Cisco Application Control Engine and Cisco Nexus 7000 Series Multi-tenancy

What You Will Learn

As the IT landscape rapidly changes, cost reduction pressures, focus on time to market, and employee empowerment are leading enterprises and IT service providers to develop innovative strategies to address these challenges. In existing deployments, environments that needed additional security and isolation required separate sets of equipment and infrastructure. Although this approach provided the required separation, efficiency dropped significantly due to lower utilization, while costs increased due to higher management and capital expenditures. The multi-tenant architecture addresses these concerns through a secure, isolated multi-tenant solution at every network layer.

Challenge

As enterprise IT environments have dramatically grown in scale, complexity, and diversity of services, they have typically deployed application and customer environments in silos of dedicated infrastructure. These silos are built around specific applications, customer environments, business organizations, and operational requirements. For example:

- Universities need to separate student user services from business operations, student administrative systems, and commercial or sensitive research projects.
- Telcos and service providers must separate billing, customer relationship management (CRM), payment systems, reseller portals, and hosted environments.
- Financial organizations need to securely isolate client records and investment, wholesale, and retail banking services.

Enabling enterprises and service providers to migrate such environments to a multi-tenant architecture requires the capability to provide secure isolation while still delivering the management and flexibility benefits of shared resources. Enterprises and external service providers must enable all customer data, communication, and application environments to be securely isolated from other tenants. With external providers, the separation must be so complete and secure that the tenants can have no visibility to each other. Enterprises must deliver the secure separation required for their organizational structure, applications, and regulatory compliance.

© 2011 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Cisco Solution

Multi-tenancy is the capability to logically partition a single physical device into many virtual devices. Each virtual device must have all the capabilities of the actual physical device, and each virtual device must be independent and isolated so that it appears to be a unique physical device from the viewpoint of the network and the network administrator. With virtualization, each virtual device can be allocated its own resources and quality of service (QoS). Each virtual device can also be assigned its own configuration files, management interfaces, and access-control policies in which access control privileges are assigned to users based on their administrative roles.

The Cisco® Application Control Engine (ACE) and Cisco Nexus® switch families offer features tailored to virtual environments, allowing consistent visibility, control, and isolation of the application stack within a multi-tenant architecture.

Benefits of Multi-tenancy with Cisco ACE and Cisco Nexus 7000 Series Switches

Accelerated and Lower-Cost Application Rollout and Upgrades

With the Cisco ACE and Cisco Nexus 7000 Series, rolling out a new application or adding application support for another department simply requires the addition of a new virtual partition to create another virtual device within the existing physical device, rather than deployment of an additional hardware platform.

Complete Isolation of Applications, Departments, and Customers

With Cisco multi-tenancy, administrators have the flexibility to allocate resources to virtual devices in any way they choose. For example, one administrator may want to allocate a virtual device for every application deployed. Another administrator may want to allocate a virtual device for each department's use, even for multiple applications. A service provider administrator may want to allocate a virtual device for each customer. Regardless of how resources are allocated, Cisco ACE and Cisco Nexus 7000 Series virtual devices are completely isolated from each other. Configurations in one virtual device do not affect configurations in other virtual devices. As a result, virtual partitioning provides a novel way of protecting a set of services configured in several virtual devices from accidental mistakes, or from malicious configurations, made in another virtual device. A configuration failure on a Cisco multi-tenancy device is limited to the scope of the virtual device in which the configuration was created. A failure in one virtual device has no effect on other virtual devices, increasing uptime for critical applications. Note that with competitors' offerings, customers need to purchase and deploy additional physical units to achieve this level of configuration isolation for applications, departments, and customers.

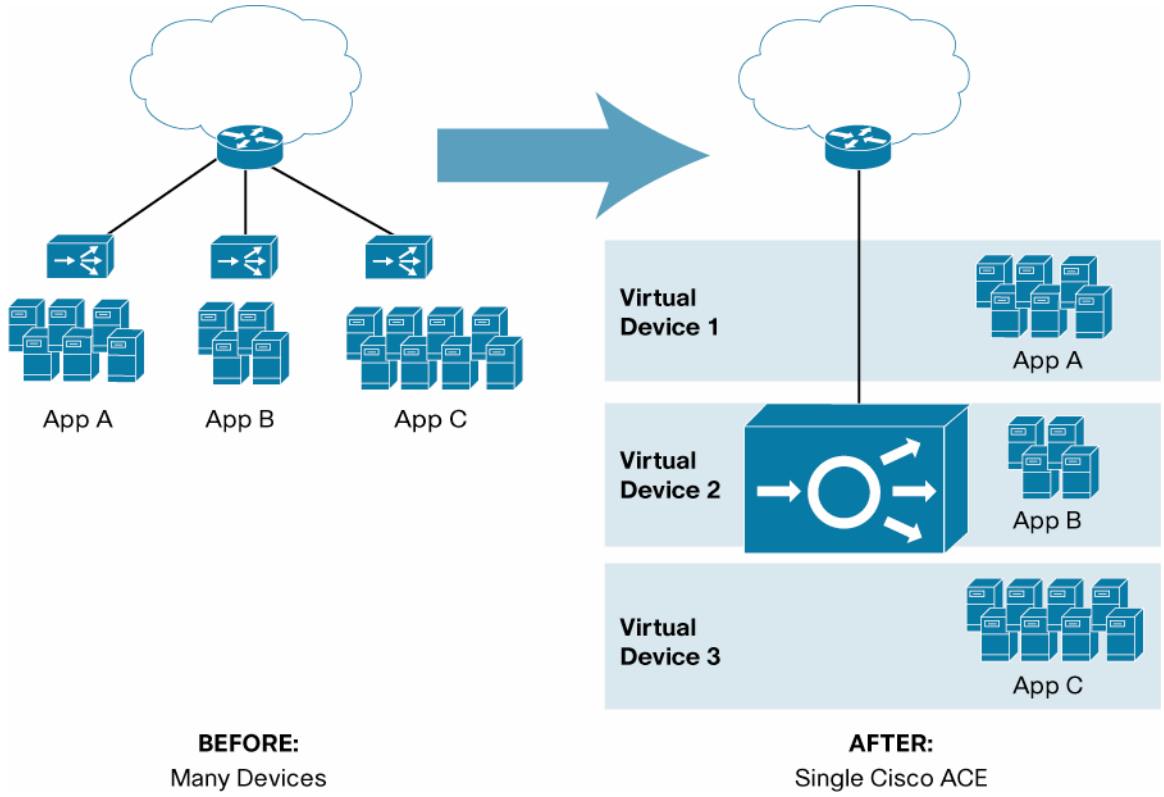
Reduced Data Center Resource Requirements

The unique multi-tenancy capabilities of the Cisco ACE and Cisco Nexus 7000 Series enable customers to drastically reduce both physical and environmental data center resources, resulting in significant overall cost savings associated with application delivery. The Cisco ACE and Cisco Nexus 7000 Series allow administrators to roll out additional network aggregation nodes and applications simply by configuring additional virtual devices within the same physical device, rather than having to deploy additional hardware platforms. As a result, network sprawl is reduced, and additional cabling requirements and incremental rack space requirements are eliminated. Multi-tenancy reduces the number of physical devices in the network, and therefore it also significantly reduces power consumption and costs in the data center.

The unique virtualization capabilities of the Cisco ACE Module enable enterprises and service providers to accelerate and scale application deployments, reduce costs in the data center, simplify application delivery network architectures, and delegate application delivery management tasks. Figure 1 shows how multi-tenancy can be achieved with Cisco ACE.

© 2011 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Figure 1. Consolidating Multiple Functions with Cisco ACE



Cisco Nexus 7000 Series virtual device contexts (VDCs) can be used to consolidate parallel physical devices that share the same functional role characteristics across one or more administrative domains or service areas. An example of this type of horizontal consolidation is the consolidation of aggregation switches in a data center that delivers service to three different service groups such as business units in an enterprise or, in the case of a service provider environment, multiple customers. In a traditional configuration, each service group's data center access domain would be isolated from that of the other service groups through physically independent aggregation devices. Figures 2 and 3 show how physical topology can be consolidated with Cisco Nexus 7000 Series VDCs.

© 2011 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Figure 2. Typical Physical Topology (Before)

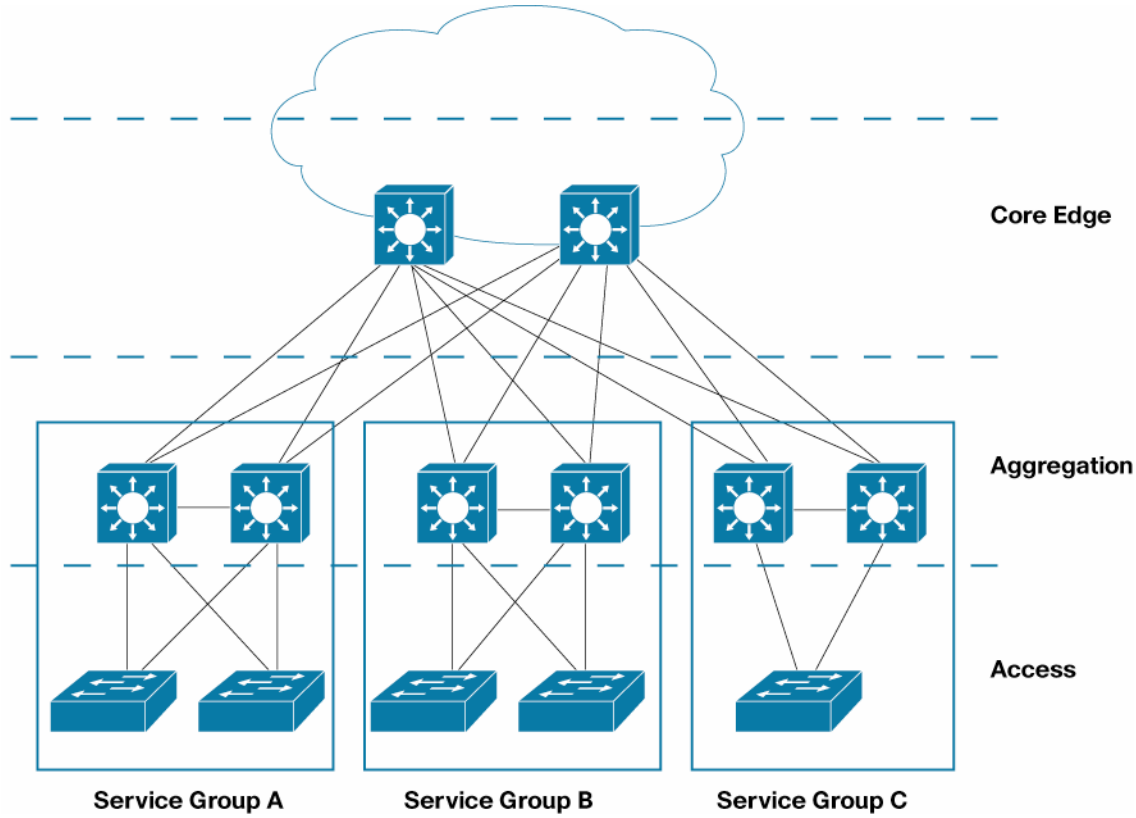
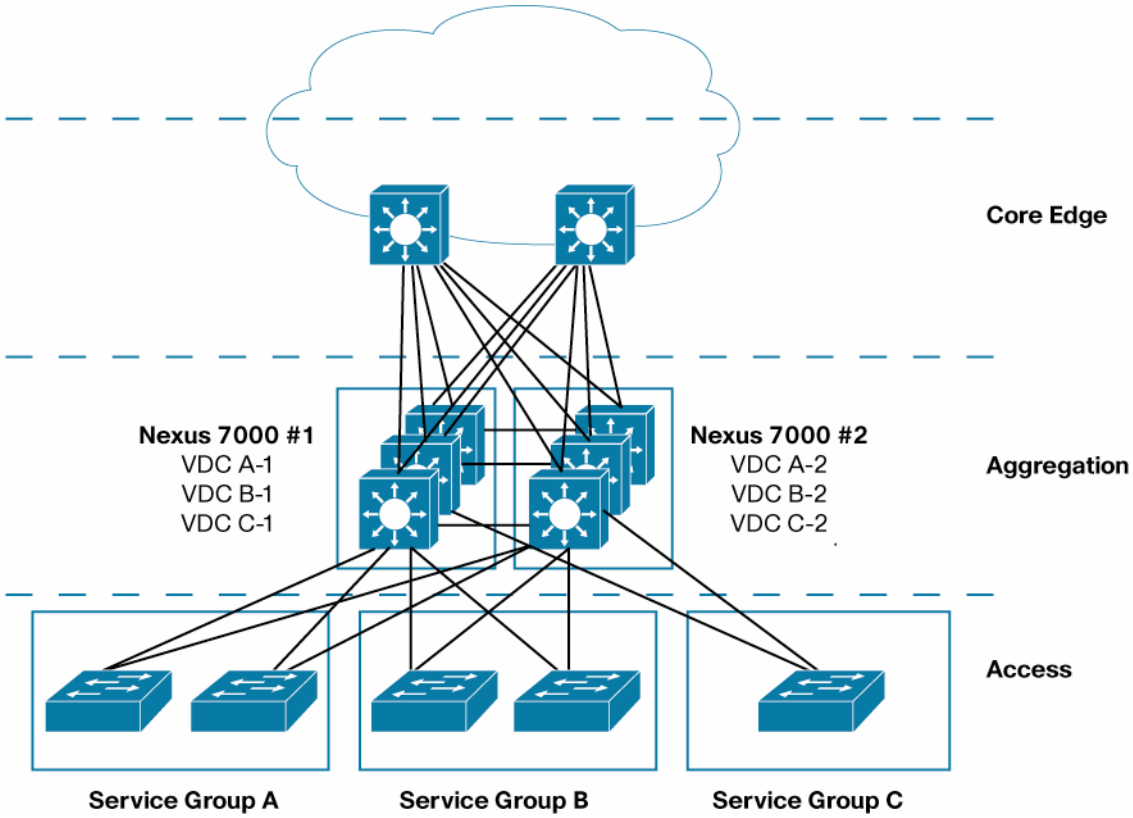


Figure 3. Horizontal consolidation with Cisco Nexus 7000 Series VDCs



© 2011 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Cisco Solution Design

Hierarchical network design has been commonly used in networking for many years. This model uses redundant switches at each layer of the network topology for device-level failover that creates a highly available transport between end nodes using the network. Data center networks often require additional services beyond basic packet forwarding, such as server load balancing, firewall, or intrusion prevention. These services may be introduced as modules populating a slot of one of the switching nodes in the network or as standalone appliances. Each service approach also supports the deployment of redundant hardware to preserve the high-availability standards set by the network topology. Taking a modular approach to data center design provides flexibility and scalability in both network topology design and utilization of physical resources.

Figure 4 shows the primary network switching layers of the hierarchical network design reference model for the data center environment. The design consists of three layers: core, aggregation, and access. The service layer can be attached to the aggregation layer as a service node.

Figure 4. Hierarchical Network Design Reference Model

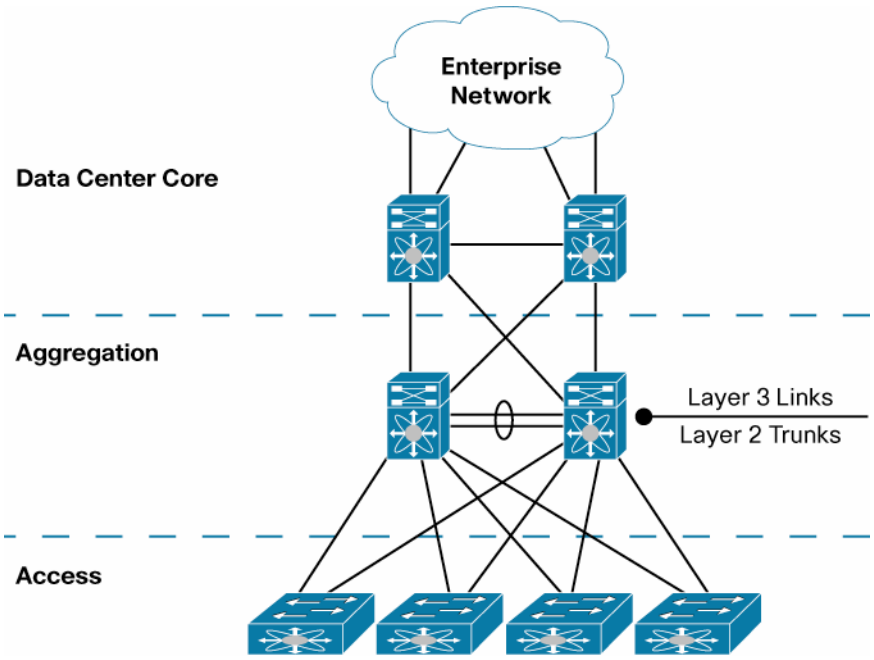
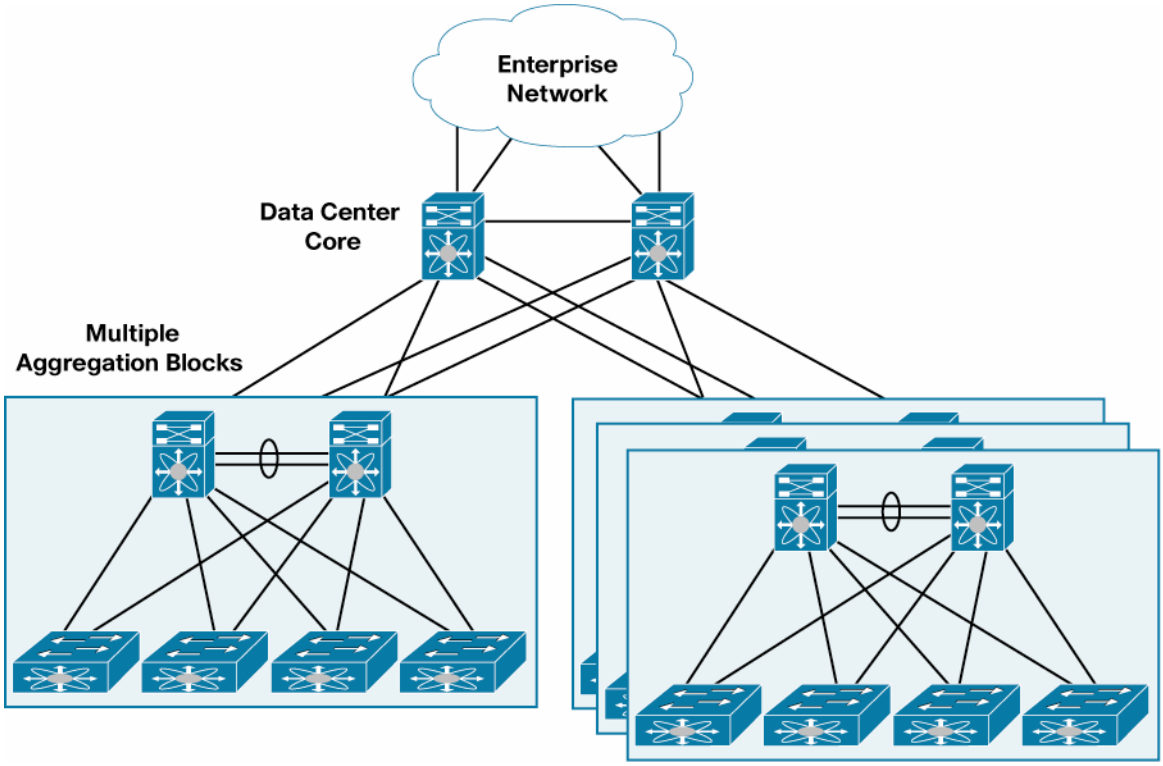


Figure 5 shows how the data center topology can be scaled with a dedicated core and multiple aggregation blocks.

© 2011 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Figure 5. Scaling the Data Center with a Dedicated Core



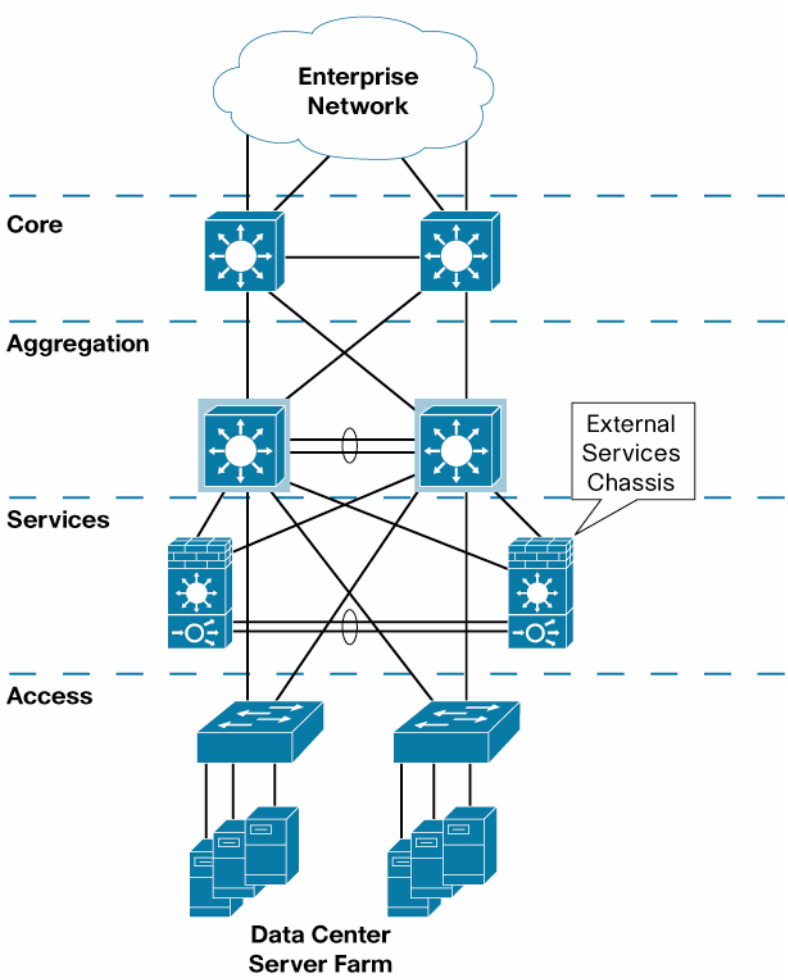
Cisco Nexus 7000 Series VDCs can be used to consolidate parallel physical devices that share the same functional role characteristics across one or more administrative domains or service areas. An example of this type of horizontal consolidation is the consolidation of aggregation switches in a data center that delivers service to three different service groups such as business units in an enterprise or, in the case of a service provider environment, multiple customers. In a traditional configuration, each service group's data center access domain would be isolated from the other service groups through physically independent aggregation devices. This isolation can be performed to satisfy availability requirements or service-level agreements (SLAs) on a per-group or customer basis. An alternative design for this deployment is to use Cisco Nexus 7000 Series VDCs to create virtualized logical aggregation devices within a single physical platform.

This configuration can provide some facility resource utilization advantages by optimizing the use of space, power, and cooling while delivering isolation comparable to separate devices between service groups.

As the data center network grows and needs to be scaled up over time, demands may be made to recover the slots that are being consumed by the service modules, to accommodate greater port density in the aggregation layer. This slot recovery would allow aggregation of a greater number of access-layer switches without the need to move to a second aggregation block. One approach is to integrate all the services into an additional pair of Cisco Catalyst® 6500 Series Switches adjacent to the aggregation layer of the data center network. These switches are commonly referred to as services chassis. Figure 6 illustrates the service chassis model.

© 2011 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Figure 6. External Service Chassis Model

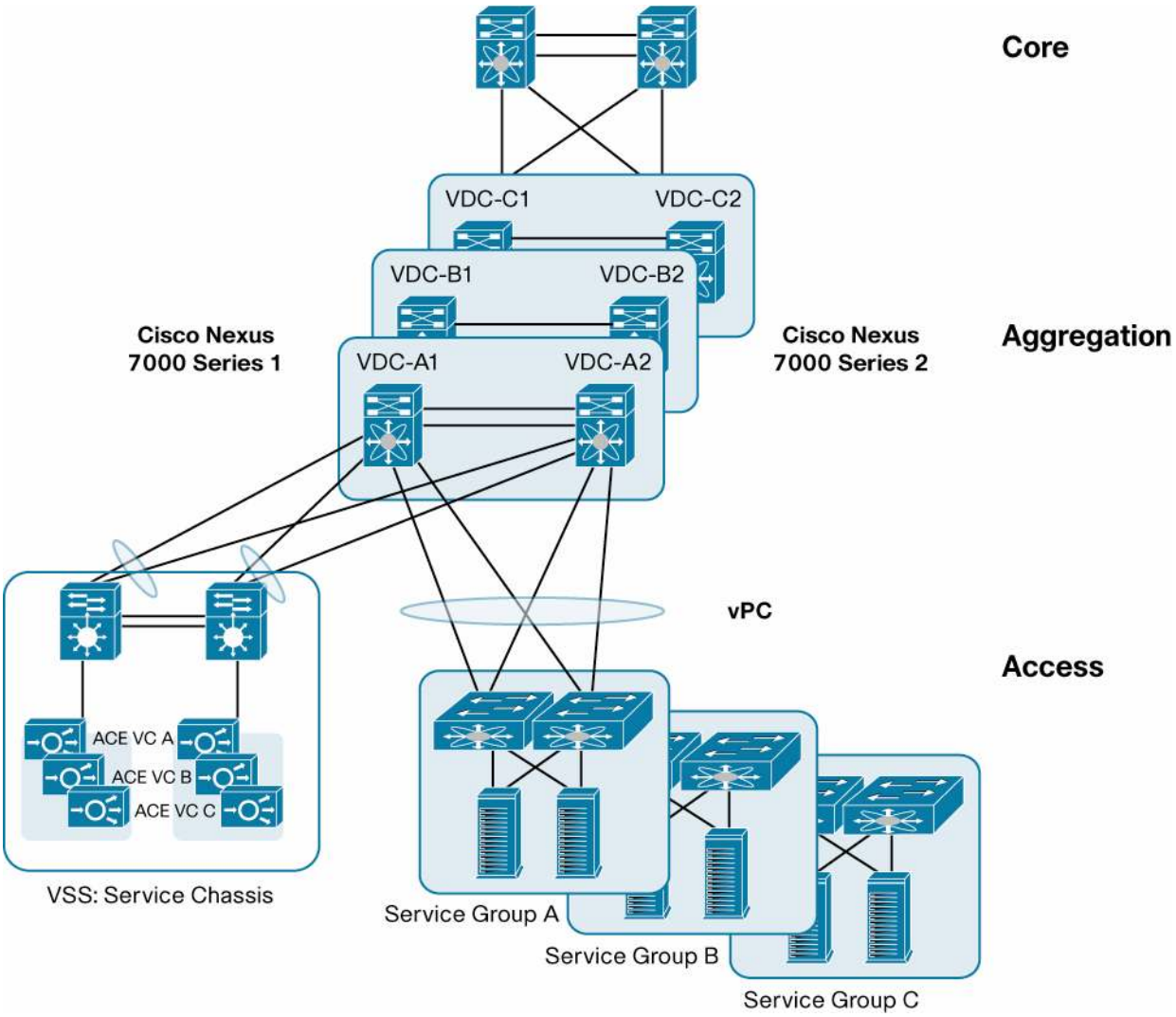


In this solution, two external service chassis will be part of one virtual switching system (VSS). The VSS combines two physical Cisco Catalyst 6500 Series Switches into one virtualized switch. This arrangement enables a unified control plane and also allows both data planes to forward simultaneously. VSS introduces Multichassis EtherChannel (MEC), allowing a PortChannel to be formed across two physical switches. A virtual PortChannel (vPC) and VSS both provide enhanced system availability through redundant systems, eliminate reliance on Spanning Tree Protocol, achieve faster convergence times, and enable full system availability at all times.

Figure 7 illustrates the Cisco multi-tenancy solution with Cisco ACE virtual contexts and Cisco Nexus 7000 Series VDCs. As shown in Figure 7, the topology uses three service groups. Each service group can be a separate organization or department within an enterprise. In the traditional model, there are three separate switches, each for one organization, in the aggregation layer, and also three separate load-balancers in the service layer. With Cisco Nexus 7000 Series VDCs and Cisco ACE virtual contexts, the aggregation layer can be horizontally consolidated with one Cisco Nexus 7000 Series Switch, and the service layer can be consolidated with VSS. As shown in Figure 7, service groups A, B, and C are isolated at the aggregation layer with VDC A, B, and C and at the service layer with Cisco ACE virtual contexts A, B, and C.

© 2011 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Figure 7. Cisco ACE and Cisco Nexus 7000 Series Multi-Tenancy Solution with VSS



Core Layer

The core layer of the solution is primarily focused on stability and high-performance Layer 3 IP-packet forwarding. It provides a layer of insulation between the aggregation layer and other places in the network. The core of a data center network is typically divided into a pair of high-performance, highly available chassis-based switches. In larger or geographically dispersed network environments, the core is sometimes extended to contain additional switches. The recommended approach is to scale the network core continuing to use switches in redundant pairs. The primary function of the data center network core is to provide highly available, high-performance Layer 3 switching for IP traffic among the other functional blocks of the network, such as the campus, Internet edge, and WAN. By configuring all links connecting to the network core as point-to-point Layer 3 connections, rapid convergence around any link failure is provided, and the control plane of the core switches is not exposed to broadcast traffic from end-node devices or required to participate in spanning tree for Layer 2 network loop prevention.

Cisco's premier switching platform for the data center core is the Cisco Nexus 7000 Series Switches. The Cisco Nexus 7000 Series has been designed from the start to support the stringent uptime requirements of the data center. The Cisco Nexus 7000 Series Switches are optimized to support high-density 10 Gigabit Ethernet, providing scalability in the 18-slot chassis of up to 128 wire-rate 10 Gigabit Ethernet interfaces when ports are configured in a dedicated mode using the Cisco Nexus 7000 Series 32-Port 10Gb Ethernet Module, 80Gb Fabric. The Cisco Nexus 7000 Series hardware is coupled with Cisco NX-OS Software, a modular operating system also designed specifically

© 2011 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

for the requirements of today's data center networks. Cisco NX-OS is built on the industry-proven Cisco MDS 9000 SAN-OS Software, adding virtualization, Layer 2, and Layer 3 features and protocols required in the data center environment. Cisco NX-OS includes high-availability features, such as granular process modularity, In-Service Software Upgrade (ISSU), and stateful process restart, that are specifically targeted at the service-level requirements of the enterprise or service provider data center.

Aggregation Layer

The aggregation layer of the data center provides connectivity for the access-layer switches in the server farm and aggregates them into a smaller number of interfaces to be connected to the core layer. In most data center environments, the aggregation layer is the transition point between the purely Layer 3 routed core layer, and the Layer 2 switched access layer. IEEE 802.1Q trunks extend the server farm VLANs between the access and aggregation layers.

The aggregation layer also provides a common connection point for inserting services into the data flows between clients and servers, or between tiers of servers in a multi-tier application. The Cisco Nexus 7000 Series offers unique virtualization features such as VDCs and vPCs that are critical for aggregation-layer switches. As shown in Figure 7, three VDCs are used in the solution to segregate three different service groups inside the same physical Cisco Nexus 7000 Series Switch. Horizontal collapsing of the aggregation layer with VDCs has a significant effect on the data center space, power, and cooling, as discussed previously.

Access Layer

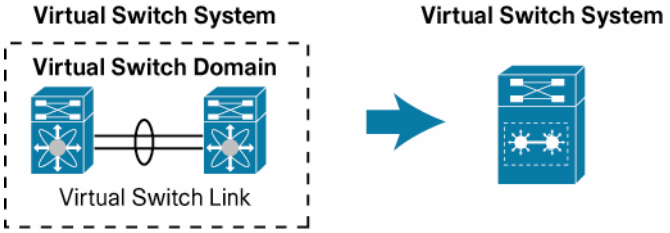
The access layer provides the physical-level attachment to the server resources and operates in Layer 2 or Layer 3 mode. The mode plays a critical role in meeting particular server requirements such as network interface card (NIC) teaming, clustering, and broadcast containment. The access layer is the first oversubscription point in the data center because it aggregates the server traffic onto Gigabit EtherChannel or 10 Gigabit Ethernet and 10 Gigabit EtherChannel uplinks to the aggregation layer. Spanning tree or Layer 3 routing protocols are extended from the aggregation layer into the access layer, depending on which access-layer model is used. Cisco recommends implementing access-layer switches logically paired in groups of two to support server redundant connections or to support diverse connections for production, backup, and management Ethernet interfaces.

Service Layer

As illustrated in Figure 7, the service layer is implemented using VSS. The VSS technology allows the grouping of two Cisco Catalyst 6500 Series Switches into a single virtual switch. A VSS system provides physical infrastructure redundancy while simultaneously simplifying the logical topology of the data center.

Figure 8 illustrates the concept of VSS. The left side of Figure 8 represents the physical layout of the VSS: two Cisco Catalyst 6500 Series Switches are physically connected through a virtual switch link (VSL). The two switches are members of a virtual switch domain, and as the right side of the figure shows, this construct forms a single logical switch with a single control plane: a virtual switching system.

Figure 8. Virtual Switch System



© 2011 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

The primary benefits of this logical grouping include the following:

- Increased operational efficiency of a simplified network using virtualization
- Increased availability and forwarding performance through interchassis stateful switchover (SSO) and nonstop forwarding (NSF)
- Increased availability and forwarding performance through MEC

The VSS will be used as a Layer 3 isolated service block with the following flexibility advantages:

- Reduced topology complexity: loop free
- Service module integration
- Up to 50 percent reduction in packet hopping between the routing node and the service node

Cisco ACE is inserted in the VSS as a service module. Cisco ACE supports a variety of topologies: routed mode, bridge mode, one-armed mode, etc. In the solution shown in Figure 7, Cisco ACE is used in a one-armed mode topology. The one-armed Cisco ACE can be introduced transparently into the network and will not be in the path of other traffic that does not need to go to the virtual IP addresses. Cisco ACE failure or failover affects only traffic that is being load-balanced or that uses other Cisco ACE application services such as SSL acceleration. A traffic-diversion mechanism is required to help ensure that both sides of a protocol exchange pass through the Cisco ACE; either Policy-Based Routing (PBR) or Source-Address Network Address Translation (Source-NAT) may be used. Source-NAT is recommended in this solution.

Conclusion

Multi-tenancy is a crucial requirement for scalable, reliable, and cost-effective application delivery and infrastructure services in the data center. Enterprises and service providers alike can reap significant cost reduction and application deployment acceleration benefits with the Cisco ACE Module and Cisco ACE 4710 appliance. Cisco ACE is the only solution on the market today that provides true application delivery virtualization capabilities. Cisco Nexus 7000 Series VDCs offer a great amount of flexibility with design options to optimize the use of existing or new data center space. With facility resources quickly becoming limiting factors in overall design scalability, having additional tools available to increase utilization while being able to preserve operations and service delivery organizational structure is critical. VDCs on the Cisco Nexus 7000 Series are a critical feature that offers these benefits to the network architect and engineer while remaining transparent to operations.

For More Information

- **Data center design—IP network infrastructure:** http://www.cisco.com/en/US/docs/solutions/Enterprise/Data_Center/DC_3_0/DC-3_0_IPInfra.html
- **Security and virtualization in the data center:** http://www.cisco.com/en/US/docs/solutions/Enterprise/Data_Center/DC_3_0/dc_sec_design.html
- **Integrating the VSS in the Cisco data center infrastructure:** http://www.cisco.com/en/US/docs/solutions/Enterprise/Data_Center/vssdc_integrate.html
- **Implementing the Cisco Nexus 7000 Series in the data center aggregation layer with services:** http://www.cisco.com/en/US/docs/solutions/Enterprise/Data_Center/nx_7000_dc.html

© 2011 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

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.**

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned 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. (1005R)

Printed in USA C22-643591-00 1/11

© 2011 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.