

Next-Generation Federal Data Center Architecture

Introduction

The United States government's [E-Gov](#) initiative established the [Federal Enterprise Architecture \(FEA\)](#) program to build a business-driven information technology (IT) blueprint for the federal government. The FEA provides a common language and framework to describe and analyze IT investments, enhance collaboration, and ultimately transform the federal government into a citizen-centered, results-oriented, and market-based organization. FEA initiatives will drive the development of next-generation [federal IT](#) architectures.

Cisco®, in response to the FEA and to enterprise IT initiatives throughout public and private industry, developed the Cisco® Service-Oriented Network Architecture (SONA). [Cisco SONA](#) is an architectural framework that promotes the ongoing evolution toward an Intelligent Information Network (IIN) to accelerate applications, business processes, productivity, and profitability.

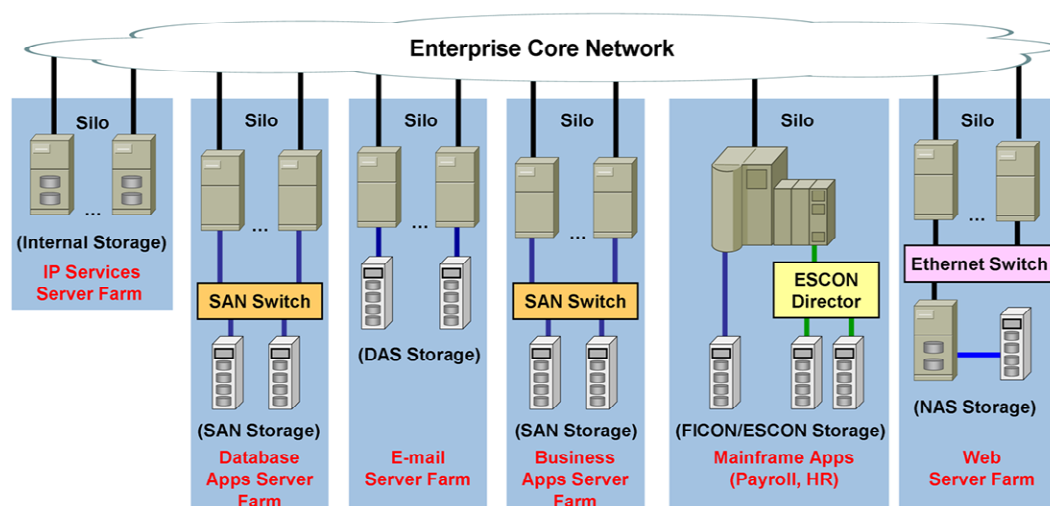
Cisco SONA establishes architectural guidelines to help federal organizations evolve their IT infrastructures toward the FEA vision—to become the cornerstone for the design, development, and implementation of information resources government wide. The FEA takes advantage of industry best practices such as the enterprise architectures within Cisco SONA to transform government business processes with network investments that increase organizational agility, efficiency, and productivity.

The FEA Infrastructure Optimization Initiative (IOI) further refines the opportunities for IT infrastructure consolidation and optimization. A key area of focus in the IOI is the data center. With the Cisco SONA framework as a base, Cisco provides a standards-based data center networking architecture that enables federal organizations to build efficient and adaptive infrastructures. The [Cisco Data Center Network Architecture](#) creates a foundation upon which federal IT executives can better align data center resources with mission priorities. Cisco's architectural approach complements the FEA vision and facilitates the IOI by establishing a road map for federal data center evolution.

The Cisco Data Center Network Architecture integrates the Network Infrastructure Services and Application Networking Services that make up the next-generation federal enterprise data center. The remainder of this paper discusses the evolution and future direction of federal data center architectures in the context of Cisco SONA and the Cisco Data Center Network Architecture.

Legacy Data Centers

Federal data centers grew rapidly during the past 20 years to maintain pace with expanding mission requirements and E-Gov initiatives. Federal IT managers often deployed servers, storage devices, and network equipment in dedicated configurations, application by application. The resulting data center architecture today consists of isolated application environments (Figure 1) with low resource utilization, higher cost, complex management, and an inordinate amount of power consumption. These isolated environments, or silos, preclude the deployment of uniform services, instead employing separate security protections, performance metrics, backup and recovery. Their power requirements greatly increase the data center's total cost.

Figure 1. Legacy Data Centers with Application Silos

The growth of applications and data continues to accelerate, due to ongoing mission requirements in homeland security and national defense, as well as regulations on information security and privacy such as the Healthcare Insurance Portability and Accountability Act (HIPAA) and the [Federal Information Security Management Act \(FISMA\)](#). Mission requirements and regulations are driving federal IT managers to view their information networks holistically and evolve their infrastructures within a new, standards-based design framework. Moreover, federal CIOs recognize the operational cost savings they can achieve by investing in systems and networks that streamline the deployment of applications and services and rein in data center power consumption.

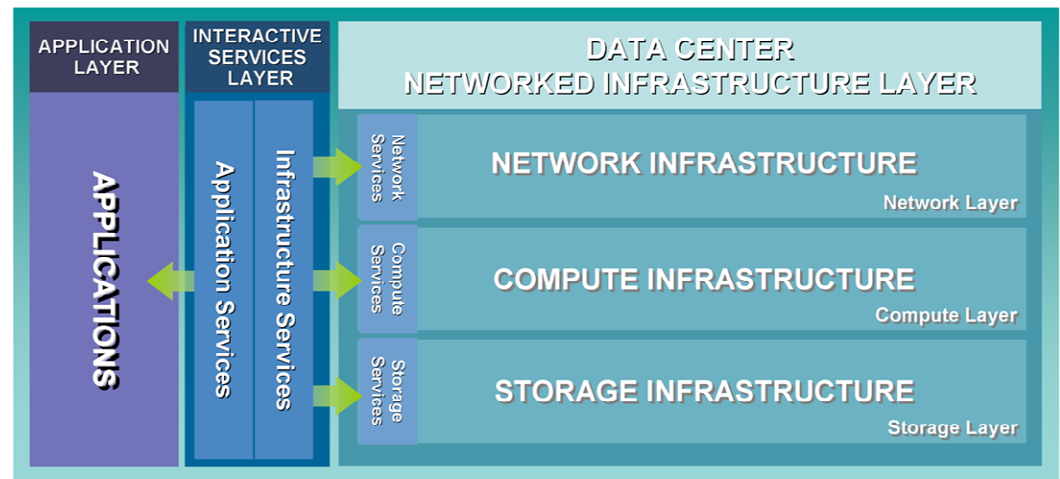
To meet these objectives, consolidated infrastructures with virtualized services must take the place of dedicated application silos in the data center. The ability to use uniform services increases the flexibility and simplicity of infrastructure and application management across the entire data center.

A New Data Center Model

The Cisco SONA framework outlines how federal enterprises can evolve to an Intelligent Information Network that optimizes applications, business processes, and resources. The principle behind Cisco SONA is that federal CIOs can dramatically increase productivity and efficiency while improving business resilience, reducing costs, and aligning with mission priorities if they make the right investment in the network.

The [Cisco Data Center Network Architecture](#), based on Cisco SONA, provides a system-level framework to address immediate data center demands for consolidation and business continuance. Cisco combines Network Infrastructure Services and Application Networking Services to enable emerging Service-Oriented Architectures (SOAs), virtualization, and on-demand computing technologies. Cisco's architecture approach presents federal IT decision makers with greater freedom to deploy storage, compute, and software technologies that best support their mission needs.

The next-generation federal data center architecture comprises three layers: network, compute, and storage (Figure 2). Each layer performs a distinct role within the Cisco Data Center Network Architecture, linking interactive services to applications and critical business process flows.

Figure 2. Three-Layer Data Center Model

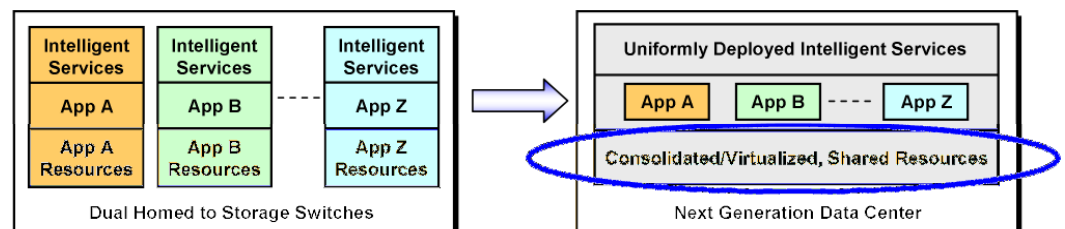
The network layer provides secure and reliable access to the compute layer. It uses Layer 2/Layer 3 network switches (e.g., Ethernet and IP) to connect users with data center resources. Appliances and service modules ensure secure access and optimize resource utilization and performance.

The compute layer provides the computing resources (i.e., servers and mainframes) that run applications invoked by users. Server switches interconnect the computing resources and provide access to the storage layer. Traditionally in the compute layer, parallel applications have run on supercomputers that are prohibitively expensive for many companies to acquire and operate. High-performance computing (HPC) clusters today use the same principles as traditional supercomputers. HPC clusters comprise multiple industry-standard computers (sometimes many thousands) using cluster software and high-performance network interconnects to run parallel applications at a fraction of the cost of traditional supercomputers.

The storage layer stores the data used by applications on storage subsystems (e.g., disk drives and tape drives). The storage layer uses storage switches and optical transport platforms to interconnect and provide access to disk resources within and between data centers.

Consolidation and End-to-End Virtualization

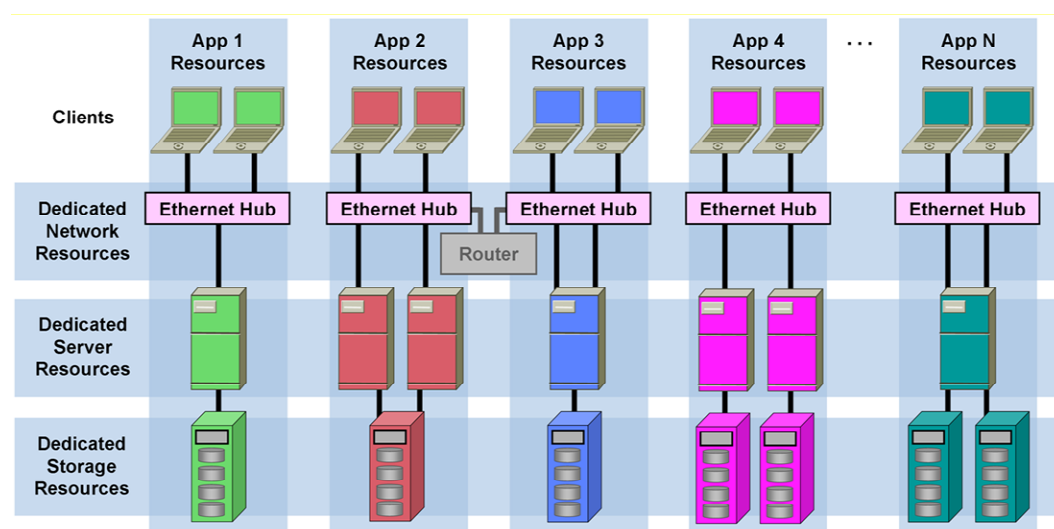
Application silos cannot effectively scale to meet the expanding demands on today's data centers. Next-generation data centers consolidate the infrastructure and virtualize resources across a smaller number of components and facilities, which saves precious kilowatt-hours. Data center resources are no longer dedicated to specific applications but are logically assigned to applications as needed (Figure 3).

Figure 3. Next-Generation Data Centers—Consolidation and Virtualization

This approach simplifies management, expedites the deployment of new applications, optimizes resource use, and reduces operating costs. A virtualized infrastructure simplifies the deployment of intelligent services and allows federal CIOs to invest thoughtfully in an intelligent information network that delivers critical support services for their ongoing mission requirements.

There are many aspects to virtualization across each layer of the data center architecture. Figure 4 illustrates a legacy data center with dedicated resources at each layer. Users within a department or workgroup connect to a LAN dedicated to the workgroup. Applications that are specific to the workgroup run on dedicated servers and storage. Each workgroup contains dedicated hubs, servers, and storage subsystems. At the network layer, routers interconnect workgroups, but back-end storage and compute resources remain dedicated. Without virtualization, the resulting application silos form by default.

Figure 4. Data Center Architecture with Dedicated Resources



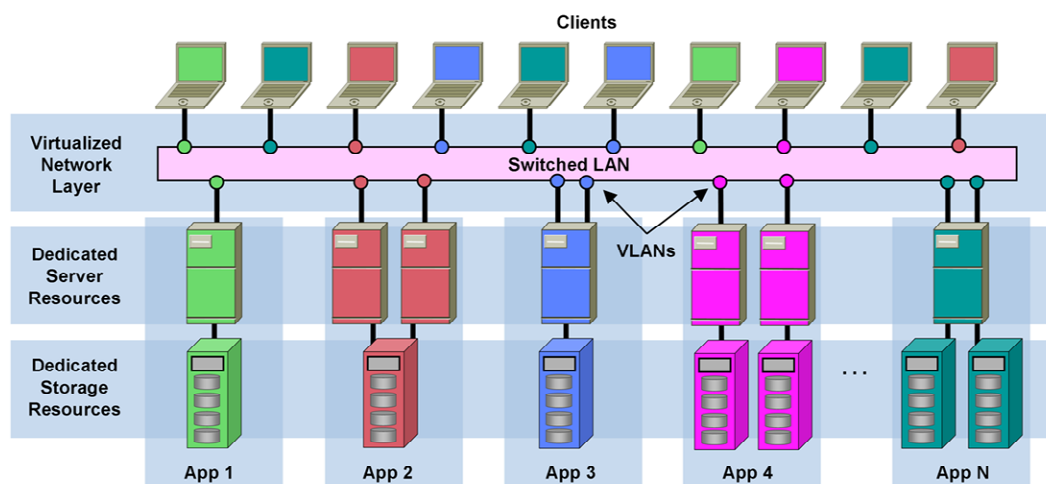
Network Layer Consolidation and Virtualization

Network layer consolidation interconnects networking resources into a shared, intelligent network. Virtualization permits the dynamic assignment of networking resources to users and applications with services such as Dynamic Host Configuration Protocol (DHCP) and Network Access Control (NAC).

Figure 5 illustrates a data center with a virtualized network layer. Virtualization at this layer begins to break down application silos by opening access to applications across a switched LAN.

Network switches supporting VLAN technology, most commonly over Ethernet, enable virtualization at the network layer. VLANs pool network resources and logically assign them to users and applications as needed. This architecture represents the state of most data centers today. By providing ubiquitous access to the application environment over the network infrastructure, a virtualized network layer eliminates the need to purchase dedicated LAN hubs or switches for new applications.

Figure 5. Data Center Architecture with Virtualized Network Layer



Storage Layer Consolidation and Virtualization

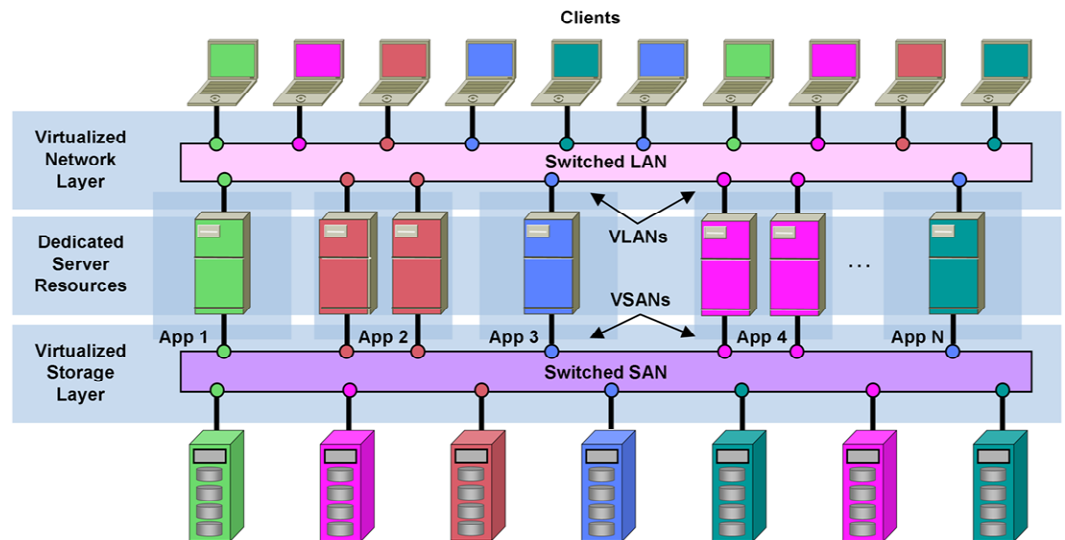
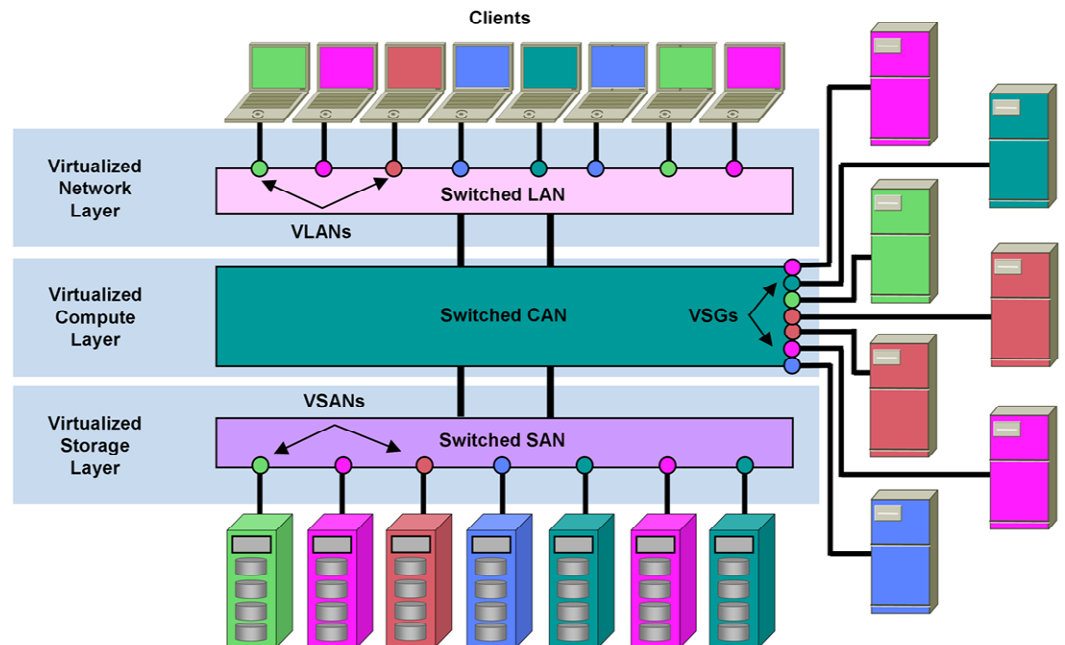
The next step in an end-to-end virtualized data center is the consolidation and virtualization of the storage layer. Applications today are often deployed with dedicated storage subsystems interconnected by a single storage area network (SAN) island. Storage consolidation combines SAN islands and further breaks down application silos by interconnecting storage resources via a single intelligent SAN. If the storage layer is virtualized, storage can be treated as a pooled resource and dynamically assigned to applications as required.

Storage switches that support virtual SAN technology enable storage layer virtualization. VSANs allow administrators to pool disks and storage arrays on a common infrastructure and logically distribute storage among applications (Figure 6). A virtualized storage layer does not require the purchase of dedicated storage or SAN switches for new applications. VSANs segregate fabric services among logical groups to decrease the fault domain and minimize fabric disruptions during planned and unplanned outages on the SAN. Administrators can then consistently manage these separate virtual fabrics and apply comprehensive security policies across the entire consolidated storage infrastructure.

As with a virtualized network layer, virtualized storage promotes efficient resource usage, reduces costs, and expedites the deployment of new applications. Virtualization also simplifies management by combining dedicated SAN islands onto a common SAN. Today's SAN switching technology provides multiprotocol support and optical transports that enable federal IT managers to address disaster recovery and Continuity of Operations (COOP) policies and regulations by extending the SAN across the WAN.

Compute Layer Consolidation and Virtualization

The final element of end-to-end data center consolidation and virtualization resides at the compute layer. Compute consolidation connects server resources via an intelligent compute or cluster area network (CAN). Server resources are assigned to virtual server groups (VSGs) and dynamically reassigned as needed (Figure 7). Based on the assigned VSG, diskless servers remotely boot the appropriate operating system (OS) and execute applications as assigned by the administrator. Compute consolidation reduces costs and increases efficiency by allowing the use of standard servers in pooled configurations. Combined with a virtualized storage layer, compute layer virtualization significantly decreases the time it takes to bring up new applications and services.

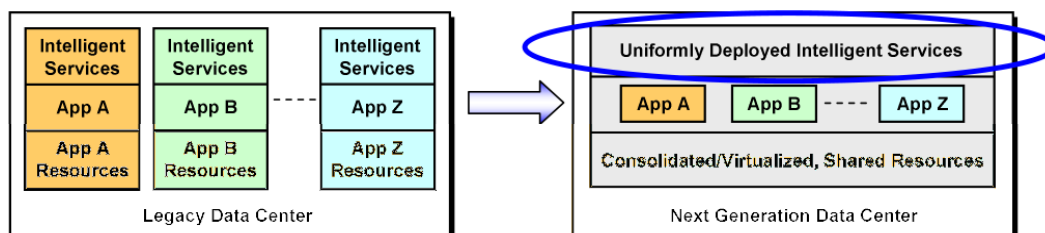
Figure 6. Data Center Architecture with Virtualized Network and Storage Layers**Figure 7.** End-to-End Virtualized Data Center Architecture

End-to-End Intelligent Services

The growth of application silos in legacy data centers poses a challenge for the deployment of intelligent services. Each silo requires separate security, optimization, backup, and disaster recovery planning, which increases complexity and cost and complicates system management across the data center. A consolidated data center with pooled resources streamlines the deployment of intelligent services. Like other data center resources, the intelligent services are shared and dynamically assigned where needed.

Intelligent data center services include an abundance of features that affect availability, resource optimization, security, and performance. The effective deployment of intelligent services requires an end-to-end design in which the requisite services are applied at each layer of the data center architecture (Figure 8).

Figure 8. Next-Generation Data Center—Uniformly Deployed Intelligent Services



Network Layer Intelligent Services

Intelligent services at the network layer ensure secure and reliable access to applications, optimize resource use, and guarantee traffic performance levels. Intelligent network layer services encompass three categories: application delivery services, traffic management services, and security services.

- *Application delivery services* optimize the delivery of applications within a data center and across the WAN. Content switching, server load balancing, and site selection services select the best server and site to handle incoming user requests. If a failure occurs, requests are automatically redirected to a different server or site.

Across the WAN, bandwidth and latency adversely affect application performance. Intelligent services such as local caching, data compression, and protocol optimization create a LAN-like experience for remote users.

Local caching dynamically stores recent or commonly requested content at the remote site. Caching decreases the WAN load and accelerates the user's perception of the application. Compression also decreases the WAN load by minimizing bandwidth usage when data is sent.

Protocol optimization services minimize traffic from verbose protocols such as common Internet file system (CIFS) and network file system (NFS), which were originally designed to operate in LAN environments. These protocols use hundreds or thousands of messages per file exchange. On a WAN, the aggregate latency therefore can be very high. Protocol optimization technologies streamline these exchanges through message suppression and message multiplexing.

- *Traffic management services* help ensure that each application receives the required level of service. Traffic management is particularly important in the data center, where voice, video, and data traffic converge. Traffic management policies dictate performance levels for application traffic within the data center and for traffic that leaves the data center and travels the WAN. Intelligent traffic management services include optimal routing, load balancing, link aggregation, and quality of service (QoS) mechanisms such as traffic prioritization and congestion control.

- *Security services* provide secure and reliable access to data center resources and are responsible for two functions: service availability, and data integrity and confidentiality. Service availability helps ensure that data center resources are available when requested. Data integrity and confidentiality helps ensure that data is complete, unaltered, and viewed only by authorized users. Security service technologies used in the data center include SSL traffic management and acceleration, firewalls, VPN load balancing, and denial-of-service (DOS) attack prevention.

Storage Layer Intelligent Services

Intelligent storage layer services include IP integration services, data replication services, traffic management services, and storage security services.

- *IP integration services* use protocols such as Small Computer System Interface over IP (iSCSI) and Fibre Channel over IP (FCIP). Universal accessibility to stored data allows users and applications to access information regardless of physical location or networking technology. Today, IP integration services provide integrated gateway functionality between IP and Fibre Channel and further extend access to SAN data onto the IP network.
- *Data replication services* copy data for failure contingencies. Data replication commonly occurs within the data center (e.g., tape backup) and to a secondary data center using integrated IP services or optical transport services. The SAN extension over IP or optical transport provides replication to multiple data centers.
- *Traffic management services* ensure that SAN (i.e., Fibre Channel) data is delivered with the required level of service. As an example, the expected performance of a bulk data transfer differs from that of a transactional process. As in the network layer, intelligent traffic management services at the storage layer include optimal routing, load balancing, link aggregation, and QoS mechanisms such as traffic prioritization and congestion control. These technologies are now available in a Fibre Channel environment.
- *Storage security services* restrict access to storage resources to authorized clients only, while protecting the integrity and confidentiality of the stored data. SAN security services include VSANs, zoning, port security, and Fibre Channel Security Protocol (FCSP) for data integrity and authentication.

Compute Layer Intelligent Services

The compute layer includes the computing resources that run applications. Compute layer intelligent services help ensure that server resources are utilized efficiently and are available and secure. Servers are often deployed in groups where each server runs an instance of the application (server farm) or where each server runs a portion of a single application (compute cluster). In either scenario, these groups of servers increase availability, improve performance, and efficiently share resources. In addition to the security services already deployed at other layers, the compute layer adds its own security features, including user authentication and intrusion prevention.

Compute layer intelligent services can be further divided into three levels: compute, OS, and application.

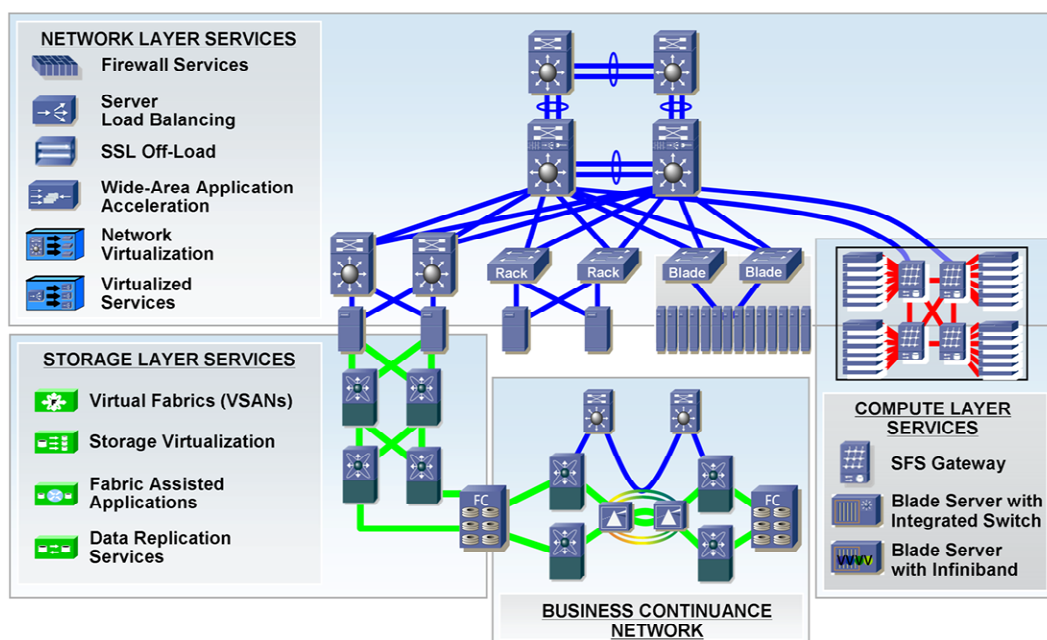
- The compute level consists of the hardware that makes up the compute resources and associated physical interconnects.

- The OS level consists of the operating system, security, and other software-based monitoring that allows for either manual or automatic actions or notifications.
- The application level supports the applications that run to provide services to the end users or to other applications.

Cisco Solutions for Next-Generation Data Centers

Cisco SONA establishes a systems approach that federal IT managers can use to evolve their data centers to a service-oriented model. Cisco solutions that propel this evolution toward next-generation data center architectures include Application Networking Services (ANS), Server Networking and Virtualization, and Storage Networking. These solutions provide a comprehensive set of infrastructure services at the network, storage, and compute layers of the data center network (Figure 9). To learn more about the Cisco portfolio of data center solutions, visit <http://www.cisco.com/go/datacenter>.

Figure 9. Next-Generation Data Center Solutions



Application Networking Services

Cisco ANS solutions allow applications and IP networks to work together seamlessly, delivering more value from existing applications. Shared application networking services hosted in the existing network improve application delivery, simplify the infrastructure required for sophisticated deployments, and propel efficiency within the IT organization.

Cisco data center solutions—such as the Cisco Application Control Engine (ACE), the Cisco Application Velocity System (AVS), and Cisco Content Services Switches—increase application control, performance, and security while simplifying the infrastructure of the data center. Cisco Wide Area Application Services (WAAS) provide optimal performance for applications delivered from the central data center to remote office users, and they consolidate the remote server, storage, and backup infrastructure into the data center. The Cisco WAAS solution maintains LAN-like service levels for remote users and minimizes WAN bandwidth expenses.

For more information, visit: <http://www.cisco.com/en/US/products/hw/contnetw/index.html>.

Server Networking and Virtualization

Cisco compute networking and virtualization solutions, which include Server Fabric Switches and VFrame Server Fabric Virtualization Software, enable server and application architects to create unified compute fabrics for high-performance cluster computing and I/O consolidation and virtualization. These solutions allow federal IT managers to better consolidate server resources, better utilize servers already in operation, and reduce the number of new servers required. Such solutions also help reduce server power consumption in the data center.

Because the network is the common platform that touches the compute, service, application, user, and storage components, integration of the server fabric with virtualization in the network provides significant benefits. By more intelligently virtualizing access to IT resources, the network can deliver more effective service to the application, operating system, and devices.

For more information, visit: <http://www.cisco.com/en/US/products/ps6418/index.html>.

Storage Networking

Cisco intelligent storage networking solutions provide a better way to access, manage, and protect growing information resources across a consolidated infrastructure. The Cisco MDS 9000 Series introduced the industry's first true multiprotocol SAN product, combining Fibre Channel, FCIP, iSCSI, and Gigabit Ethernet in a single director-class platform. The Cisco MDS 9000 Series presents VSAN technology and legacy interoperability features that simplify and accelerate migration from discrete SAN islands to consolidated fabrics with multiple layers of intelligence.

Delivering industry-leading availability, scalability, security, and management, the Cisco MDS 9000 Series allows the deployment of high-performance SANs while lowering the total cost of ownership. Layering a rich set of intelligent features onto a high-performance, open-protocol switch fabric, the Cisco MDS 9500 Series Multilayer Directors address the stringent mission requirements of federal data centers while supporting the transparent integration of new technologies.

Synchronous mirroring applications for disaster recovery are provided via the Cisco ONS 15454 dense wavelength-division multiplexing (DWDM) and SONET solutions. DWDM is ideal for reliable metro area connectivity between data centers, and SONET provides high time-division multiplexing (TDM) bandwidth over longer distances. Both technologies provide excellent transport options for remote replication over Fibre Channel or FCIP.

For more information, visit: <http://www.cisco.com/en/US/products/hw/ps4159/index.html>.

Conclusion

Consolidation and optimization of federal IT infrastructures represent a significant opportunity to realize future cost savings by taking a more structured approach to infrastructure investment. Isolated application environments, or application silos, will not meet the objectives of the FEA. To move toward the service-oriented FEA vision, next-generation federal data center architectures must build upon a solid framework and take advantage of the benefits of infrastructure consolidation, optimization, and services virtualization. Next-generation data centers will promote efficient resource utilization, provide secure and reliable access to resources, and allow the rapid deployment of new applications. IT infrastructure consolidation and optimization will help federal agencies improve IT service levels and help turn their focus toward their core mission priorities and the desired results.

Cisco SONA enables federal agencies to evolve to an Intelligent Information Network that achieves increased IT efficiencies and has a positive impact on agency mission. Cisco has the proven enterprise architectures, breadth of partners, and advanced technologies, lifecycle services, and experience across industries to help federal organizations meet their business imperatives in real time.

Acronyms	
ACE	Application Control Engine
ANS	Application Networking Service
AVS	Application Velocity System
CAN	Cluster Area Network
CIFS	Common Internet File System
CIO	Chief Information Officer
COOP	Continuity of Operations
DHCP	Dynamic Host Configuration Protocol
DOS	Denial of Service
DWDM	Dense Wavelength-Division Multiplexing
FCIP	Fibre Channel over Internet Protocol
FEA	Federal Enterprise Architecture
FISMA	Federal Information Security Management Act
HIPAA	Healthcare Insurance Portability and Accountability Act
HPC	High-Performance Computing
HTTP	Hypertext Transfer Protocol
IIN	Intelligent Information Network
I/O	Input/Output
IOI	Infrastructure Optimization Initiative
IP	Internet Protocol
iSCSI	Small Computer System Interface over Internet Protocol
IT	Information Technology
LAN	Local Area Network
MDS	Multilayer Director Switch
NAC	Network Access Control
NFS	Network File System
OS	Operating System
QoS	Quality of Service
SAN	Storage Area Network
SOA	Service-Oriented Architecture
SONA	Service-Oriented Network Architecture
SONET	Synchronous Optical Network
TCP/IP	Transmission Control Protocol/Internet Protocol
TDM	Time Division Multiplexing
VLAN	Virtual Local Area Network
VSAN	Virtual Storage Area Network
VSG	Virtual Server Group
WAAS	Wide-Area Application Services
WAN	Wide Area Network

References

Enabling Citizen-Centered Electronic Government 2005–2006 FEA PMO Action Plan, March 2005
 President's Management Agenda, Office of Management and Budget, Fiscal Year 2002
 Infrastructure Optimization Initiative, Request for Information, April 6, 2006.



Americas Headquarters
 Cisco Systems, Inc.
 170 West Tasman Drive
 San Jose, CA 95134-1706
 USA
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
 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
 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.

©2007 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, iPhone, 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. (0701R)