

## Network-Based Virtualization

Virtualizing network-based services and resources yields Cisco IT greater applications availability, agility, resiliency, and broad cost savings.

The inherent constraints of any physical component in terms of failure, provisioning, and limited utilization have always constituted an obstacle to optimizing the application hosting environment. Now, with network-based virtualization, this obstacle can be practically eliminated for both network resources and application services—with impressive results. Network-based virtualization yields greater availability because the uptime no longer depends on an individual physical component. As virtualization turns a hard resource into a soft one, most of the operations associated with its lifecycle are transformed from manual tasks to configuration changes, enabling automation and fostering increased agility and resiliency. And the

increased flexibility to deal with limited capacity leads to better utilization, which is a core enabler for consolidation, rationalization, and pervasive cost savings in the data center.

“Increased utilization, availability, resilience, operability, and agility simply outweigh all the overhead associated with adoption of the new technology.”

—Koen Denecker, IT Architect, Network and Data Center Services, Cisco

Cisco IT defines virtualization as the decoupling of logical and physical entities, and categorizes virtualization on two levels: *resource* (or infrastructure) virtualization and *service* (or application) virtualization. In resource virtualization, physical resources such as network, compute, and storage resources

are segmented or pooled as logical resources. An example of resource virtualization: Sharing a load balancing device (hardware) between multiple applications virtualizes the infrastructure. In service virtualization, on the other hand, multiple physical service instances are grouped to act as one logical instance. Service virtualization includes application services (fully functional application instances) and network services (application component instances that are used to build fully functional applications). An example of service virtualization: Load balancing an application (service) between two servers virtualizes the application and enables high availability. With virtualization, the role of the network is twofold: the network resources themselves are virtualized, and the network also acts as an enabler for service virtualization.

Since 2000, Cisco IT has virtualized five network-based resources and services:

- Server load balancing
- Firewalling
- Secure Sockets Layer (SSL) encryption and decryption
- Web services gateway
- Global site selection

For Cisco IT, virtualizing load balancing alone has increased utilization of the hardware involved from 5 to 75 percent. Simultaneously, the physical footprint for the load balancers decreased by 50 percent while the total number of virtualized applications increased sixfold. Load balancing was, in fact, the first shared network service Cisco IT offered across the network that severed the one-to-one link between application and device.

“Before 2000, everything was siloed,” says Wilson Ng, network engineer in the IT Networking Design and Engineering group at Cisco. “If a client wanted load balancing, IT would procure the system, go through a learning curve on how to use it for the particular application, and finally deploy it. The whole process would take two to three months.”

Multiple load balancing systems were increasingly becoming harder for IT to manage and maintain and produced low average utilization. Moreover, the number of application environments that required load balancing was doubling each year. By 2003 the group was operating 14 pairs of load balancers. “We concluded that this was not the way we should provide the network service,” Ng says.

So in 2003 Cisco IT introduced a virtualized, horizontal load balancing service using the Cisco Catalyst 6500 Series Switch Content Switching Module (CSM) and partitioning techniques to create logical, individual load balancers. The first application to use a virtualized load balancer was the Cisco employee intranet; the CSM was located in a data center at the company’s headquarters in San Jose, California. With the success of that application, Cisco IT migrated other applications to the virtualized load balancing service.

Today one pair of CSM modules has been configured to handle the entire production load balancing required across the Cisco data center at Research Triangle Park, North Carolina. Where only 5 percent of capacity was being used on average with the 14 pairs of load balancers, now up to 75 percent of the CSM (paired for redundancy) capacity is used.

### **Into the IT Infrastructure**

The virtualized load balancing service was the first instance of bringing a service into the IT infrastructure rather than having it reside on dedicated systems paid for by application owners. It became the model and motivation for Cisco IT to virtualize other services.

Now Cisco IT is migrating from the CSM to the Cisco Application Content Engine (ACE) Module, which can divide resources into 250 different virtual partitions.

Each partition can be defined by application, customer, or business organization, and resource allocations such as bandwidth or number of connections can be defined for each partition. In addition, role-based access control (RBAC) in the ACE Module allows each virtual partition to be managed by the appropriate IT team.

With the ACE Module, even large applications, such as enterprise resource planning (ERP) can be served by up to 250 virtual load balancers, with a percentage of the module’s load balancing resources dedicated to ERP when needed.

Next, Cisco IT initiated the virtualization of firewalling, deployed on a Cisco Catalyst 6500 Series Firewall Services Module (FWSM). Like the ACE Module, the FWSM can be partitioned into multiple logical firewalls assigned to specific applications. It, too, runs horizontally across the data center.

Eliminating various siloed load balancing appliances has given Cisco IT consistent configuration, deployment, and monitoring capabilities, and has also significantly increased service availability and load balancing infrastructure utilization. What’s more, requests for load balancing can be satisfied in hours, rather than months.

The CSM and ACE Module are also the key enabling technologies for application service virtualization. Cisco’s primary Internet presence, Cisco.com or www.cisco.com, consists of multiple server farms, each with multiple physical servers, which have been optimized for specific application functionality.

For example, one server farm serves static content, a second serves dynamic content, and a third provides a supporting authentication role. To the outside world, however, the Internet presence appears as one giant server. In addition, physical server failures and server maintenance can be hidden from end users.

This deployment of application virtualization enables greater availability, agility, and operability.

### **Some Complexity of Integration**

The next two services that Cisco IT sought to virtualize require more involvement from application owners: SSL encryption and decryption and an XML Gateway. SSL encryption and decryption, using the Cisco Catalyst 6500 ACE Module or the earlier SSL Service Module (SSLSM), was first used in 2004 to enable content switching of encrypted HTTP traffic in the Java 2 Enterprise Edition environment. This environment hosts more than 40 percent of Cisco's internal and external applications and is mission-critical to Cisco's business.

Later, in 2006, it was adopted to support employees who use a non-Windows-based operating system, such as UNIX, and who need access to Windows-based e-mail. The SSLSM offloads the encryption and decryption required from the e-mail server, resulting in much faster access for the employees. This functionality is being transitioned to the newer, more scalable ACE Module, which integrates it better into the load balancing and content switching function.

The application owner's involvement with this service must increase because there is more integration work, according to Koen Denecker, IT architect in the Network and Data Center Services group at Cisco. "There is the benefit to the owner of not paying for the hardware, but the owner must sit down with IT to discuss the application's specific needs."

The SSLSM has been installed in all major Cisco IT production centers, and Cisco IT is using it to support other services in a virtual way. Additionally, Denecker says, IT now uses the SSLSM to support application environments, not just individual applications, for example, the Java-to-enterprise environment. "We use the SSLSM to encrypt and decrypt for hundreds of applications by putting it on that single environment," he says.

Cisco IT is also using the SSLSM with the CSM to enable back-end migration and vendor transition in the Java 2 Enterprise Edition environment, which

hosts the bulk of the internal and external HTTP-based applications. Because these communications include queries about personnel matters, the entire payload, including incoming URLs, is encrypted and must be decrypted before the application can go to the appropriate application server selected by the content switch. The SSLSM performs the first task; the CSM performs the second. Today, both functions can be performed within a single pair of ACE Modules.

The Cisco ACE XML Gateway is another example of network-based service virtualization. It provides a virtual web services gateway to the Internet for a broad range of users whose applications need XML links to other software, to databases, or other systems to do their jobs.

"The ACE XML Gateway can act as a virtual front door for B2B [business to business] interactions within Cisco," says Sandeep Puri, IT architect in the Platform Services and Support group at Cisco. "This gives us one interface point through which our partners may talk to us. The XML Gateway can transform different data formats involved in B2B interactions on the fly to what we use at Cisco. The appliance gives us a central point to enforce different service policies that we may have for services that Cisco hosts. In addition, the gateway can be positioned to add an additional layer of security by using the appliance's XML level firewall policies," he explains.

### **An Enabler of Virtualization**

The latest service to be virtualized is as much an enabler of the technology as a use of it. The Cisco ACE GSS 4400 Series Global Site Selector (GSS) performs global server load balancing. It distributes client requests for applications to different geographic instances of those applications.

"Users anywhere in the world can reach the nearest instance of an application for faster access and response times—it's a form of

application acceleration,” says Jon Woolwine, IT architect in the IT Networking Design and Engineering group at Cisco.

It is also very useful for disaster recovery and even routine maintenance and software upgrades. When a system goes down, whether planned or not, the GSS can reroute application requests from clients to an application instance in a different geographic location.

### Recommendations

Global server load balancing, like local server load balancing and firewalling, have been easy to pitch as virtualized network-based services. Whether easy to pitch or not, any virtualized service must be undertaken only after considerable planning.

Woolwine, who has worked closely with applications teams within Cisco IT and with application owners, believes that it is imperative to bring both these groups together with network engineers and architects. This collaboration, he says, is required “to get an end-to-end perspective and an understanding of all the complexities of a given application, its dependencies, how it links to servers and storage, and other intricacies, along with how they will be affected by virtualizing a given service. That is a challenge, because typically people are from one camp or another.”

Cisco IT chose to employ this process not for all of the thousands of applications it uses, but rather for the large and critical ones and those with common environments or front ends.

Virtualizing network-based services might also require the convergence of technologies and multiple groups within a company, not unlike that seen when voice and data converged.

“The server, storage, and network teams need to work together to develop policies and standards for areas that will be virtualized,” says Ng. “For example, when using VMware, the network and server teams had to standardize to 801.1Q trunking for VMware servers. This allows virtual server provisioning and network service access.”

When integrating services into the network, IT staff should also look for opportunities to maintain current data center architecture and keep existing logical components. Cisco IT took advantage of the flexibility built into the CSM, ACE, SSL, and FWSM modules to deploy them without any change to the application’s server. The IT group also kept the same access controls, spanning tree protocols, and other data center provisions.

In addition, the costs to virtualize should be factored in at the beginning.

“Virtualization makes operations more complex, and tracking down a complex network application integration problem may take significantly more resources and last longer if the support staff has not been trained appropriately,” says Denecker. “It is critical to accompany the introduction of new technologies with the appropriate organizational evolution and skillset developments.”

Some tasks, he adds, increase in importance, such as capacity planning, fault containment, testing, quality management, monitoring, dependency management, and change management. Then again, virtualization increases cross-functional collaboration and avoids silos of technical expertise.

Even so, says Denecker, “The value of the increased availability that virtualization brings will outweigh the cost issues and risks. Increased utilization, availability, resilience, operability, and agility simply outweigh all the overhead associated with adoption of the new technology.”

And very tantalizing are the possibilities inherent in the level of service integration attainable with virtualization, when services are abstracted from applications and components (e.g., a reusable pricing module in an ordering tool) may be distributed among many locations and shared with many applications.

This abstraction gives IT enormous flexibility in provisioning and even compiling applications.

“We can begin to build services in a service-oriented architecture,” says Denecker. “We might take one component from one application, another from a second, and so on to compile a new application, as long as all the parts operate within the same environment. This is how Cisco IT sees the data center becoming the computer with the network as the enabling platform.” ■

For more Cisco IT featured content and case studies, visit <http://www.cisco.com/go/ciscoit>.

## FURTHER READING

- Cisco on Cisco Featured Content: “Server Virtualization on Fast Track”  
[http://www.cisco.com/web/about/ciscoit/work/featured\\_content/fc\\_july\\_aug\\_2007\\_article01.html](http://www.cisco.com/web/about/ciscoit/work/featured_content/fc_july_aug_2007_article01.html)
- Cisco on Cisco Featured Content: “Storage Virtualization a Work in Progress”  
[http://www.cisco.com/web/about/ciscoit/work/featured\\_content/fc\\_july\\_aug\\_2007\\_article03.html](http://www.cisco.com/web/about/ciscoit/work/featured_content/fc_july_aug_2007_article03.html)
- Cisco ACE Module  
<http://www.cisco.com/en/US/products/ps6906/index.html>
- Cisco ACE XML Gateway  
<http://www.cisco.com/en/US/products/ps7314/index.html>
- Cisco ACE GSS 4400 Series Global Site Selector  
<http://www.cisco.com/en/US/products/hw/contnet/ps4162/index.html>



**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, Inc.  
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).

©2006 Cisco Systems, Inc. All rights reserved. CCVP, the Cisco logo, and the Cisco Square Bridge logo 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, BPX, 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, GigaStack, HomeLink, Internet Quotient, IOS, IP-TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, Packet, PIX, ProConnect, RateMUX, ScriptShare, SlideCast, 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. (0609R)