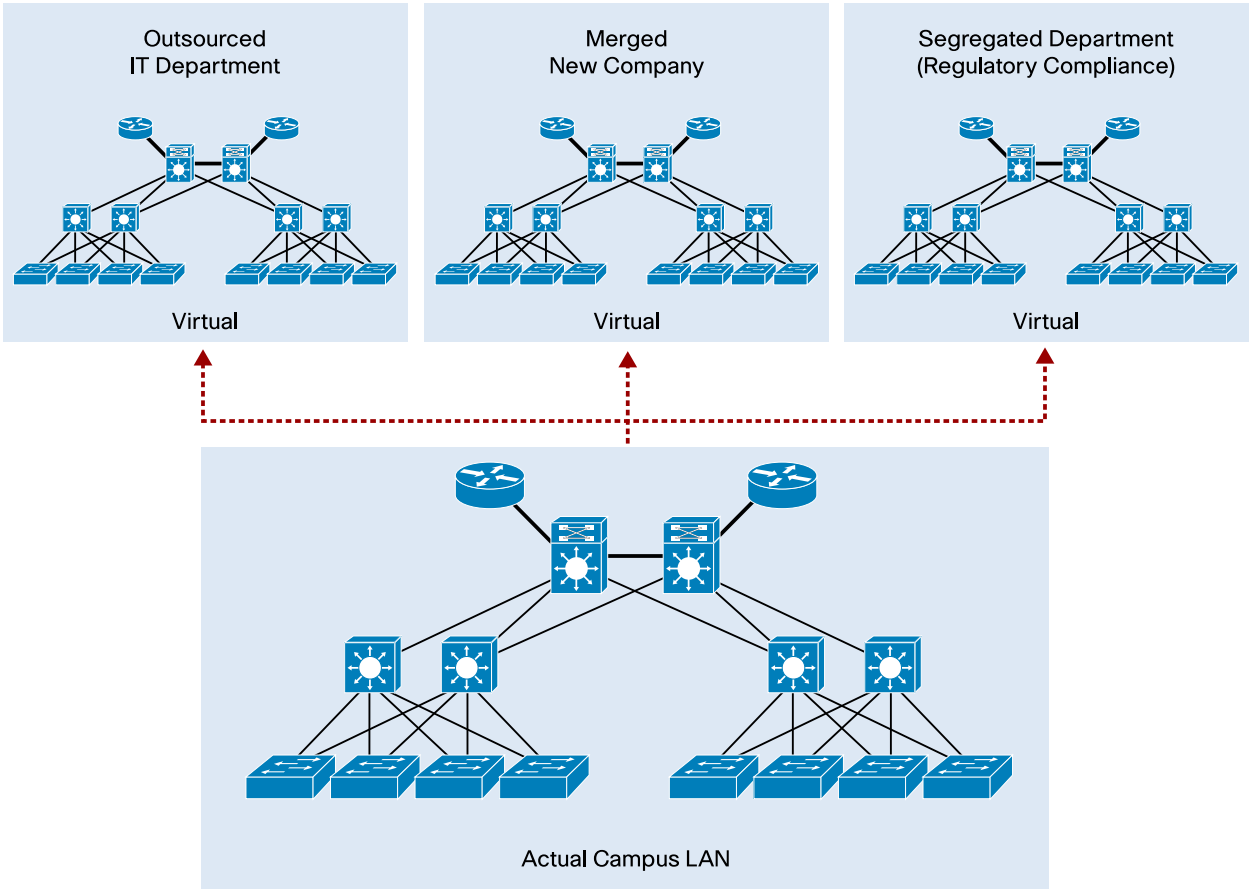
Network Services Virtualization

What Is Network Virtualization?

Business and IT leaders require a more responsive IT infrastructure that can help accelerate business initiatives and remove inefficiencies. To meet this challenge, the IT infrastructure needs to be based on an IT model with a new services delivery architecture that enables services as needed. It needs to evolve from a traditional campus architecture that delivers basic connectivity to separate, siloed departments into an agile, resilient, and adaptive architecture that delivers service orchestration. With these changes, the IT department becomes a business unit that delivers services to improve the enterprise rather than simply a cost center. The technology that helps deliver this new dynamic IT infrastructure is called *Network Virtualization* (Figure 1).

Figure 1. Network Virtualization



Business Challenges

In this new economy of globally distributed workforces and global competition, enterprises continue to use collaborative technologies to help connect geographically dispersed user groups so that they act and feel like a single, centralized entity. These collaborative technologies improve employee productivity while reducing operating expenses by creating the notion of a borderless enterprise in which employees, customers, and partners all share significant information and connect their business processes efficiently.

Adoption of collaborative technologies demands the network infrastructure to:

- **Be agile:** IT leaders are looking for ways to be more responsive to changing market dynamics, requiring them to accelerate deployment of new applications such as video conferencing equipment to help reduce travel costs. To accomplish this, they are looking at new service delivery options that can provide incremental services on the same infrastructure, achieving better device utilization.
- **Connect a globally distributed workforce, with ubiquitous devices and omnipresent users:** Users expect more control over when and how they work, with an increasing emphasis on service delivery.
- **Manage growth in user groups that need similar services:** As the number of groups increases, keeping them separate and secure is a challenge that IT leaders must continue to address.
- **Reduce operating expenses:** IT needs to increase asset utilization and simplify services provisioning.
- **Become energy efficient:** IT needs to control the power and cooling requirements for the network infrastructure and service nodes.

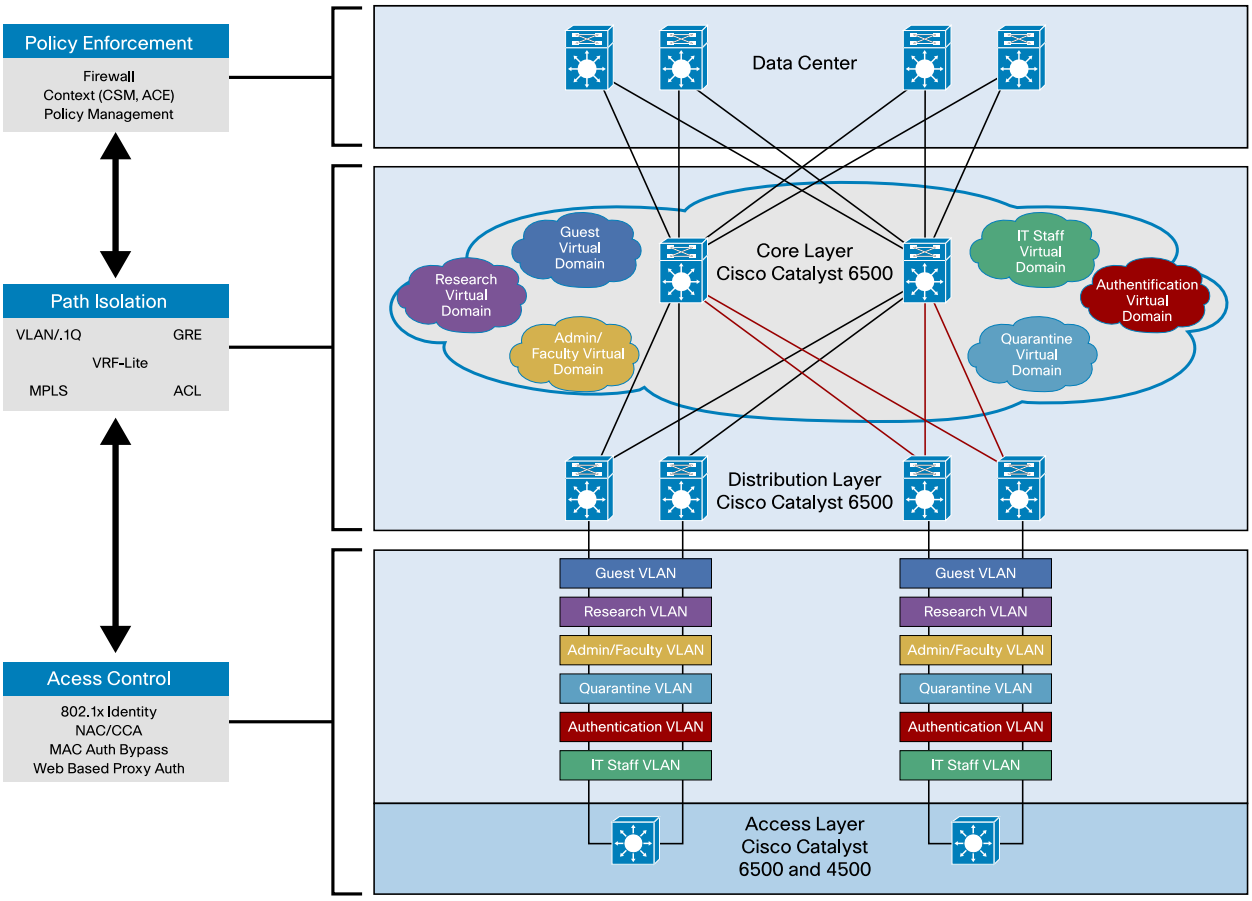
Cisco Network Virtualization Architecture

The concept of virtualization is not new and has been employed since the days of mainframe computers. It has been widely deployed as part of data center network designs and is seeing increasing adoption in campus networks. Network services virtualization within the campus helps IT focus on providing a unique set of policies to different network segments without having to deploy dedicated service nodes.

Network virtualization architecture has three main components (Figure 2):

- **Network access control and segmentation of classes of users:** Users are authenticated and either allowed or denied into a logical partition. Users are segmented into employees, contractors and consultants, and guests, with respective access to IT assets. This component identifies users who are authorized to access the network and then places them into the appropriate logical partition.
- **Path isolation:** Network isolation is preserved across the entire enterprise: from the edge to the campus to the WAN and back again. This component maintains traffic partitioned over a routed infrastructure and transports traffic over and between isolated partitions. The function of mapping isolated paths to VLANs and to virtual services is also performed in component.
- **Network Services virtualization:** This component provides access to shared or dedicated network services such as security, quality of service (QoS), and address management (Dynamic Host Configuration Protocol [DHCP] and Domain Name System [DNS]). It also applies policy per partition and isolates application environments, if required.

Figure 2. Cisco Network Virtualization Architecture



What Is Network Services Virtualization?

Network services virtualization is a critical building block in network virtualization. Although all the building blocks can be deployed in isolation, network services virtualization is an excellent strategy for consolidating multiple appliances into one, simplifying network operations and reducing overall acquisition cost. Network services virtualization virtualizes a network service node such as a firewall module, for example, by partitioning the available hardware resources among different virtual firewalls. The service virtualization provides independent instances of name space, configuration, inspection engines, and other resources within each instance. Network services virtualization negates the need to acquire separate devices every time the network service is required by using the software instance on the same physical hardware. Some implementations such as the Cisco Catalyst® 6500 Series Firewall Services Module (FWSM) can support nearly 250 separate virtual firewall instances.

Network services virtualization provides numerous business and IT benefits:

- **Efficient utilization:** Acquisition cost is reduced as network services delivery is removed from a physical device to a virtual context, extending its access without the need to deploy specialized hardware for every instance of the network service that is required. From an expense-management perspective, users see:
  - Reduced total cost of ownership (TCO) and increased return on investment (ROI) through improved asset utilization, achieved by enabling additional capabilities within existing infrastructure
  - Pay-as-you-grow licensing model for the virtualized service, giving the end user greater flexibility in deploying the right number of virtual instances; further, it is easy to scale to a greater number of instances if future needs increase

- **Green:** Reduced power consumption is achieved by consolidating multiple service instances into a single physical device without requiring deployment of dedicated hardware for each instance. Eliminating the need for additional physical devices effectively removes the need for additional power supplies, cooling, and rack space that would otherwise have been required.
- **Manageability:** Virtual service instances offer simplified provisioning. To enable a particular service within existing siloed infrastructure requires addition of network infrastructure equipment and changes to network cabling. With the network service virtualization approach, a virtual service node instance can be created on the same physical infrastructure without the need for additional network cabling. The management interface becomes more flexible as many network service instances can be managed as one, or each instance can have its own, separate management interface.
- **Regulatory compliance:** Compliance with regulations such as Health Insurance Portability and Accountability Act (HIPAA), Office of the Controller of the Currency (OCC) rules, and Sarbanes-Oxley require customers to segment their network services on a group basis. This segmentation of network services helps ensure that the security, QoS, and traffic path manipulation of one group is different from the other groups within the enterprise.

Network Services Virtualization: Before and After

Consider a typical enterprise before it implements virtualization. Its choices are to share everything or nothing. If it uses a single physical services node (for example, a firewall), applications must compete for resources, changes to one policy can affect the others, and device configuration is complex. Adding more physical service nodes creates an inefficient isolation of applications and results in device sprawl, underutilized resources, and complexity in upgrading.

With a virtualized architecture, such as that enabled by Cisco® products, abstraction and partitioning allow one physical network service node to provide multiple virtual contexts, enabling isolated, secure applications with essentially guaranteed resources and role-based access. This approach results in dramatic reductions in provisioning cycles, operating expenditures (OpEx), and power requirements.

Network Services Virtualization – Cisco Catalyst 6500

Virtualized network services available on the Cisco Catalyst 6500 series platform include:

- **Network security virtualization through multicontext virtual firewall contexts, also called security contexts:** Each security context is an independent firewall with its own security policy, interfaces, and administrators. The overall system resources within a single physical firewall can be administrated separated for other contexts. This system resource administration is required to make sure that no context inadvertently affects another context.
- **Virtual Route Forwarding (VRF) network services:** VRF-aware network services include:
  - VRF-Aware Address anagement services; VRF-aware DHCP helps enable pervasive DHCP policies for groups of geographically dispersed users
  - Optimized traffic redirection using VRF-aware Policy-Based Routing (PBR) and PBR-set VRF
  - Facilitating operational manageability with VRF-aware syslog and VRF Aware Telnet. , facilitating operational manageability

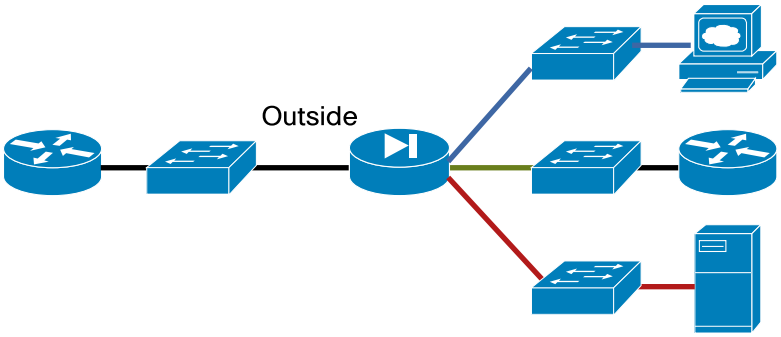
Network Security Virtualization: Firewalls

Network security using firewalls has evolved from a process that limit access to secure data and networks beginning with simple access lists to a technology that provides context-based stateful application inspection capabilities.

Evolution to Firewall Virtualization:

Conventional Stand-alone Firewalls: Conventional firewalls allow users to apply security policies on the data passing between networks (that is, the interfaces of a firewall). In the conventional firewall case, the firewall applies a single set of policies for traffic traveling between the inside and the outside interface (Figure 3).

Figure 3. Conventional Firewalls



Firewall Virtualization:

Virtualization in its simplest form can be achieved by supporting IEEE 802.1q VLAN tags on the same physical interface. IEEE 802.1q support on firewalls allows customers to easily integrate into existing networks that have already been segmented using VLANs (IEEE 802.1q VLANs).

Virtualization techniques have evolved far beyond traditional VLAN integration. Virtualization at the next level involves partitioning a single physical firewall into multiple virtual firewalls, known as the security contexts. Today's virtualization technologies enable an abstraction layer that decouples the security policies from the physical hardware to deliver greater network resource utilization and flexibility. Virtualization allows multiple virtual machines, with heterogeneous security policies, to run independently and simultaneously on the same physical firewall hardware module. Each virtual context has its own set of virtual interfaces to which the security policies can be applied. Each security context is an independent firewall, with its own security policy, interfaces, and administrators.

Targeted Firewall Virtualization Applications

Multiple security contexts are useful for both enterprise campus and data center deployments. IT departments managing internal campus networks can now partition a physical firewall into multiple contexts for each group of users (either segmenting them by role or by business unit) without investing in a dedicated physical firewall for each group. Each individual context can be configured based on the group's security policies without affecting other contexts. IT managers can also allocate the firewall's shared resources such as bandwidth, total connections, and memory to each of the contexts based on customer needs and the needs of each group.

Cisco Catalyst 6500 Series FWSM Virtualization Architecture

The Cisco Catalyst 6500 Series Firewall Services Module allows the customer to configure up to 250 mixed-mode multiple virtual firewalls. These contexts can be routed firewalls (Layer 3) or transparent firewalls (Layer 2, or stealth) as well as mixed-mode firewalls, which are a combination of both Layer 2 and Layer 3 firewalls coexisting on the same physical firewall. Each virtual firewall is called a context because it is one partition or instance of a fully functional firewall. Even though all the configured contexts are emulated by a single firewall CPU, the traffic inspection and security policies of each context are independent of each other, as if being handled by a dedicated physical firewall. Therefore, each context can be configured and managed by different administrators, or they can all be managed by one administrator who has access to each of the contexts.

The capability to run multiple security contexts on single Cisco Catalyst 6500 Series FWSMs helps customers limit the cost of additional hardware. Multiple firewall contexts can be added in the module on the basis of the license

limits. To effectively share the system resources across all contexts, the administrator can allocate system resources such as connections and seconds as a percentage or an absolute number for each individual context.

Figures 4 and 5 show how the internal architecture of the Cisco Catalyst 6500 Series FWSM functions before and after virtualization.

Figure 4. Single Firewall Before Virtualization

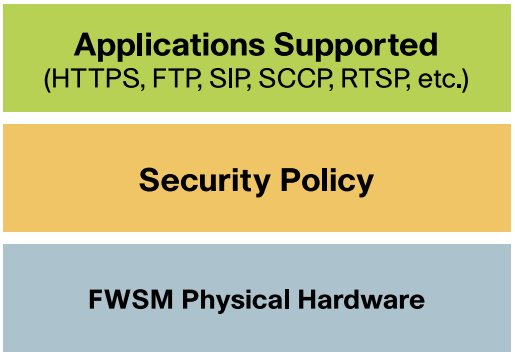


Figure 5. Firewall Virtualization

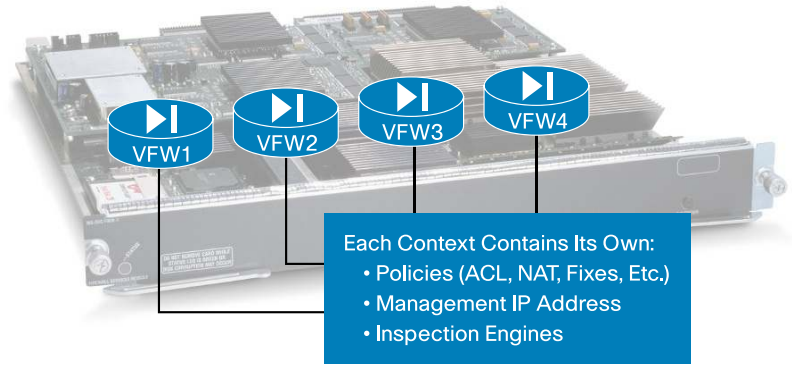
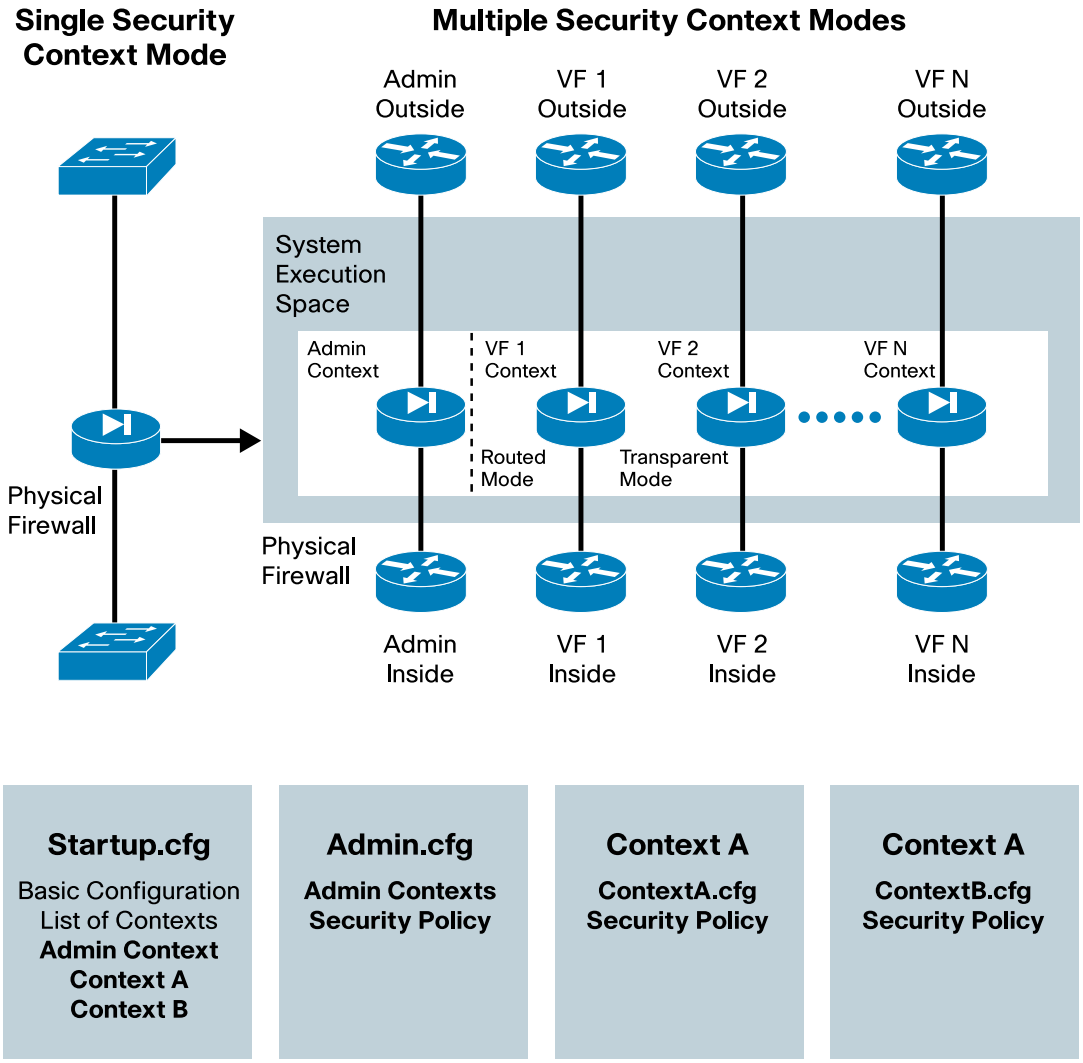


Figure 6 shows how a single Cisco Catalyst 6500 Series FWSM can be organized into multiple security contexts, both routed and transparent, creating virtual firewalls (VFs).

Figure 6. Virtualized Firewall



Multiple Virtual Contexts

Network Services Virtualization: VRF-Aware Services

The Cisco Catalyst 6500 and 4500 Series Switches enable VRF support for features that help provide network services. Main functions include:

- **Ease of operational manageability within VRF instances**: The Cisco Catalyst 6500 Series supports features that enable switch management within a VRF instance. Main features include:
  - **NetFlow on VRF interfaces:** Allows NetFlow statistics collection on interfaces that are part of a VRF instance
  - **VRF-aware syslog:** Allows the switch to send system logging (syslog) messages to a syslog server host connected through a VRF interface
  - **VRF-aware Telnet:** Allows the management interface to be part of a VRF instance instead of the global interface list

  - **VRF-aware TACACS:** Allows the authentication, authorization, and accounting (AAA) TACACS server to be part of the VRF instance; the switch should be able to send AAA messages to an AAA server within a VRF instance
- **Virtualized address management policies using VRF-aware DHCP:** This feature helps enable pervasive DHCP policies for groups of geographically dispersed users.
- **Optimized traffic redirection using PBR-set VRF:** This feature helps segment and redirect traffic from the global routing table to a VRF instance.

Conclusion

Cisco offers a proven, end-to-end Network virtualization solution that spans the entire network infrastructure, from the backbone to every endpoint. Using the Cisco Network Virtualization architecture, organizations can reap the benefits of end-to-end virtualization and policy-driven service orchestration. This shared services architecture enables flexibility and agility while streamlining resources and reducing operational expenses.

The Cisco Catalyst 6500 platform is a key component of the Cisco Network Virtualization architecture which allows customers to manage the networks services, making it easier and faster to enable new network services. The Cisco Catalyst 6500 has a broad range of hardware and software features that enable customers to deploy virtualization across all places in the network to help reduce the management complexity of services including Unified Communications, mobility, and security.

For More Information

Go online to learn more about Cisco Network virtualization solutions: www.cisco.com/go/networkvirtualization.

Network Services Virtualization design guides:
http://www.cisco.com/en/US/docs/solutions/Enterprise/Network_Virtualization/ServEdge.html

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

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.

Printed in USA C11-531522-00 04/09