virtual partition is the virtual instance of the Cisco ACE module, where the configuration and statistics for the virtual partition reside. The virtual partition defines how traffic is classified and which actions are taken on the classified traffic. VLANs are allocated per virtual partition to provide each virtual partition with its own well-defined input/output access. The module employs an innovative resource allocation manager to control system resources based on rates and memory utilization per virtual partition. The resource allocation manager defines the performance, capacity, and scalability of each virtual partition. These resources can be allocated in three ways: fixed, oversubscription, and "free-for-all."

This comprehensive virtualization solution allows the Cisco ACE module to meet the needs of many different customer deployments. Virtual partitions can mirror the current network operation structure, align with a company's business model, be deployed to provide a managed/unmanaged service, and so forth. The use of virtualization allows the 4G, 8G, or 16G Cisco ACE module, with its industry-leading throughput, connections per seconds, and other resources, to be divided into

logical virtual partitions to support multiple applications within a data center, while adding security between tiers of applications.

The virtualization solution allows you to combine your shared and dedicated environments into one device. This consolidation can be achieved easily by integrating the Cisco ACE module into your existing network architecture. After installing the Cisco ACE module in a Cisco Catalyst® 6500 Series Switch, you can allocate existing VLANs to the module using VLAN groups. Within the module, these VLANs can be allocated to the appropriate virtual partitions. This approach helps ensure complete VLAN separation between the virtual partitions within the Cisco ACE module.

As VLANs are allocated to virtual partitions, resource classes may also be applied to the virtual partitions. A resource class defines how the Cisco ACE module's resources are allocated to a virtual partition. The resource class defines the capacity and scalability of a given virtual partition for handling client traffic. This innovation allows the Cisco ACE module to apply software constraints on virtual partitions and to grow or reduce the capacity of a given virtual partition in real time in production networks. The module supports up to 100 unique resource classes that can be shared across all 250 virtual partitions. The granular control of resource allocation allows for the exact fit of resources combined with traffic and management separation to meet the requirements of any data center.

For high availability, Cisco ACE module pairs can be deployed as a statefully redundant solution in either active-standby or active-active designs, either within the same Cisco Catalyst chassis or, more commonly in redundant data center designs, across two distinct chassis. The Cisco ACE module provides stateful high availability per virtual partition, and has the capability to group virtual partitions to allow for nearly instant application service failover. Redundancy per virtual partition permits you to use both Cisco ACE modules actively and to granularly control primary data flows through the data center network.

In addition to providing resource-controlled virtualization and stateful redundancy, the Cisco ACE module offers innovative network device management using Application Infrastructure Control. Application Infrastructure Control allows:

- Users to be created per virtual partition and/or across virtual partitions
- Roles to be defined within a virtual partition to allow user access to Cisco ACE module functionality
- Users to be associated with domains to constrain the user's access to a subset of the configuration within the virtual partition

The Application Infrastructure Control complements the Cisco ACE module's virtualization to provide a complete virtualization solution. Furthermore, the module supports a fully developed XML API with XML Document Type Definition (DTD), which is integrated with the Application Infrastructure Control. This allows any user access to the XML API, while providing the same user functionality, protection, and constraints that are found in the command-line interface (CLI). To round out management, the Cisco ACE module supports virtualized syslogs, MIBs, SNMPv1, v2c, and v3, and the Application Network Manager for graphical management.

## Business Benefits

**Consolidation:** One physical device can be partitioned to multiple systems, resulting in fewer high-performance devices, mixed test and production environments on the same hardware, and consolidation of server load balancing (SLB) between tiers.

**Resources:** Resources are guaranteed for critical applications, with support for over-subscription. Resources can be quickly and easily shifted to the workload (partition) that requires them. This improves utilization of the data center's physical infrastructure (power, cables, rack space, etc.).

**Availability:** Partitions are completely independent; any misconfiguration of a partition does not affect the operation of other partitions. Virtualized partitions can be set up with high availability across multiple devices.

**Increased utilization of network resources:** Provides more profitable return on the network investment.

**Management:** The Cisco ACE module enables simplified configuration per partition, provisioning through XML API, Layer 7 policies delegation to applications teams, and configuration validation on a test partition before production rollout.

**Security:** Secured/critical application isolation, and simplified and centralized configuration are easily attained with the Cisco ACE module.

## Considerations for Implementation

Prior to deploying the Cisco ACE module in the network, you should consider how to implement virtual partitions and resources. There are very clear recommendations as to how to initially allocate resources; however, virtual partitioning will require more reflection on how virtualization can best benefit a given environment.

To accommodate scaling and capacity planning, new Cisco ACE module installations should not exceed 60 to 80 percent of the device's total capacity. When initially planning resource allocation, consider creating a reserved resource class in the module with a fixed resource class of 5 to 10 percent of all module resources. Plan to create a reserver virtual partition dedicated to ensuring these resources are reserved. Resources, reserved in this manner, can be dynamically distributed to other virtual partitions as capacity demands for handling client traffic increase over time.

When planning the initial resource allocations for the virtual partitions, allocate only the minimal required or estimated resources. The Cisco ACE module protects resources in use, thus to decrease a virtual partition's resources, those resources must be unused. Although it is possible to decrease the resource allocations in real time, it may require additional management overhead to clear any used resources before reducing them. Thus it is a best practice to initially keep as many resources in reserve as possible and allocate the unused reserved resources as needed.

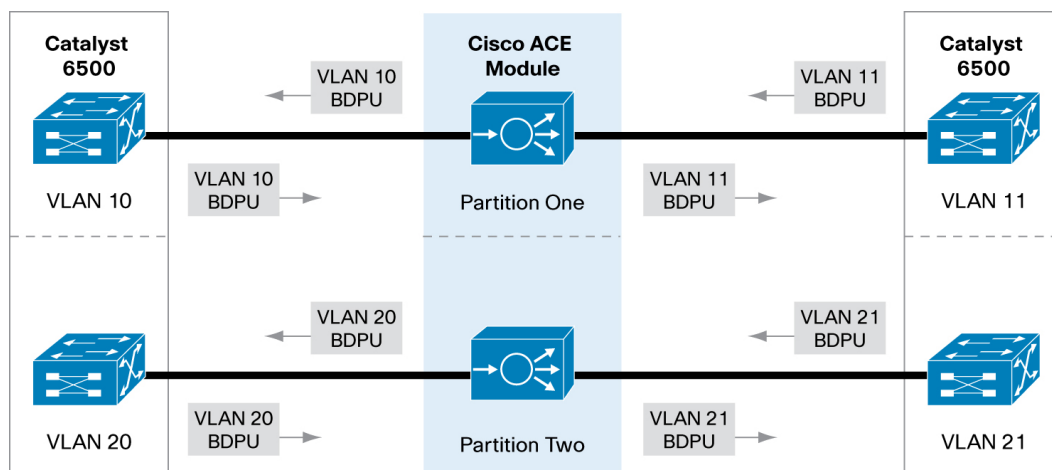
The Cisco ACE module allows you the flexibility to deploy virtual partitions based on tier applications, function (security, load balancing, application optimization, and so forth), internal organizational structure, alignment with client businesses, and so on. The type and extent of virtualization used will impact the way resource classes are created and likely the use of application infrastructure control. Although there may not be a single best way to virtualize the Cisco ACE module, its flexibility will allow you to more effectively align your network resources with your business.

High-availability designs may require virtual partitioning, especially when two Cisco ACE modules are used actively. The high-availability Cisco ACE solution is used on a per-virtual-partition basis. In a traditional active/standby high-availability design, the primary Cisco ACE module is active and all the virtual partitions within the primary module are active. If the primary module or a virtual partition fails, the backup module will take over and all virtual partitions will move to the backup module. In an active/active high-availability design, both the primary and backup Cisco ACE modules are active simultaneously. The active virtual partitions are distributed across both modules, such that approximately half are active on the primary module and the remaining are active on the backup module. In the event of a virtual partition failure, the backup virtual partition will take over on the opposite module. In the event of a module failure, all previously active virtual partitions will fail over to the remaining active module. With this design it is imperative to never exceed 100 percent capacity for a single Cisco ACE module within a highly available module pair to avoid oversubscription during an HA event.

Another consideration in an active/active high-availability design, when deployed across two Cisco Catalyst 6500 Series Switches, is the impact of a virtual partition failure to potential trunk traffic between the switches. The Cisco ACE module provides tracking mechanisms within the failover technology to allow multiple virtual partitions to be grouped together. In the event that one virtual partition fails, all the virtual partitions supporting the same application or service can be transitioned to the backup module. This can prevent trunks between the Cisco Catalyst switches from becoming oversubscribed in the event of a partial application failover, due to a single virtual partition failure.

As plans for the overall virtualization design begin to solidify, consider how the usage of VLANs could effect virtual partition allocations. There are three designs that impact how VLANs are allocated: bridge mode, routed mode, and cascading virtual partitions. When a virtual partition is configured for bridging, the integration of the Cisco ACE module with the Cisco Catalyst 6500 Spanning Tree Protocol prevents unexpected bridge loops by preventing the bridged VLANs from being shared across virtual partitions.

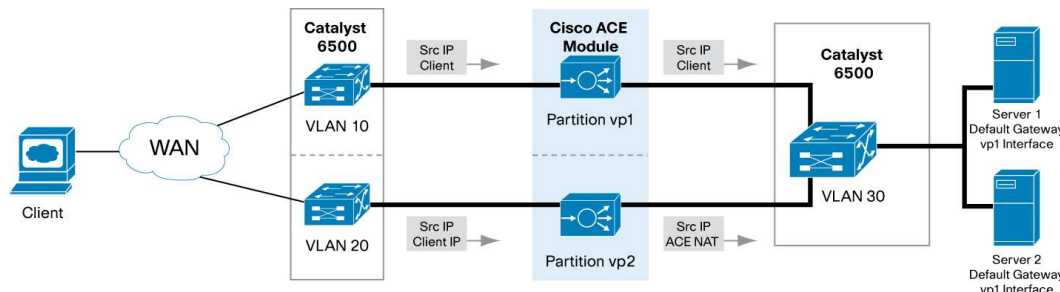
**Figure 1.** BDPU Handling in Bridge Mode with multiple virtual partitions



To provide scalability, the Cisco ACE module allows you to configure multiple bridged VLAN pairs and to add additional VLANs for routing within a single virtual partition. In a routed design VLANs can be freely shared; however, if the server VLAN is to be shared between two or more virtual partitions it could require using source Network Address Translation (NAT) for the load-balanced traffic and applying static routes on the servers. For example servers using the Cisco ACE

module's virtual partition vp1 as a default gateway will require the Cisco ACE module to perform source NAT for client traffic from vp2 to a unique subnet. Then static routes must be applied to the real server to force responses back to vp2.

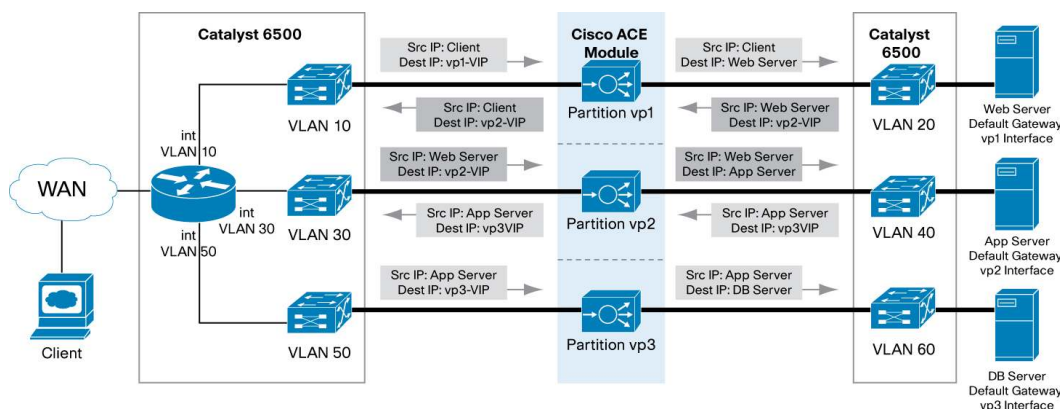
**Figure 2.** Controlling server response using source NAT



Although often not required, altering the source address enables the Cisco ACE module to control the return flows in a variety of complex deployments. Companies needing to meet regulations requiring audit trails may need to reconsider sharing server VLANs. By obscuring the true client IP address from the server, clear audit trails become difficult to deploy to meet regulation standards.

In the cascading virtual partitions design (Figure 3), client traffic flows from vp1 for Web traffic, then to vp2, for applications, and then to vp3 for database transactions. Tiered designs require separate client networks for each virtual partition within the Cisco ACE module. Tiered designs are common in Cisco ACE module deployments. The one requirement of tiered virtual partitions is there must be a Layer 3 hop between the virtual partitions. Most designs use the Multilayer Switch Feature Card (MSFC), Virtual Route Forwarding (VRF) instances, or Firewall Services Module (FWSM) within the Cisco Catalyst 6500 Series Switch as the routing interface between virtual partitions.

**Figure 3.** Tiered Design with Cascading Virtual Partitions



Lastly, the Cisco ACE module offers five virtual partitions by default. If you plan to migrate existing services over to the module in a tradition single-partition design, to keep the migration simple and straightforward, consider taking advantage of the free virtual partitions as new projects develop and as the data center continues to expand in the future.

To summarize the considerations for implementation:

- Reserve 5 to 10 percent of Cisco ACE module resources for future scaling
- Do not plan for too much capacity during the initial rollout

- Match virtual partition usage to purpose or business
- Consider virtualization based on applications, function (security, SLB, application optimization), business organization, or client business
- Regardless of the extent of virtualization implemented, consider the impact of a high-availability design
- When planning virtual partition allocation, consider VLAN usage requirements per virtual partition
- Five free virtual partitions are available by default; do not hesitate to use them

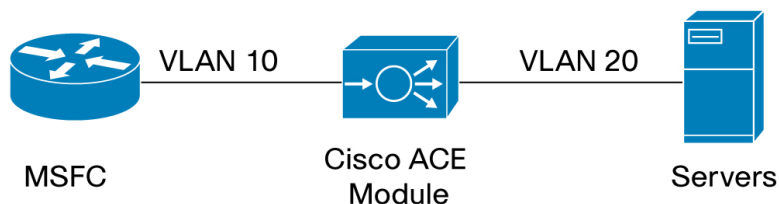
### Designing the Network Architecture

The Cisco ACE module easily integrates into the Cisco Catalyst 6500 Series Switches and Cisco 7600 Series Routers running native Cisco IOS® Software Release 12.2(18)SXF4<sup>1</sup> or later. Although details of the Cisco ACE module integration with the Cisco Catalyst 6500 Series are outside the scope of this document, it is important to know that the module can take advantage of port awareness and security provided by the Cisco Catalyst 6500 Series through integration with features such as autostate and private VLANs. The Cisco ACE module adds value to the Cisco Catalyst 6500 Series by providing VRF-aware Route Host Injection. Look for details on these topics in other Cisco ACE documentation and on Cisco.com.

The initial step to deploy the Cisco ACE module into a network is to allocate the VLANs that the module will use from the Cisco Catalyst 6500 Series. There is a new Cisco IOS command to allocate VLANs called “svclc” (service line card). The svclc command is used to allocate VLANs to VLAN groups and to apply the VLAN groups to the Cisco ACE module. There is an additional command “svclc multiple interfaces” which must be used when allocating multiple Layer 3 VLANs (MSFC routed Switch Virtual Interfaces [SVIs]) to a Cisco ACE module. This command brings awareness of potential routing loops that could occur if the VLANs are improperly configure within the Cisco ACE Module.

In a simple scenario, when the MSFC is sharing VLANs with the Cisco ACE modules, the basic VLAN structure is as follows (See Figure 4).

**Figure 4.** VLANs Shared Between Cisco Catalyst 6500 Series MSFC and Cisco ACE Module



VLAN Names	Common names for Data Center VLANs	VLAN ID
<b>Public VLAN</b>	Cisco ACE Client VLAN	VLAN 10
<b>Private VLAN</b>	Cisco ACE Server VLAN	VLAN 20

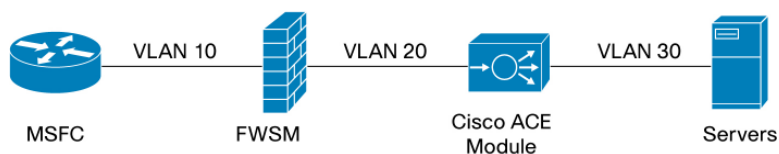
In this example VLANs 10 and 20 need to be allocated to the Cisco ACE module:

<sup>1</sup> Please see the Cisco ACE Application Control Engine Module release notes for complete hardware and software compatibility.

```
svclc multiple-vlan-interfaces
svclc module 1 vlan-group 7
svclc vlan-group 7 10,20
```

When allocating VLANs to a VLAN group, be aware that a specific VLAN can only be allocated to one VLAN group. This requirement can dictate the use of multiple VLAN groups. In the common scenario with both the Cisco Catalyst 6500 Series FWSM and Cisco ACE modules, the basic VLAN structure is as follows (Figure 5):

**Figure 5.** VLANs Shared Between Cisco Catalyst 6500 Series MSFC, Cisco Firewall Services Module, and Cisco ACE Module



VLAN Names	Common names for Data Center VLANs	VLAN ID
<b>Internet Facing VLAN</b>	FWSM outside	VLAN 10
<b>DMZ VLAN</b>	FWSM inside	VLAN 20
<b>DMZ VLAN</b>	Cisco ACE client VLAN	VLAN 20
<b>Private VLAN</b>	Cisco ACE server VLAN	VLAN 30

In this example intuitively VLANs 10 and 20 need to be allocated to the FWSM and VLANs 20 and 30 allocated to the Cisco ACE module. Due to the VLAN group constraint, an additional VLAN group must be allocated for the shared VLAN between the FWSM and Cisco ACE modules.

```
svclc multiple-vlan-interfaces
firewall module 1 vlan-group 3
firewall module 1 vlan-group 5
svclc module 2 vlan-group 5
svclc module 2 vlan-group 7
firewall vlan-group 3 10
firewall vlan-group 5 20
svclc vlan-group 7 30
```

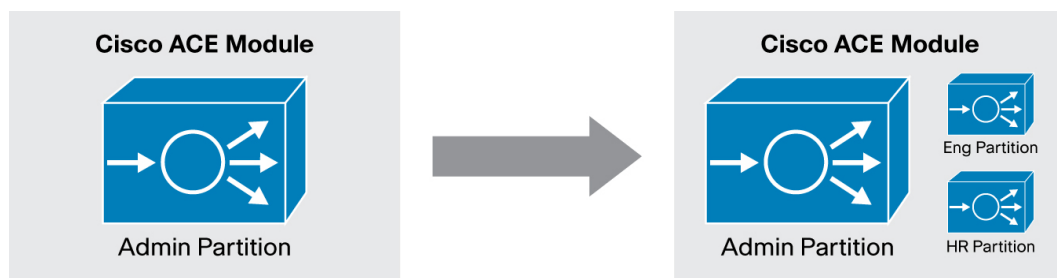
Notice either firewall or svclc commands can be used to define a VLAN group. However, the firewall command must be used to allocate VLAN groups to a FWSM, and the svclc command must be used to allocate VLAN groups to a Cisco ACE module. Once VLANs have been allocated to the module, the process of virtualization and resource allocation can begin.

Each Cisco ACE module has a single virtual partition, created by default, which is known as the Admin virtual partition. This partition is a member of the default resource class. The default resource class has no defined minimal resources, and is permitted to use any available resources. All VLANs allocated to the module are accessible in the Admin virtual partition. These default settings allow the Admin virtual partition to be used when operating the Cisco ACE module in a traditional single-use and single-purpose design.

In a virtualized configuration the Admin virtual partition is used to create new virtual partitions and dedicate client and server VLAN traffic to the appropriate virtual partitions (Figure 6). This way you

can deploy the Cisco ACE module in a single-use design and then add new virtual partitions as needed.

**Figure 6.** Admin Virtual Partitions



Although the Admin virtual partition is designed to have all the functionality of other virtual partitions, it has four main functions in addition to those found in regular virtual partitions.

- Creation of other virtual partitions (only the Admin virtual partition can do this)
- Creation and application of resources classes
- Allocation of VLANs to virtual partitions
- The configuration of fault tolerance for high-availability deployments

Within the Admin virtual partition there is a default account known as the admin. The admin account has complete access to all Cisco ACE commands and access to any virtual partition created with the Cisco ACE module. The module allows user accounts to be created in any virtual partition. There are two privileges granted to users specifically defined within the Admin virtual partition. First, these users are the only users who have access to the `changeto` command, which allows them to easily change between virtual partitions within the Cisco ACE module. Second, any user granted an Admin role within the Admin virtual partition will have system-wide privileges similar to the admin account. Further information regarding Role-Based Access Control (RBAC) can be found in other Cisco ACE module implementation guides.

The Cisco ACE module allows for various system resources to be allocated at the same or varying levels. The resource allocations are grouped in user-defined classes. Any virtual partition that is a member of the resource class will receive the resources as defined by the class. Table 1 lists the resources that the Cisco ACE module can allocate and the upper limit per module.

**Table 1.** Resource Allocations

Resource Metric	Description	System limit
<b>ALL</b>	Allows all Cisco ACE resources* to be allocated with a single command	
<b>ACL Memory</b>	Maximum ACL memory	75 MB
<b>Concurrent Connections</b>	Maximum concurrent connections (through-the-box traffic) (conn objects)	4 million (8 million)
<b>Management Connections</b>	Maximum management connections (to-the-box traffic)	5000
<b>Proxy Connections</b>	Maximum proxy connections (L7 connection objects)	512,000 (1 million)
<b>Regular Expressions</b>	Maximum amount of regular expression memory	1 MB
<b>Sticky Entries</b>	Maximum number of sticky entries	4 million
<b>Translations (xlates)</b>	Maximum number of translation entries	1 million
<b>Resource Buffers</b>		

<b>Syslog Buffer</b>	Limit amount of buffering for Syslog Messages	4 Million
<b>Resource Rates</b>		
<b>Bandwidth</b>	Maximum bandwidth in bytes per second	4/8/16 Gbps
<b>Connections</b>	Maximum connections per second (CPS)	348,000 CPS
<b>Inspected Connections</b>	Maximum inspected connections per second	6000 CPS
<b>Mac-miss</b>	Maximum MAC miss traffic (punted to-the-box) in packets per second	2000
<b>Management Traffic</b>	Maximum management traffic (to-the-box) in bytes per second	1 Gbps
<b>SSL Conn Rate</b>	Maximum number of SSL transactions per second	1000/5000/10,000/15,000
<b>Syslog</b>	Maximum syslog messages per second	358K dataplane
<b>Bandwidth</b>	Maximum bandwidth in bytes per second	4/8/16 Gbps

\* The sticky resource must be specifically allocated to each class requiring sticky resources. Because the default resource class does not allocate resources for sticky, this needs to be done manually if persistence is required.

The Cisco ACE module supports up to 100 unique resource classes. Any resource class can be applied to any single virtual partition or all virtual partitions if resources are available for allocation. There are three ways to allocate individual resources within a resource class:

- Fixed: Minimally allocate x% and maximum may not exceed x%.
- Oversubscription: Minimally allocate x% with the option to use any available resources.
- Free-for-all: Any available resource can be used, but no minimal allocations are defined.

Rate-limited resources are reserved by the Cisco ACE module when allocated to a virtual partition. This allocation method can either be assigned to help ensure a virtual partition has enough resources to properly handle client traffic, or to help ensure a virtual partition does not exhaust resources that are used in other virtual partitions. To configure a rate-limited resource, define the guaranteed value as the minimum limit and configure the maximum limit as “equal-to-min.”

```
ACE/Admin(config)# resource-class 10-guaranteed
ACE/Admin(config-resource)# limit-resource all min 10 maximum equal-to-min
```

Resources can be allocated to allow oversubscription in scenarios where a virtual partition is required to perform at a minimum level and may need to draw upon additional resources during peak times. When configuring a resource for oversubscription, define the guaranteed value as the minimum limit and configure the maximum limit as “unlimited.”

```
ACE/Admin(config)# resource-class 15-plus
ACE/Admin(config-resource)# limit-resource all min 15 maximum unlimited
```

Use the free-for-all allocation to allow fair competition for resources between virtual partitions. By default all resources (except sticky) are allocated to the “default-class.” By default this class is applied to all new virtual partitions when the virtual partition is created. To configure a free-for-all allocation of a resource, define the minimum limit as zero and configure the maximum limit as “unlimited.”

```
ACE/Admin(config)# resource-class any-available
```

```
ACE/Admin(config-resource)# limit-resource all min 0 maximum unlimited
```

Resources are not reserved until they are allocated to virtual partitions. As resources are allocated, the minimum value is tallied to prevent oversubscription of guaranteed resources. If a resource is allocated to a virtual partition and the allocation would require more than 100 percent of the module resources to be available, the Cisco ACE module will prevent the allocation from being made by issuing a CLI error.

```
ACE/Admin(config)# resource-class all-resources
ACE/Admin(config-resource)# limit-resource all min 99 maximum equal-
to-min
ACE/Admin(config-resource)# virtual partition app-tier
ACE/Admin(config-virtual partition)# member all-resources
Error: resources in use
```

When resources are applied as either guaranteed or oversubscription allocations, the Cisco ACE module checks to ensure the total minimum value for the applied resources does not exceed 100.

```
ACE/Admin(config)# resource-class 10-guaranteed
ACE/Admin(config-resource)# limit-resource all min 10 maximum equal-
to-min
ACE/Admin(config-resource)# virtual partition web-tier
ACE/Admin(config-virtual partition)# member 10-guaranteed
ACE/Admin(config-resource)# virtual partition web-tier
ACE/Admin(config-virtual partition)# member 10-guaranteed
ACE/Admin(config)# resource-class 10-guaranteed
ACE/Admin(config-resource)# limit-resource all min 99 maximum equal-
to-min
Error: checking resource parameter limit failed
```

Resource allocations can be added to resource classes individually or all of them may be added.

```
ACE-Pod3/Admin(config)# resource-class half
ACE-Pod3/Admin(config-resource)# limit-resource all minimum 50 maximum
equal-
to-min
```

If all resources are allocated to a class, any additional limits override those made when adding all resources to a class. For example if one were to limit certain resource metrics individually and then limit all resources, the metrics added individually would be preserved.

```
ACE/Admin(config)# resource-class HR-Dept
ACE/Admin(config-resource)# limit-resource sticky minimum 35 maximum
equal-to-min
ACE/Admin(config-resource)# limit-resource regexp minimum 40 maximum
unlimited
ACE/Admin(config-resource)# limit-resource rate connections minimum 20
maximum
equal-to-min
ACE-Pod3/Admin(config-resource)# limit-resource all minimum 25 maximum
equal-to-
min
```

The Cisco ACE module provides a default class where all resource metrics (except the sticky resource) apply with a free-for-all allocation (no minimum guarantee, and a maximum of unlimited) to newly created virtual partitions. The sticky resource must be defined separately to a resource class and the resource class applied to the virtual partition to enable a virtual partition to provide client connection persistence. Thus any virtual partition not requiring client persistence can use the default virtual partition, while a virtual partition requiring persistence (sticky) will need to be configured as a member of a resource class, where the sticky resource is well defined.

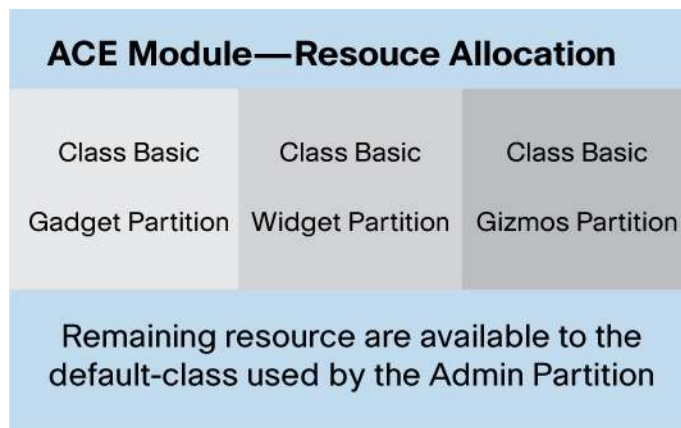
```

ACE/Admin(config)# resource-class shopping-carts
ACE/Admin(config-resource)# limit-resource sticky minimum 1 max equal-to-min
ACE/Admin(config-resource)# limit-resource all minimum 0.00 maximum unlimited
ACE/Admin(config-resource)# exit

ACE/Admin(config)# virtual partition Ecommerce
ACE/Admin(config-virtual partition)# allocate-interface vlan 20
ACE/Admin(config-virtual partition)# allocate-interface vlan 30
ACE/Admin(config-virtual partition)# member shopping-cart
    
```

Once resource classes are defined, they can be applied to a virtual partition by configuring the virtual partition as a member of an existing resource class. When a virtual partition is made a member of a resource class, the minimum resources for the class are pulled from the available resources within the Cisco ACE module. Thus if three different virtual partitions are each members of the same resources class, there are three resources allocations made, one for each virtual partition. It is important to note that a single resource class is not sharing resources between all class members. Rather each member is allocated its own distinct resources as defined by the resource class. Figure 7 shows how a class of resources is allocated for each virtual partition that is added as a member of the class. Virtual partitions are not in contention for the resources defined by a resource class.

**Figure 7.** Resource Allocation



If there are not enough resources to meet the minimal requirements defined in the resource class, the Cisco ACE module will issue an error upon adding a virtual partition as a member of the resource class.

```

ACE/Admin(config)# resource-class max
    
```

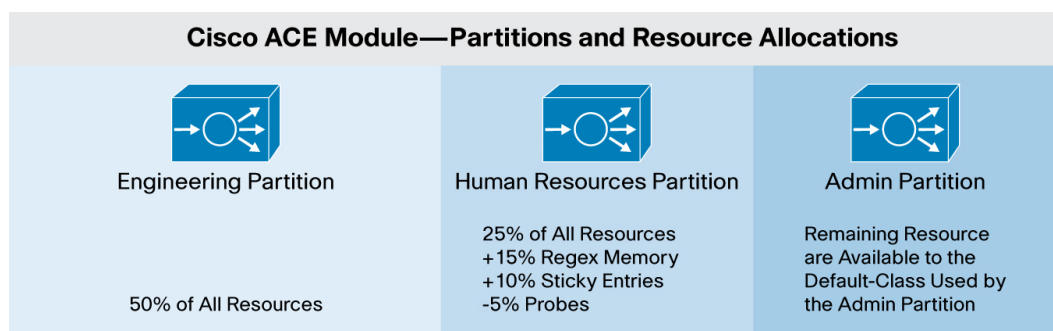
```
ACE/Admin(config-resource)# limit-resource all min 99 maximum equal-
to-min
```

```
ACE/Admin(config-resource)# virtual partition example
ACE/Admin(config-virtual partition)# member max
Error: resources in use
```

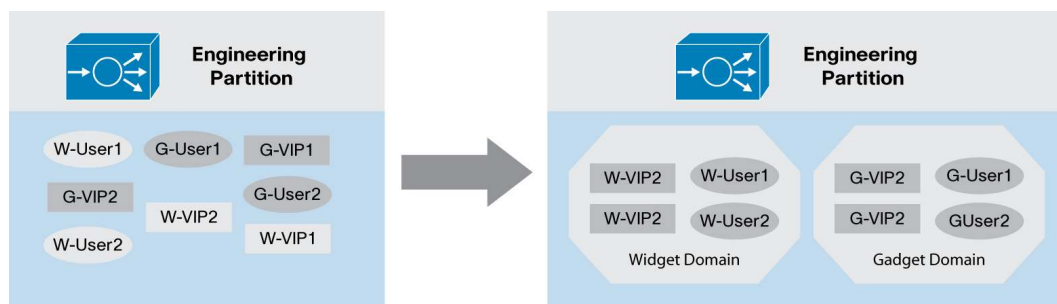
If this occurs deallocate resources from the reserve virtual partition to free-up enough resources to add the new virtual partition. If the reserve virtual partition is depleted or was not provisioned during the initial deployment, the difference in available and minimally required resources will need to be acquired from the existing virtual partitions. This can be done dynamically by modifying the minimal limits within the other resource classes or lowering the minimal requirements for the resource class that is being applied. If more resources are required, then you can investigate migration of specific virtual partitions to a separate Cisco ACE module, within the same chassis. Up to four Cisco ACE modules are supported within the Cisco Catalyst 6500 Series Switch.

The flexibility of the resource-allocation mechanism in the Cisco ACE module allows a wide range of resource control per virtual partition (Figure 8).

**Figure 8.** Virtual Partitions and Resource Allocations



In addition to using multiple virtual partitions to align with service management groups, enterprise business units, and so forth, the Cisco ACE module provides domains to further subdivide any virtual partition. Domains are designed to allow division between departments, workgroups, or any other logical grouping for managing client requests to application services within a given virtual partition. Essentially a domain is a logical group of configured objects, and the domain's intent is to limit the access of these objects to a defined set of users. A common scenario for an enterprise is when an engineering group is assigned a virtual partition to contain all of the engineering services. Within this engineering group there are two groups called widgets and gadgets. Rather than having to create a new virtual partition for each group, domains can be assigned to the widget and gadget services and to the respective user account supporting either widgets or gadgets services.

**Figure 9.** Cisco ACE Module Domains

Remember that a virtual partition is implemented using the keyword `virtual partition` within the Cisco ACE module command-line interface (CLI). The virtual partition is the main component of the Cisco ACE virtualization. The separate Cisco ACE configurations and various files associated with them are stored within a virtual partition. The virtual partition defines the configuration, stores files, permits users access, and allocates domains. From within the Admin virtual partition, any user who is a member of the Admin role can create additional virtual partitions. Before a new virtual partition can be created, the admin of the default Admin virtual partition must ensure that the VLANs to be allocated to the new virtual partition are allowed from the Cisco Catalyst 6500 Series Supervisor Engine to the Cisco ACE module. The admin must also ensure that the resource class required for the virtual partition is created and configured to allow the correct resource allocations. Once these prerequisites are met, a new virtual partition can be created.

```
ACE/Admin(config)# virtual partition Eng
ACE/Admin(config-virtual partition)# description "Engineering
Services"
ACE/Admin(config-virtual partition)# allocate-interface vlan 10
ACE/Admin(config-virtual partition)# allocate-interface vlan 40
ACE/Admin(config-virtual partition)# member department
ACE/Admin(config-virtual partition)# exit
ACE/Admin(config-virtual partition)# do show run virtual partition
Generating configuration....
```

```
virtual partition Eng
  description Engineering Services
  allocate-interface vlan 10
  allocate-interface vlan 40
```

After a virtual partition is created, the virtual partition will appear as though it were a unique physical device. From within the virtual partition each virtual partition can be configured with its own unique parameters for management such as service policy for management access, ACLs, AAA, syslog, and for load balancing client traffic. In the Admin virtual partition the virtualization allocations can be viewed for each resource class, whereas from within a given virtual partition you can only see the resource allocation for that specific virtual partition.

ACE/Admin# show resource allocation

```

-----
-----
Parameter                Min      Max      Class
-----
-----
acl-memory                0.00%   500.00%  default
                        25.00%   25.00%   reserved
                        8.00%    8.00%    basic
                        50.00%   50.00%   department

syslog buffer             0.00%   500.00%  default
                        25.00%   25.00%   reserved
                        8.00%    8.00%    basic
                        50.00%   50.00%   department

conc-connections         0.00%   500.00%  default
                        25.00%   25.00%   reserved
                        8.00%    8.00%    basic
                        50.00%   50.00%   department

mgmt-connections        0.00%   500.00%  default
                        25.00%   25.00%   reserved
                        8.00%    8.00%    basic
                        50.00%   50.00%   department

proxy-connections       0.00%   500.00%  default
                        25.00%   25.00%   reserved
                        8.00%    8.00%    basic
                        50.00%   50.00%   department

bandwidth                 0.00%   500.00%  default
                        25.00%   25.00%   reserved
                        8.00%    8.00%    basic
                        50.00%   50.00%   department

connection rate          0.00%   500.00%  default
                        25.00%   25.00%   reserved
                        8.00%    8.00%    basic
                        50.00%   50.00%   department

inspect-conn rate        0.00%   500.00%  default
                        25.00%   25.00%   reserved
                        8.00%    8.00%    basic
                        50.00%   50.00%   department

```

syslog rate	0.00%	500.00%	default
	25.00%	25.00%	reserved
	8.00%	8.00%	basic
	50.00%	50.00%	department
regex	0.00%	500.00%	default
	15.00%	25.00%	reserved
	8.00%	8.00%	basic
	75.00%	75.00%	department
sticky	0.00%	500.00%	default
	25.00%	25.00%	reserved
	8.00%	8.00%	basic
	50.00%	50.00%	department
xlates	0.00%	500.00%	default
	25.00%	25.00%	reserved
	8.00%	8.00%	basic
	50.00%	50.00%	department
ssl-connections rate	0.00%	500.00%	default
	25.00%	25.00%	reserved
	8.00%	8.00%	basic
	50.00%	50.00%	department
mgmt-traffic rate	0.00%	500.00%	default
	25.00%	25.00%	reserved
	8.00%	8.00%	basic
	50.00%	50.00%	department
mac-miss rate	0.00%	500.00%	default
	25.00%	25.00%	reserved
	8.00%	8.00%	basic
	50.00%	50.00%	department

Notice the resources allocated are shown as the guaranteed resources (minimum column) and the potential of oversubscription per resource class. From this output you can determine that 83 percent of all resources are currently allocated, except for the regular expression (regex) resource which is 98 percent allocated. This leaves the virtual partitions that are members of the default class to use the remaining 17 percent of the Cisco ACE module resources; however, they can only use 2 percent of the regular expression capacity.

Notice the default virtual partition is oversubscribed. Due to the maximum resource allocation being unlimited, the Cisco ACE module assumes a worst case of 100 percent. Because there are five virtual partitions that are members of the default class, the default class is reported as having a risk of being oversubscribed by 500 percent. As virtual partitions grow they will require additional resources. These resources can be acquired from the reserved class, which can be adjusted to free up the required resources, or by transitioning some virtual partitions to a different Cisco ACE module. Although resources could be freed from the other classes, there is a risk to some of the

resources that are in use, and thus those resources cannot be de-allocated immediately. By using a reserved class, you can easily and effectively adjust resources in a production environment.

Once created, a virtual partition can scale to use all of the resources allocated to it. As the virtual partition begins to hit resource allocation limits, more resources can be allowed dynamically.

```
ACE/Admin# show resource usage virtual partition eng
```

Resource	Current	Peak	Allocation		
			Min	Max	Denied
-----					
Virtual partition: eng					
conc-connections	1076261	2852238	4000000	4000000	0
mgmt-connections	8	24	2500	2500	0
proxy-connections	136152	201376	524288	524288	0
xlates	170226	293546	524288	524288	0
bandwidth	62946459	156087362	250000000	250000000	0
connection rate	117652	283887	500000	500000	0
ssl-connections rate	124	397	500	500	0
mgmt-traffic rate	16754661	313562819	62500000	62500000	0
mac-miss rate	0	0	1000	1000	0
inspect-conn rate	824	1782	3000	3000	0
acl-memory	9806253	20248853	39305216	39305216	0
regexp	148878	524288	524288	524288	3
syslog buffer	577166	1199438	2097152	2097152	0
syslog rate	234	786	1500	1500	0

Notice in the sample output above, the regexp resource has peaked to the virtual partition's maximum value, as indicated by both the Peak and Denied columns. These events could have occurred due to a local user attempting to implement an inefficient or overly complex set of rules, which consumed too many regexp resources, and which was later optimized to fit within the regexp limits. However, increments in the Denied column can indicate an immediate need for more resources in the regexp area for the virtual partition. If additional resources are warranted, more can be allocated dynamically by adjusting allocation of the regexp resource.

```
ACE/Admin(config)# do show run resource-class
Generating configuration....

resource-class department
  limit-resource all minimum 50.00 maximum equal-to-min
  limit-resource sticky minimum 50.00 maximum equal-to-min

ACE/Admin(config)# resource-class department
ACE/Admin(config-resource)# limit-resource regexp minimum 75.00 maximum
equal-
to-min
```

As a virtual partition grows it may be useful to subdivide it to allow for more granular management of services by using domains<sup>2</sup>. Domains are provided to control user access to configuration objects. Some examples of domain usage: ACLs and NAT can be controlled by the security group, system administrators can have access to only the server farms and real servers they maintain, the application administrators can be given access to Layer 7 rule matches so they can be configured to meet application requirements, and so forth.

```
ACE/Lab-Basic-31# show run domain
Generating configuration...

domain infosec
  add-object interface vlan 20
  add-object interface vlan 30
  add-object access-list extended everyone
  add-object access-list extended web
```

```
ACE/Lab-Basic-31# show domain
```

```
Name: default-domain , Id: 0
All objects: Yes
```

```
Name: infosec , Id: 1
```

```
-----
Object Type      Object Name
-----
Interface        vlan20
Interface        vlan30
ACL extended     everyone
ACL extended     web
```

Domains provide a separation within a virtual partition, but do not impact resource allocation, usage, or VLAN allocation. Thus, true virtualization requires a new virtual partition. However, if you just want to limit user access to the virtual partition configuration, then you should consider using domains along with RBAC.

### Cisco Solutions in Action

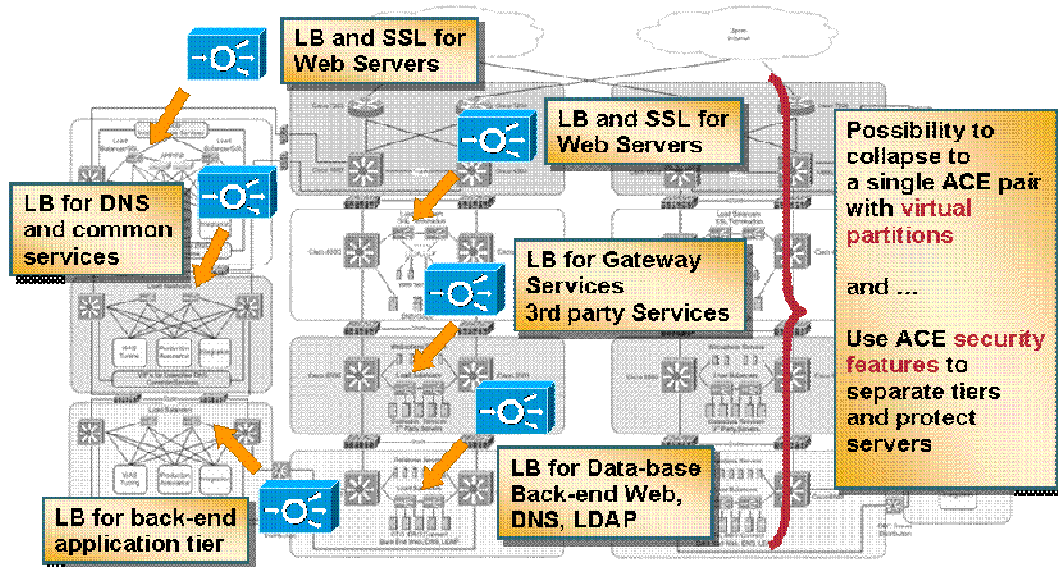
The vast functionality of the Cisco ACE virtualization solution provides many ways for you to meet your organization's specific needs. However, there are a few typical scenarios that can serve as the basis for the majority of customers. The most common scenarios are:

- Large enterprise data centers, where the Cisco ACE module provides content switching and server offload for multiple applications, while preserving secure segregation between applications and networks. This is a common design for enterprise Internets, B2B, and B2C applications.
- Large portals or public Websites (such as news and shopping sites, or search engines), where the Cisco ACE module can help sustain continuous traffic growth and spikes (for example, during holiday seasons) and virtualization is aligned with application tiers for improved management and availability.

- ISP data centers for Web and application hosting, where virtual partitions can be used to separate customers and resources can be allocated to support additional services offerings.
- Data center consolidation, where multiple data centers can be consolidated into a few globally positioned large data centers, and Cisco ACE virtualization maintains traffic separation and solves the problems of overlapping IP addressing.
- Environments where combined deployments, production, staging, and development infrastructures can reside within virtual partitions, eliminating the need for duplicate equipment in each network environment.

Large enterprise data centers can migrate dedicated load balancing and SSL acceleration services to virtual partitions within a Cisco ACE module. Many main firewall resources within the Cisco Catalyst 6500 Series FWSM or other firewall products in the data center can be freed by migrating HTTP, FTP, DNS, and RTSP protocol inspections to virtual partitions on the Cisco ACE module. In some cases these security services can be completely integrated into the same virtual partitions providing load balancing. When multiple services share a virtual partition, the number of TCP termination points to handle the flow is reduced, resulting in a reduction of the latency of client connections. The Cisco ACE module can also take advantage of Cisco Catalyst 6500 Series feature such as Route Health Injection (RHI), private VLANs, autostate, and Policy Based Routing (PBR) to help ensure secure and reliable network connectivity and to reduce the possibility of asynchronous.

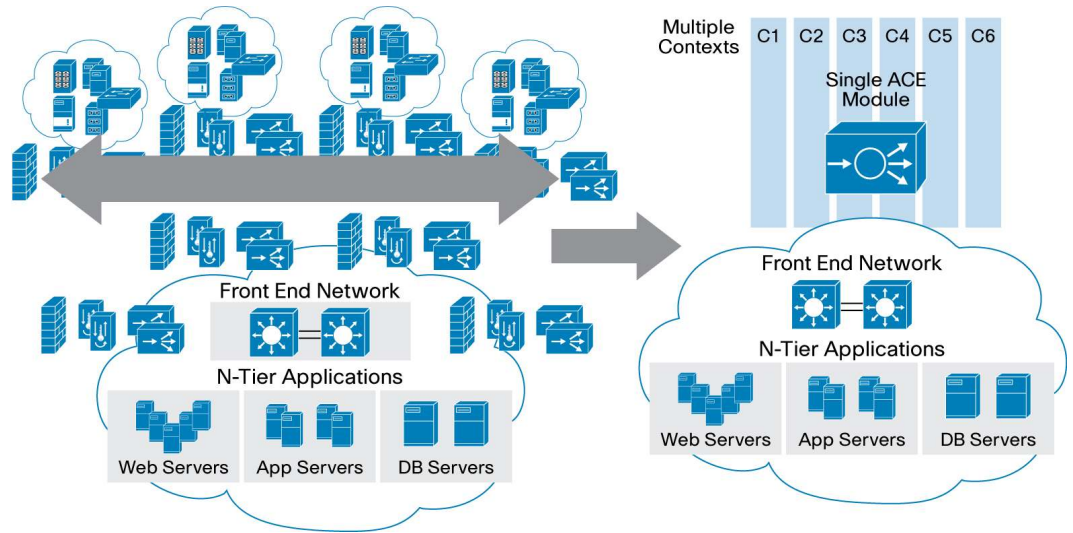
Figure 10. High-level overview of an Enterprise Datacenter



Large portals or public Websites can deploy service and application silos within a single virtual partition and use Role-Based Access Control (RBAC) and domains to provide the proper level of device access to the authorized personnel. For environments requiring more separation, cascading virtual partitions can be used to provide resource allocation per application or application tier. Within each virtual partition the ACLs, NAT, and protocols inspection features can be applied to provide additional security to existing services. The security benefits of the Cisco ACE module can also be applied to new rollouts as part of the standard deployment procedures, thus increasing the entire data center’s security. The module also offers an XML API, which many



**Figure 12.** Data Center Consolidation



Combined deployments can use the complete separation of virtual partitions, allowing for smaller sites to use one high-availability Cisco ACE module pair as the production and development device. For larger data centers typically either the development and staging, or the staging and production, share a single module. While some smaller businesses may use the same Cisco ACE module for their development and production networks in order to reduce costs, larger companies are not likely to use a single Cisco ACE module. In medium-sized to large data centers it is common to have separate production, staging, and development/testing environments. These environments would typically not use the same Cisco ACE module, due to the risk of having test traffic and production traffic within the same network. With two Cisco ACE modules and network infrastructures, the production network is not at risk if test traffic causes a network outage.

**Figure 13.** Tiered services

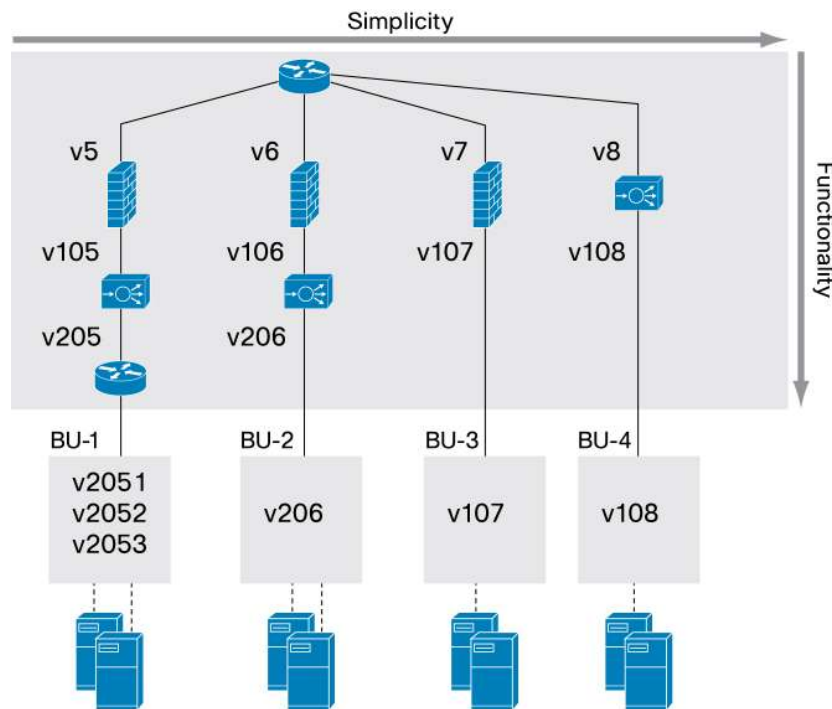


Figure 13 shows the flexibility of the module's virtual partitioning. The Cisco ACE module can be used to provide different combinations of functionalities within the data center, while preserving the simplicity required for reducing errors and improving security. The flexible functionality of the module allows it to easily integrate in Cisco's end-to-end virtualization solution for the data center network. For example, MPLS VRFs on WAN edge/core can be mapped to FWSM partitions, which are then mapped to virtual partitions on the Cisco ACE module at the aggregation layer. This facilitates server virtualization through VMWare and virtual machines, and so forth. The Cisco ACE module plays a significant role in Cisco's end-to-end virtualization solution within the data center network, and provides a major competitive advantage for large enterprise and service provider customers.

## Conclusion

To achieve the cost-effectiveness of sharing and automation in the data center, a virtualized load-balancing infrastructure is needed. Cisco has the only truly virtualized application-delivery and security services device in the industry today. The Cisco ACE Application Control Engine Module supports 250 virtual partitions with hard allocation of resources and RBAC. The following benefits summarize the value of the Cisco ACE module and its virtualization within the more demanding data centers:

- Lower capital cost: Very often individual load balancers are used for a single application or set of applications at the server access layer. In this case, similar applications can be placed off the same switch distribution layer sharing a high-performance virtualized load balancer in the distribution layer while maintaining isolation. Locally, a customer can migrate from a Cisco content services switch to a Cisco ACE module, consolidating 30 pairs of switches (60 total) to a set of six Cisco ACE modules in three server distribution layers representing three classes of applications.
- Lower administrative complexity from fewer physical devices to manage. It can be compared to managing several stackable switches versus a single switch with VLANs.
- Less space, power, and heat: A customer with 60 Cisco CSS 11503 Content Services Switches consumes 440W for each switch, totaling 26.4 KW. This customer can consolidate that into six Cisco ACE blades consuming 220W each, totaling 1.3 KW.
- Easier change control: Virtualization enables you to make a change to one application without impacting the applications in another virtual load balancer (virtual partition). This allows each application owner to take advantage of more opportunities for change without all applications on a load balancer being restricted by the least common denominator application. In addition, Cisco ACE software can be upgraded in a hitless way to further mitigate the risk of changes.
- Easier scaling and provisioning: In instances where a new application is coming online, it is simple to provision an additional virtual load balancer rather than having to purchase a new load balancer.

## Product List

- Cisco ACE Application Control Engine Module – Includes 1000 SSL TPS and 5 virtual partitions: ACE10-6500-K9
- Cisco ACE 4-Gbps Throughput License: ACE-04G-LIC
- Cisco ACE 8-Gbps Throughput License: ACE-08G-LIC

- Cisco ACE Upgrade License from 4 Gbps to 8 Gbps: ACE-UPG1-LIC=
- Cisco ACE 5,000 SSL Transactions per Second License: ACE-SSL-05K-K9
- Cisco ACE 10,000 SSL Transactions per Second License: ACE-SSL-10K-K9
- Cisco ACE 15,000 SSL Transactions per Second License: ACE-SSL-15K-K9
- Cisco ACE Upgrade License from 5,000 to 10,000 SSL Transactions per Second: ACE-SSL-UP1-K9=
- Cisco ACE Upgrade License from 10,000 to 15,000 SSL Transactions per Second: ACE-SSL-UP2-K9=
- Cisco ACE 20 Virtual Contexts License: ACE-VIRT-020
- Cisco ACE 50 Virtual Contexts License: ACE-VIRT-050
- Cisco ACE 100 Virtual Contexts License: ACE-VIRT-100
- Cisco ACE 250 Virtual Contexts License: ACE-VIRT-250
- Cisco ACE Upgrade License from 20 to 50 Virtual Contexts: ACE-VIRT-UP1
- Cisco ACE Upgrade License from 50 to 100 Virtual Contexts: ACE-VIRT-UP2
- Cisco ACE Upgrade License from 100 to 250 Virtual Contexts: ACE-VIRT-UP3
- Cisco ACE Security Feature Set License: ACE-SEC-LIC-K9
- Cisco ACE 6504 Bundle with 4G ACE Module: WS-C6504-E-ACE-K9
- Cisco ACE 6509 Bundle with 8G ACE Module: WS-C6509-E-ACE-K9

### Deployment and Support Services

Cisco Customer Advocacy Application Networking Services (ANS) and Data Center Networking (DCN) combines depth and breadth of expertise across the data center networking technologies to assist customers throughout the prepare, plan, design, implement, operate, and optimize (PDIOO) network lifecycle. Cisco Customer Advocacy also advises customers on aligning their data center and ANS and DCN strategy with their business objectives and their operational processes to industry standards and best practices. Cisco services for ANS and DCN complement those of Cisco's partners to form an end-to-end solution. For services inquiries relating to ANS or DCN, contact Advanced Services ([ask-dcn-as@cisco.com](mailto:ask-dcn-as@cisco.com)).

For more information about the Cisco ACE Application Control Engine, please visit:

[http://www.cisco.com/en/US/partner/products/hw/modules/ps2706/products\\_data\\_sheet0900aecd8045861b.html](http://www.cisco.com/en/US/partner/products/hw/modules/ps2706/products_data_sheet0900aecd8045861b.html) (requires a Cisco.com username and password)



**Americas Headquarters**  
 Cisco Systems, Inc.  
 170 West Tasman Drive  
 San Jose, CA 95134-1706  
 USA  
[www.cisco.com](http://www.cisco.com)  
 Tel: 408 526-4000  
 800 553-NETS (6387)  
 Fax: 408 527-0883

**Asia Pacific Headquarters**  
 Cisco Systems (USA) Pte. Ltd.  
 168 Robinson Road  
 #28-01 Capital Tower  
 Singapore 068912  
[www.cisco.com](http://www.cisco.com)  
 Tel: +65 6317 7777  
 Fax: +65 6317 7799

**Europe Headquarters**  
 Cisco Systems International BV  
 Haarlerbergpark  
 Haarlerbergweg 13-19  
 1101 CH Amsterdam  
 The Netherlands  
[www-europe.cisco.com](http://www-europe.cisco.com)  
 Tel: +31 0 800 020 0791  
 Fax: +31 0 20 357 1100

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](http://www.cisco.com/go/offices).

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, IQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARtNet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website 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. (0711R)