Newer Cisco SBA Guides Available

This guide is part of an older series of Cisco Smart Business Architecture designs. To access the latest Cisco SBA Guides, go to http://www.cisco.com/go/sba

Cisco strives to update and enhance SBA guides on a regular basis. As we develop a new series of SBA guides, we test them together, as a complete system. To ensure the mutual compatibility of designs in Cisco SBA guides, you should use guides that belong to the same series.
Who Should Read This Guide

This Cisco® Smart Business Architecture (SBA) guide is for people who fill a variety of roles:

- Systems engineers who need standard procedures for implementing solutions
- Project managers who create statements of work for Cisco SBA implementations
- Sales partners who sell new technology or who create implementation documentation
- Trainers who need material for classroom instruction or on-the-job training

In general, you can also use Cisco SBA guides to improve consistency among engineers and deployments, as well as to improve scoping and costing of deployment jobs.

Release Series

Cisco strives to update and enhance SBA guides on a regular basis. As we develop a new series of SBA guides, we test them together, as a complete system. To ensure the mutual compatibility of designs in Cisco SBA guides, you should use guides that belong to the same series.

All Cisco SBA guides include the series name on the cover and at the bottom left of each page. We name the series for the month and year that we release them, as follows:

  month year Series

For example, the series of guides that we released in August 2011 are the “August 2011 Series”.

You can find the most recent series of SBA guides at the following sites:

  Customer access: http://www.cisco.com/go/sba
  Partner access: http://www.cisco.com/go/sbachannel

How to Read Commands

Many Cisco SBA guides provide specific details about how to configure Cisco network devices that run Cisco IOS, Cisco NX-OS, or other operating systems that you configure at a command-line interface (CLI). This section describes the conventions used to specify commands that you must enter.

Commands to enter at a CLI appear as follows:

  configure terminal

Commands that specify a value for a variable appear as follows:

  ntp server 10.10.48.17

Commands with variables that you must define appear as follows:

  class-map [highest class name]

Commands shown in an interactive example, such as a script or when the command prompt is included, appear as follows:

  Router# enable

Long commands that line wrap are underlined. Enter them as one command:

  wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100

Noteworthy parts of system output or device configuration files appear highlighted, as follows:

  interface Vlan64
    ip address 10.5.204.5 255.255.255.0

Comments and Questions

If you would like to comment on a guide or ask questions, please use the forum at the bottom of one of the following sites:

  Customer access: http://www.cisco.com/go/sba
  Partner access: http://www.cisco.com/go/sbachannel

An RSS feed is available if you would like to be notified when new comments are posted.
# Table of Contents

## What's In This SBA Guide
- About SBA .......................................................... 1
- About This Guide .................................................. 1

## Introduction
- Design Goals ..................................................... 3
- Business Overview ................................................ 3
- Technology Overview .............................................. 5

## Physical Environment
- Business Overview ................................................ 9
- Technology Overview .............................................. 9

## Ethernet Infrastructure
- Business Overview ................................................ 11
- Technology Overview .............................................. 11
- Deployment Details ................................................. 15
- Configuring Out of Band Management ......................... 15
- Configuring the Data Center Core ............................... 19

## Storage Infrastructure
- Business Overview ................................................ 33
- Technology Overview .............................................. 33
- Deployment Details ................................................. 33
- Configuring Fibre Channel SAN on Cisco Nexus 5500UP Switch ................................................. 35
- Configuring Cisco MDS 9148 Switch SAN Expansion ......................... 44
- Configuring for FCoE Host Connectivity ....................... 49

## Compute Connectivity
- Business Overview ................................................ 53
- Technology Overview .............................................. 53
- Cisco Nexus Virtual Port Channel ............................... 54
- Cisco Nexus Fabric Extender ..................................... 55
- Cisco UCS System Network Connectivity ..................... 56
- Single-Homed Server Connectivity ............................. 58
- Server with Teamed Interface Connectivity ................ 59
- Third-Party Blade Server System Connectivity ............. 59
- Summary ............................................................. 60
# Table of Contents

## Network Security ..........................................................61
- Business Overview .....................................................61
- Technology Overview ...................................................61
- Deployment Details .......................................................65
- Configuring Cisco ASA Firewall Connectivity ..................65
- Evaluating and Deploying Firewall Security Policy ..........69
- Deploying Cisco Intrusion Protection System (IPS) ..........71

## Application Resiliency ..................................................78
- Business Overview .....................................................78
- Technology Overview ...................................................79
- Deployment Details .......................................................80
- Configuring Connectivity to the Data Center Core Switches .80
- Configuring Cisco ACE Appliance Network .......................81
- Setting up Load Balancing for HTTP Servers ....................84
- Load Balancing and SSL Offloading for HTTPS Servers ....87

## Appendix A: Product List ...............................................92

## Appendix B: Changes ....................................................93
Cisco SBA helps you design and quickly deploy a full-service business network. A Cisco SBA deployment is prescriptive, out-of-the-box, scalable, and flexible.

Cisco SBA incorporates LAN, WAN, wireless, security, data center, application optimization, and unified communication technologies—tested together as a complete system. This component-level approach simplifies system integration of multiple technologies, allowing you to select solutions that solve your organization’s problems—without worrying about the technical complexity.

For more information, see the How to Get Started with Cisco SBA document:
The Cisco Smart Business Architecture for Midsize Organizations Data Center Foundation is a comprehensive architecture for networks with up to 2500 users. This out-of-the-box approach is simple, easy to use, affordable, scalable, and flexible. The architecture for the midsize data center builds upon the server room deployment detailed in the Cisco SBA for Midsize Organizations—Borderless Networks Foundation Deployment Guide.

The Cisco Smart Business Architecture for Midsize Organizations Data Center Foundation incorporates Ethernet, storage network, compute, security, and application resiliency tested together as a solution. This solution-level approach to building out an architecture simplifies the system integration normally associated with multiple technologies, allowing you to select the modules that meet your organization’s requirements rather than worrying about matching components and worrying about interoperability.

We have designed the Cisco SBA to be easy to configure, deploy, and manage. This architecture:

- Provides a solid foundation
- Makes deployment fast and easy
- Accelerates your ability to easily deploy new servers and additional services
- Avoids the need to re-engineer the network as your organization grows

This guide includes the following modules:

- The first module covers elements of the data center design regarding the physical environment. The aspects of power, cooling, mounting racks, and space required are outlined for consideration in your data center design.
- The Ethernet Infrastructure module establishes the foundation connectivity for your data center network as it outgrows the server farm size. This section focuses on building a central connection point for the application servers that drive the organization and the services that surround them. The Ethernet module explains how to configure Layer 2 and Layer 3 connectivity in the data center and the communications path to the rest of the organization.
- The Storage Networking module shows how the foundation Ethernet design accommodates IP-based network storage for network attached storage (NAS). The storage networking module shows in depth how to deploy a Fibre Channel storage area network (SAN) using the Cisco Nexus 5500UP switches as the SAN core.
- The Compute Connectivity module explains the various host connectivity options that may be used in the data center. The module covers dual-homed and single-homed servers, and blade server systems connectivity to the network.
- The Network Security module focuses on the deployment of firewalls to protect the critical and sensitive information assets of your organization. The Intrusion Protection System (IPS) section explains how to deploy Cisco IPS to monitor your network for intrusions and attacks.
- The Application Resiliency module shows how server load balancing can be used to quickly grow server application farms, monitor server and application operation, and balance loads across multiple servers for better performance.
- The appendices provide the complete list of products used in the lab testing of this architecture, as well as the software revisions used on the products and a list of major changes to the guide.

To enhance the architecture, there are also a number of supplemental guides that address specific functions, technologies, or features from Cisco and Cisco partners that may be important to solving your organization’s requirements.
**Design Goals**

The Cisco SBA program follows a consistent design process of building a network based on layers of services. The primary building block is the foundation layer upon which all other services rely. The data center foundation must be resilient, scalable, and flexible to support data center services, which add value, performance, and reliability. The ultimate goal of the design is to support the user services that drive the organization’s success. Figure 1 illustrates the Cisco SBA data center architecture layered services.

*Figure 1 - SBA data center pyramid of service layers*

The Cisco SBA deployment guides are all designed to use a modular concept of building out a network. Each module is focused on the following principles:

- **Ease of use**—A top requirement was to develop a design that could be deployed with the minimal amount of configuration and day-two management.
- **Cost-effective**—Another critical requirement in the selection of products was to meet the budget guidelines for a company of this size.
- **Flexibility and scalability**—As the company grows, so too must its infrastructure. Products selected needed to have the ability to grow or be repurposed within the architecture.
- **Reuse**—The goal, when possible, was to reuse the same products throughout the various modules to minimize the number of products required for spares.

**Business Overview**

Midsize organizations encounter many challenges as they work to scale their information-processing capacity to keep up with demand. In a new organization, a small group of server resources may be sufficient to provide necessary applications such as file sharing, email, database applications, and web services. Over time, demand for increased processing capacity, storage capacity, and distinct operational control over specific servers can cause a growth explosion commonly known as “server sprawl”. A midsize organization can then use some of the same data center technologies that larger organizations use to meet expanding business requirements in a way that keeps capital and operational expenses in check. This deployment guide provides reference architecture to facilitate rapid adoption of these data center technologies by using a common, best-practices configuration.

The Cisco SBA Data Center for Midsize Organizations architecture provides an evolution from the basic “server room” infrastructure. The Data Center for Midsize Organizations is designed to address four primary business challenges:

- Supporting rapid application growth
- Managing growing data storage requirements
- Optimizing the investment in server processing resources
- Securing the organizations’ critical data

**Supporting Rapid Application Growth**

As applications scale to support a larger number of users, or new applications are deployed, the number of servers required to meet the needs of the organization often increases. The first phase of the server room evolution is often triggered when the organization outgrows the capacity of the existing server room network. Many factors can limit the capacity of the existing facility, including rack space, power, cooling, switching throughput, or basic network port count to attach new servers. The architecture outlined in this guide is designed to allow the organization to smoothly scale the size of the server environment and network topology as business requirements grow.
Managing Growing Data Storage Requirements

As application requirements grow, the need for additional data storage capacity also increases. This can initially cause issues when storage requirements for a given server increase beyond the physical capacity of the server hardware platform in use. As the organization grows, the investment in additional storage capacity is most efficiently managed by moving to a centralized storage model. A centralized storage system can provide disk capacity across multiple applications and servers providing greater scalability and flexibility in storage provisioning.

A dedicated storage system provides multiple benefits beyond raw disk capacity. Centralized storage systems can increase the reliability of disk storage, which improves application availability. Storage systems allow increased capacity to be provided to a given server over the network without needing to physically attach new devices to the server itself. More sophisticated backup and data replication technologies are available in centralized storage systems, which helps protect the organization against data loss and application outages.

Optimizing the Investment in Server Processing Resources

As a midsize organization grows, physical servers are often dedicated to single applications to increase stability and simplify troubleshooting. However, these servers do not operate at high levels of processor utilization for much of the day. Underutilized processing resources represent an investment by the organization that is not being leveraged to its full potential.

Server virtualization technologies allow a single physical server to run multiple virtual instances of a “guest” operating system, creating virtual machines (VMs). Running multiple VMs on server hardware helps to more fully utilize the organization’s investment in processing capacity, while still allowing each VM to be viewed independently from a security, configuration, and troubleshooting perspective.

Server virtualization and centralized storage technologies complement one another, allowing rapid deployment of new servers and reduced downtime in the event of server hardware failures. Virtual machines can be stored completely on the centralized storage system, which decouples the identity of the VM from any single physical server. This allows the organization great flexibility when rolling out new applications or upgrading server hardware.

Securing the Organizations Critical Data

With communication and commerce in the world becoming increasingly Internet-based, network security quickly becomes a primary concern of a growing organization. Often organizations will begin by securing their Internet edge connection, considering the internal network a trusted entity. However, an Internet firewall is only one component of building security into the network infrastructure.

Frequently, threats to an organization’s data may come from within the internal network. This may come in the form of onsite vendors, contaminated employee laptops, or existing servers that have already become compromised and may be used as a platform to launch further attacks. With the centralized repository of the organization’s most critical data typically being the data center, security is no longer considered an optional component of a complete data center architecture plan.

The SBA Midsize Data Center Architecture illustrates how to cleanly integrate network security capabilities such as firewall and intrusion prevention, protecting areas of the network housing critical server and storage resources. The architecture provides the flexibility to secure specific portions of the data center or insert firewall capability between tiers of a multi-tier application according to the security policy agreed upon by the organization.
Increase Application Availability

With the expanding global presence and around the clock operations of organizations, key applications that drive the business must be available when the workforce needs them. Availability of applications can be threatened by overloaded servers, and server or application failure. Unbalanced utilization can drive unacceptable response times for some users and satisfactory operation for others making it difficult for IT teams to diagnose.

*Figure 2 - Application server farm in various states of operation*

Application availability drives productivity and customer satisfaction, which are critical to an organization’s success. IT organizations require the ability to monitor beyond simple server availability to application availability, and to be able to add more servers to an application server farm quickly and transparently.

**Technology Overview**

The SBA Midsize Data Center Architecture is designed to allow organizations to take an existing server room environment to the next level of performance, flexibility, and security. Figure 3 provides a high-level overview of this architecture.
Figure 3 - Cisco SBA midsize data center architecture
The SBA Midsize Data Center Architecture is designed to stand alone if deployed at an offsite facility, or to connect to one of the SBA Layer-3 Ethernet core solutions, as documented in Cisco SBA for Midsize Organizations—Borderless Networks Foundation Design Overview. The following technology areas are included within this reference architecture:

**Ethernet Infrastructure**

The Ethernet infrastructure forms the foundation for resilient Layer 2 and Layer 3 communications in the data center. This layer provides the ability to migrate from your original server farm to a scalable architecture capable of supporting Fast Ethernet, Gigabit Ethernet, and 10-Gigabit Ethernet connectivity for hundreds of servers in a modular approach.

The core of the Cisco SBA midsize data center is built on the Cisco Nexus 5500UP series switches. The Cisco Nexus 5500UP series is a high-speed switch capable of Layer 2 and Layer 3 switching with the Layer 3 daughter card tested in this design. The Cisco Nexus 5500UP series has a 48 port model used in this design, and a 96-port model for higher density requirements. The Cisco Nexus 5500UP supports Fabric Extender (FEX) technology which provides a remote line card approach for fan out of server connectivity to top of rack for Fast Ethernet, Gigabit Ethernet, and 10-Gigabit Ethernet requirements. The physical interfaces on the Cisco FEX are programmed on the Cisco Nexus 5500UP switches, simplifying the task of configuration by reducing the number of devices you have to touch to deploy a server port.

The Cisco Nexus 5500UP series features the Virtual Port Channel technology, which provides a loop free approach to building out the midsize data center in which any VLAN can appear on any port in the topology without spanning tree loops or blocking links. The data center core switches are redundant with sub-second failover so that a device failure or maintenance does not prevent the network operation.

**Storage Networking**

Storage networking is key to solving the growing amount of data storage that the midsize organization has to struggle with. Centralized storage reduces the amount of disk space trapped on individual server platforms and eases the tasks of providing backup to avoid data loss. The SBA midsize data center design uses Cisco Nexus 5500UP series switches as the core of the network. The importance of this model switch is that it has universal port (UP) capabilities. A universal port is capable of supporting Ethernet, Fibre Channel, and Fibre Channel over Ethernet (FCoE) on any port. This allows the data center core to support multiple storage networking technologies like Fibre Channel storage area network (SAN), Internet Small Computer System Interface (iSCSI), and network attached storage (NAS) on a single platform type. This not only reduces costs to deploy the network but saves rack space in expensive data center hosting environments.

The Cisco Nexus 5500UP Fibre Channel capabilities are based on the Cisco NX-OS operating system and seamlessly interoperate with the Cisco MDS series SAN switches for larger Fibre Channel requirements. This deployment module includes procedures for interconnecting between Cisco Nexus 5500UP series and Cisco MDS series for Fibre Channel SAN. The Cisco MDS series can provide an array of advanced services for Fibre Channel SAN environments where high speed encryption, inter-VSAN routing, tape services, or Fibre Channel over IP extension might be required.

**Compute Connectivity**

There are many ways to connect a server to the data center network for Ethernet and Fibre Channel transport. This module provides an overview of connectivity ranging from single homed Ethernet servers to a dual-homed Fabric Extender, and dual-homed servers that might use active/standby network interface card (NIC) teaming or EtherChannel for resiliency. Servers that use 10-Gigabit Ethernet can collapse multiple Ethernet NICs and Fibre Channel host bus adapters (HBA) onto a single wire using converged network adapters and FCoE. Dual-homing the 10-Gigabit Ethernet servers with FCoE provides resilient Ethernet transport and Fibre Channel connections to SAN-A/SAN-B topologies. This module also provides an overview of how Cisco Unified Computing System (UCS) blade server systems integrated connectivity works and considerations for connecting a non-Cisco blade server system to the network.
Network Security

Within a data center design, there are many requirements and opportunities to include or improve security for customer confidential information and the organization's critical and sensitive applications. The data center design is tested with the Cisco ASA 5500 series firewall. The Cisco ASA 5500 provides high-speed processing for firewall rule sets, and high bandwidth connectivity with multiple 10-Gigabit Ethernet ports for resilient connectivity to the data center core switches. The Cisco ASA 5500 also has a slot for services, and in this design provides an IPS module to inspect application layer data, to detect attacks and snooping, and to block malicious traffic based on the content of the packet or the reputation of the sender. The Cisco ASA 5500 firewalls with IPS modules are deployed in a pair which provides an active/hot-standby resilience to prevent downtime in the event of a failure or platform maintenance.

Application Resiliency

Application performance and availability directly affect employee productivity and customer satisfaction, which drives the bottom line of an organization. As organizations expand to do business in a 24-hour globally available environment, it becomes even more important to make sure that critical applications are operating at peak performance.

This architecture includes the Cisco Application Control Engine (ACE) to provide the latest technology for Layer 4 through Layer 7 switching and server load balancing (SLB). Server load balancers can spread the load across multiple servers for an application, and actively probe the servers and applications for load and health to prevent overload and application failures. The Cisco ACE also offers TCP processing offload, Secure Socket Layer (SSL) offload, compression, and various other acceleration technologies. The Cisco ACE 4710s used in this architecture are scalable to multi-Gigabit operation and are deployed as an active/hot-standby pair to prevent outage from device failure or maintenance.

This architecture is designed to allow a midsize organization to position its network for growth while controlling both equipment costs and operational costs. The deployment processes documented in this guide provide concise step-by-step instructions for completing the configuration of the components of the architecture to get your network up and running. This approach allows you to take advantage of some of the newer technologies being used in the data centers of very large organizations without encountering a steep learning curve for the IT staff. Although this architecture has been designed and validated as a whole, the modular nature of this guide allows you to perform a gradual migration by choosing specific elements of the architecture to implement first.

The remaining sections of this guide detail the various technologies that comprise this architecture.
Physical Environment

Business Overview
When building or changing a network, you have to carefully consider the location where you will install the equipment. When building a server room, a switch closet, or even a midsize data center, take three things into consideration: power, cooling, and racking. Know your options in each of these categories, and you will minimize surprises and moving of equipment later on.

Technology Overview
The Cisco Smart Business Architecture for Midsize Organizations Data Center architecture provides a resilient environment with redundant platforms and links, however this cannot protect your data center from a complete failure resulting from a total loss of power or cooling. When designing your data center you must consider how much power you will require, how you will provide backup power in the event of a loss of your power feed from your provider, and how long you will retain power in a backup power event. The servers, networking equipment, and appliances in your data center dissipate heat as they operate, which requires a proper cooling design that includes equipment rack locations to prevent hotspots.

Power
Know what equipment will be installed in the area. You cannot plan electrical work if you do not know what equipment is going to be used. Some equipment requires standard 110v outlets that may already be available. Other equipment can require great power needs. Does the power need to be on all the time? In most cases this answer will be yes if there are servers and storage involved. Applications don’t react very well when the power goes out. To prevent power outages, an uninterruptable power supply (UPS) is needed. During a power interruption, the UPS will switch over the current load to a set of internal or external batteries. Some UPSs are online, which means the power is filtered through the batteries all the time; others are switchable, meaning they use batteries only during power losses. UPSs vary by how much load they can carry and for how long. Careful planning is required to make sure the correct UPS is purchased, installed, and managed correctly. Most UPSs provide for remote monitoring and the ability to trigger a graceful server shutdown for critical servers if the UPS is going to run out of battery.

Distributing the power to the equipment can change the power requirements as well. There are many options available to distribute the power from the outlet or UPS to the equipment. One example would be using a power strip that resides vertically in a cabinet that usually has an L6-30 input and then C13/C19 outlets with the output voltage in the 200-240 range. These strips should be at a minimum metered so one does not overload the circuits. The meter provides a current reading of the load on the circuit. This is critical as a circuit breaker tripping due to being overloaded will bring down everything plugged into it with no warning, causing business downtime and possible data loss. For complete remote control, power strips are available with full remote control of each individual outlet from a web browser. These vertical strips also assist in proper cable management of the power cords. Short C13/C14 and C19/C20 power cords can be used instead of much longer cords to multiple 110 volt outlets or multiple 110 volt power strips.

Cooling
With power comes the inevitable conversion of power into heat. Without going into great detail, power in equals heat out. Planning for cooling of one or two servers and a switch with standard building air may work. Multiple servers and blade servers (along with storage, switches, etc.) need more than building air for proper cooling. Be sure to at least plan with your facilities team what the options are for current and future cooling. Many options are available, including in-row cooling, overhead cooling, raised floor with underfloor cooling, and wall mounted cooling.
Equipment Racking
Where to put the equipment is a very important detail you don’t want to overlook. Proper placement and planning allow for easy growth. With the power and cooling properly evaluated, racking or cabinets need to be installed. Most servers are fairly deep and, with network connections and power connections, take up even more space. Most servers will fit in a 42-inch deep cabinet, and deeper cabinets give more flexibility for cable and power management within the cabinet. Be aware of what rails are required by your servers. Most servers now come with rack mounts that use the square-hole style vertical cabinet rails. Not having the proper rails can mean having to use adapters or shelves and making management of servers and equipment difficult if not sometimes impossible without removing other equipment or sacrificing space. Data center racks should use the square rail mounting options in the cabinets. Cage nuts can be used to provide threaded mounts for such things as routers, switches, shelves, etc. that may be needed.

Summary
The physical environmental requirements for a data center require careful planning to provide for efficient use of space, scalability, and ease of operational maintenance. Working towards deployment of the Cisco Smart Business Architecture allows you to plan the physical space for your data center with a vision towards the equipment you will be installing over time, even if you begin with a smaller scale. For additional information on data center power, cooling, and equipment racking, contact Cisco partners in the area of data center environmental products such as Panduit and APC.
Business Overview

As your midsize organization grows, you may outgrow the capacity of the basic “server-room” Ethernet switching stack illustrated in the SBA Midsize Foundation Architecture. It is important to be prepared for the ongoing transition of available server hardware from 1-Gigabit Ethernet attachment to 10-Gigabit. Multi-tier applications often divide browser-based client services, business logic, and database layers into multiple servers, increasing the amount of server-to-server traffic and driving performance requirements higher. As the physical environment housing the organization’s servers grows to multiple racks, it also becomes more challenging to elegantly manage the cabling required to attach servers to the network. The use of 10-Gigabit Ethernet connections help to improve overall network performance, while reducing the number of physical links required to provide the bandwidth.

In some organizations the data center may be located at a facility other than the headquarters building. Some organizations will locate their data center at a remote facility where power or cooling more suitable for a data center is located, others may rent floor space, racks, and power from a communications service provider to lower their capital costs. The ability to locate the data center in a number of different locations requires a data center architecture that is flexible to adapt to different locations while still providing the core elements of the architecture.

Technology Overview

The foundation of the Ethernet network in the Cisco SBA Midsize Data Center Architecture is a resilient pair of Cisco Nexus 5500UP Series switches. These switches offer the ideal platform for building a scalable, high-performance data center supporting both 10-Gigabit and 1-Gigabit Ethernet attached servers. The Cisco SBA Midsize Data Center Architecture is designed to allow easy migration of servers and services from your original server farm to a data center that can scale with your organization’s growth.

The Nexus 5500UP switches with universal port capabilities provide support for Ethernet, Fiber Channel over Ethernet (FCoE), and Fiber Channel (FC) ports on a single platform. The Nexus 5500UP can act as the Fiber Channel SAN for the midsize data center and connect into an existing Fiber Channel SAN. The Cisco Nexus 5000 Series also supports the Cisco Nexus 2000 Series Fabric Extenders. Fabric Extenders allow the switching fabric of the resilient switching pair to be physically extended to provide port aggregation in the top of multiple racks, reducing cable management issues as the server environment expands.

The Cisco SBA Midsize Data Center Architecture leverages many advanced features of the Cisco Nexus 5500UP Series switch family to provide a central Layer 2 and Layer 3 switching fabric for the data center environment that provides the scalability for most midsize data centers:

- The Layer 3 routing table can accommodate up to 8000 routes.
- The Layer 3 engine supports up to 8000 adjacencies or MAC addresses for the Layer 2 domain.
- The solution provides for up to 1000 IP multicast groups when operating in the recommended virtual port channel mode.


Reader Tip
The Layer 3 data center core connects to the Layer 3 LAN core designed in the Cisco SBA for Midsize Organizations—Borderless Networks Foundation Deployment Guide as shown in Figure 4.

**Figure 4 - Data center core and LAN core change control separation**

The result of using Layer 3 to interconnect the two core layers is:
- A resilient Layer 3 interconnect with rapid failover.
- A logical separation of change control for the two core networks.
- The LAN core provides a scalable interconnect for LAN, WAN, and Internet Edge.
- The data center core provides interconnect for all data center servers and services.
- Intra-data center Layer 2 and Layer 3 traffic flows between servers and appliances are switched locally on the data center core.
- The data center has a logical separation point for moving to an offsite location while still providing core services without redesign.

This section provides an overview of the key features used in this topology and illustrates the specific physical connectivity that applies to the example configurations provided in the deployment section.

**Resilient Data Center Core**

The data center needs to provide a topology where any data center VLAN can be extended to any server in the environment to accommodate new installations without disruption, and the ability to move a server load to any other physical server in the data center. Traditional Layer 2 designs with LAN switches use spanning tree, which creates loops when a VLAN is extended to multiple Access Layer switches. Spanning Tree Protocol blocks links to prevent looping as shown in Figure 5.

**Figure 5 - Traditional design with spanning tree blocked links**
The Cisco Nexus 5500UP Series switch pair providing the central Ethernet switching fabric for the Cisco SBA midsize data center architecture is configured using the Virtual Port Channel (vPC) feature. vPC allows links that are physically connected to two different Cisco Nexus switches to appear to a third downstream device to be coming from a single device and as part of a single Ethernet Port Channel. The third device can be a server, switch, or any other device or appliance that supports IEEE 802.3ad Port Channels. This capability allows the two data center core switches to build resilient, loop-free Layer 2 topologies that forward on all connected links instead of requiring Spanning Tree Protocol blocking for loop prevention.

Cisco NX-OS Software vPC used in the data center design, and Cisco Catalyst Virtual Switching Systems (VSS) used in the Cisco SBA for Midsize Organizations—Borderless Networks Foundation Design Overview are similar technologies in that they allow the creation of Layer 2 Port Channels that span two switches. For Cisco EtherChannel technology, the term “multichassis EtherChannel” (MCEC) refers to either technology interchangeably. MCEC links from a device connected using vPC to the data center core and provides spanning tree loop-free topologies allowing VLANs to be extended across the midsize data center while maintaining a resilient architecture.

vPCs consist of two vPC peer switches connected by a peer link. Of the vPC peers, one is primary and one is secondary. The system formed by the switches is referred to as a vPC domain.

**Figure 6 - Cisco NX-OS vPC design**

This feature enhances ease-of-use and simplifies configuration for the data center-switching environment.

---

**Reader Tip**

For more information on vPC technology and design, refer to the documents “Cisco NX-OS Software Virtual PortChannel Fundamental Concepts” and “Spanning-Tree Design Guidelines for Cisco NX-OS Software and Virtual PortChannels” on [www.cisco.com](http://www.cisco.com).

The Cisco SBA midsize data center design uses Hot Standby Router Protocol (HSRP) for IP default gateway resilience for data center VLANs. When combining HSRP with vPC there is no need for aggressive HSRP timers to improve convergence as both gateways are always active and traffic to either data center core will be locally switched for improved performance and resilience.

### Ethernet Fabric Extension

The Cisco Nexus 2000 Series Fabric Extender (FEX) delivers cost-effective and highly scalable 1-Gigabit and 10-Gigabit Ethernet environments. Fabric extension allows you to aggregate a group of physical switch ports at the top of each server rack, without needing to manage these ports as a separate logical switch. The Cisco FEX behaves as a remote line card to the Cisco Nexus 5500UP switches. All configuration for Cisco FEX connected servers is done on the data center core switches, which provide a centralized point to configure all connections for ease of use. Because the Cisco FEX acts as a line card on the Cisco Nexus 5500UP switch, extending VLANs to server ports on different Cisco FEXs does not create spanning tree loops across the data center.

You can provide network resiliency by dual-homing servers into two separate fabric extenders, each of which is single homed to one member of the Cisco Nexus 5500UP Series switch pair. To provide high availability for servers that only support single-homed network attachment, the Cisco FEX itself may instead be dual-homed using vPC into the two members of the data center core switch pair. Both the single-homed and dual-homed topologies provide the flexibility to have a VLAN appear on any port without loops or spanning tree blocked links.
Our reference architecture example shown in Figure 8 illustrates single-homed and dual-homed Cisco FEX configurations with connected servers. Each Cisco FEX includes dedicated fabric uplink ports that are designed to connect to upstream Cisco Nexus 5500UP Series switches for data communication and management. Any 10-Gigabit Ethernet port on the Cisco Nexus 5500UP switch may be used for a Cisco FEX connection.

**Tech Tip**

When the Cisco Nexus 5500UP series switches are configured for Layer 3 operation, they support up to 8 connected Cisco FEXs as of NX-OS release 5.1(3)N1. The Cisco FEX will support up to 4 or 8 uplinks to the Cisco Nexus 5500UP parent switches depending on the model Cisco FEX in use and the level of oversubscription you want in your design. It is recommended, when possible, to configure the maximum number of fabric uplinks leveraging either twinax (CX-1) cabling or the Fabric Extender Transceiver (FET) and OM3 multi-mode fiber. At least 2 Cisco FEX uplinks to the data center core is recommended for minimum resiliency.
Deployment Details

The following configuration procedures are required to configure the Ethernet switching fabric for the Cisco SBA Midsize Data Center Architecture.

### Process

Configuring Out of Band Management

1. Apply platform-specific configuration
2. Apply global configuration
3. Configure link to Layer 3 core
4. Configure access ports

An increasing number of switching platforms, appliances, and servers utilize discrete management ports for setup, monitoring, and keep alive processes. The typical midsize organization data center is an ideal location for an Ethernet out-of-band management network as the equipment is typically contained within in a few racks and does not require fiber optic interconnect to reach far away platforms.

In this design we will use a fixed configuration Layer 2 switch for the out-of-band Ethernet management network. A switch like the Cisco Catalyst 3560X is an ideal switch for this purpose because it has dual power supplies for resiliency.

The out of band network provides:

- Layer 2 path, independent of the data path of the Cisco Nexus 5500UP data center core switches, for Virtual Port Channel keepalive packets running over the management interface.
- Path for configuration sync between Nexus 5500UP switches via the management interfaces.
- Common connection point for data center appliance management interfaces like the firewalls and load balancers.
- Connectivity point for “lights out” management ports on servers.

While the Layer 2 switch does provide a common interconnect for packets inside the data center, it needs to provide the ability for IT management personnel outside of the data center to access these devices. The options for providing IP connectivity depends on the location of your data center.

If your data center is at the same location as your HQ LAN, then the core LAN switch can provide Layer 3 connectivity to the data center management subnet.

*Figure 9 - Core LAN switch providing Layer 3 connectivity*
If your data center is located at a facility separate from a large LAN, the WAN router can provide Layer 3 connectivity to the data center management subnet.

**Figure 10 - WAN router providing Layer 3 connectivity**

A third option for providing Layer 3 connectivity to the data center management subnet is to use the data center core Cisco Nexus 5500UP switches. We will configure this connectivity option in this guide.

**Figure 11 - Providing Layer 3 connectivity by using core Cisco Nexus 5500UP switches**

---

**Tech Tip**

When using the data center core Cisco Nexus 5500UP switches for the Layer 3 connectivity, the Layer 2 path for vPC keepalive packets will use the Ethernet out-of-band switch, as the Nexus 5500UP management ports are in a separate management virtual routing and forwarding path (vrf) than the global packet switching of the Nexus 5500UP switches. Also, the management ports are in the same IP subnet so they do not need a Layer 3 switch for packets between the data center core switches. The Layer 3 switched virtual interface will provide connectivity for access outside of the data center.

---

**Procedure 1**

**Apply platform-specific configuration**

**Step 1:** Configure the Catalyst 2960-S and 3750-X platform.

```plaintext
switch [switch number] priority 15
```

When there are multiple Cisco Catalyst 2960-S or Cisco Catalyst 3750-X Series switches configured in a stack, one of the switches controls the operation of the stack and is called the stack master. When three or more switches are configured in a stack, configure a switch that does not have uplinks configured as the stack master.

**Step 2:** Ensure the original master MAC address remains the stack MAC address after a failure.

```plaintext
stack-mac persistent timer 0
```

The default behavior when the stack master switch fails is for the newly active stack master switch to assign a new stack MAC address. This new MAC address assignment can cause the network to have to reconverge because LACP and many other protocols rely on the stack MAC address and must restart. As such, the stack-mac persistent timer 0 command should be used to ensure that the original master MAC address remains the stack MAC address after a failure.
Procedura 2 Apply global configuration

The out-of-band LAN management switch requires basic global configuration.

Step 1: Apply the configuration described in the "Global Configuration Module" section of the Cisco SBA for Midsize Borderless Networks – Foundation Deployment Guide. This enables infrastructural requirements such as management access and network time configuration.

Step 2: Configure device resiliency features

Virtual Trunk Protocol (VTP) allows network managers to configure a VLAN in one location of the network and have that configuration dynamically propagate out to other network devices. However, with the out of band management network, VLANs are defined once during switch setup with few, if any, additional modifications.

    vtp mode transparent

Rapid Per-VLAN Spanning-Tree (PVST+) provides an instance of RSTP (802.1w) per VLAN. Rapid PVST+ greatly improves the detection of indirect failures or linkup restoration events over classic spanning tree (802.1D).

While this architecture is built without any Layer 2 loops, spanning tree must still be enabled. Having spanning tree enabled ensures that if any physical or logical loops are accidentally configured, no actual layer 2 loops occur.

    spanning-tree mode rapid-pvst

Unidirectional Link Detection (UDLD) is a Layer 2 protocol that enables devices connected through fiber-optic or twisted-pair Ethernet cables to monitor the physical configuration of the cables and detect when a unidirectional link exists. When UDLD detects a unidirectional link, it disables the affected interface and alerts you. Unidirectional links can cause a variety of problems, including spanning-tree loops, black holes, and non-deterministic forwarding. In addition, UDLD enables faster link failure detection and quick reconvergence of interface trunks, especially with fiber, which can be susceptible to unidirectional failures.

    udld enable

Step 3: EtherChannels are used extensively in this design because of their resiliency capabilities. If you want to normalize the method in which traffic is load-shared across the member links of the EtherChannel, set the management switch uplinks to use the traffic source and destination IP address when calculating which link to send the traffic across.

    port-channel load-balance src-dst-ip

Step 4: Configure the switch with an IP address so that it can be managed via in-band connectivity.

    interface vlan [management vlan]
    ip address [ip address] [mask]
    no shutdown
    ip default-gateway [default router]

Step 5: Configure the management VLAN.

The out-of-band management network will use a single VLAN, VLAN 163, for device connectivity.

    vlan [163]
    name DC-Management
Procedure 3  Configure link to Layer 3 core

As described earlier, there are various methods to connect to Layer 3 for connectivity to the data center out-of-band management network. The following steps describe configuring an EtherChannel for connectivity to the data center core Cisco Nexus 5500UP switches.

**Step 1:** Configure two or more physical interfaces to be members of the EtherChannel and set the link aggregation control protocol to active on both sides. This ensures a proper EtherChannel is formed and does not cause any issues.

```
interface range [interface type] [port 1], [interface type] [port 2]
channel-protocol lacp
channel-group 1 mode active
```

**Step 2:** Configure the trunk.

An 802.1Q trunk is used for the connection to this upstream device, which allows it to provide the Layer 3 services to all the VLANs defined on the server room switch. The VLANs allowed on the trunk are pruned to only the VLANs that are active on the server room switch.

```
interface Port-channel11
switchport trunk allowed vlan [management vlan]
switchport mode trunk
no shutdown
```

---

**Reader Tip**

The configuration on the data center core Cisco Nexus 5500UP switches for Layer 3 connectivity to the out-of-management network will be covered in Procedure 9 “Configure management switch connection” in this guide.

---

Procedure 4  Configure access ports

**Step 1:** Configure switch interfaces to support management console ports. This host interface configuration supports management port connectivity.

```
interface range [interface type] [port number]–[port number]
switchport access vlan [163]
switchport mode access
```

**Step 2:** Shorten the time it takes for a port to go into the forwarding state by setting the switchport to mode host.

```
switchport host
```

**Step 3:** (Optional) Save your management switch configuration.

```
copy running-config startup-config
```
Procedure 1  Establish physical connectivity

Complete the physical connectivity of the Cisco Nexus 5500UP Series switch pair according to the illustration below.

Step 1: Connect two available Ethernet ports between the two Cisco Nexus 5500UP Series switches.

These ports will be used to form the vPC peer-link, which allows the peer connection to form and supports forwarding of traffic between the switches if necessary during a partial link failure of one of the vPC port channels. It is recommended to use at least two links for the vPC peer-link resiliency, although more can be added to accommodate higher switch-to-switch traffic.
Step 2: Connect two available Ethernet ports on each Cisco Nexus 5500UP Series switch to the SBA core.

Four 10-Gigabit Ethernet connections will provide resilient connectivity to the SBA LAN core with aggregate throughput of 40 Gbps to carry data to the rest of the organization.

Step 3: Connect to dual-homed FEX.

To support a dual-homed FEX with single-homed servers, connect fabric uplink ports 1 and 2 on the Cisco FEX to an available Ethernet port, one on each Cisco Nexus 5500UP Series switch. These ports will operate as a port channel to support the dual-homed Cisco FEX configuration.

Tech Tip

Depending on the model Cisco FEX being used, up to 4 or 8 ports can be connected to provide more throughput from the Cisco FEX to the core switch.

Step 4: Connect to single-homed FEX.

Support single-homed FEX attachment by connecting fabric uplink ports 1 and 2 on each FEX to two available Ethernet ports on only one member of the Cisco Nexus 5500UP Series switch pair. These ports will be a port-channel, but will not be configured as a vPC port-channel, because they have physical ports connected to only one member of the switch pair.

Step 5: Connect to Out of Band Management switch.

In this design we will use a physically separate standalone switch for connecting the management ports of the Cisco Nexus 5500s. The management ports will provide out-of-band management access and transport for vPC peer keepalive packets. vPC keepalive packets are a part of the protection mechanism for vPC operation.

Procedure 2 Perform initial device configuration

Software license prerequisites

The Cisco Nexus 5500UP Series offers a simplified software management mechanism based on software licenses. These licenses are enforceable on a per switch basis and enable a full suite of functionalities. The data center core layer is characterized by a Layer 3 configuration, so the Cisco Nexus 5500UP Series switch requires the Layer 3 license, which enables full Enhanced Interior Gateway Routing (EIGRP) functionality. The Fibre Channel license will be required when running native Fibre Channel or Fibre Channel over Ethernet (FCoE).

Step 1: Connect to switch console interface by connecting a terminal cable to the console port of the first Cisco Nexus 5500UP Series switch, and then powering on the system to enter the initial configuration dialog box.

Step 2: Run the setup script and follow the Basic System Configuration Dialog for initial device configuration of the first Cisco Nexus 5500UP Series switch. This script will setup a system login password, Secure Shell (SSH) login, and the management interface addressing. Some setup steps will be skipped and covered in a later configuration step.

Do you want to enforce secure password standard (yes/no): y

Enter the password for “admin”:

Confirm the password for “admin”:

---- Basic System Configuration Dialog ----

This setup utility will guide you through the basic configuration of the system. Setup configures only enough connectivity for management of the system.

Please register Cisco Nexus 5000 Family devices promptly with your supplier. Failure to register may affect response times for initial
service calls. Nexus devices must be registered to receive entitled support services.

Press Enter at anytime to skip a dialog. Use ctrl-c at anytime to skip the remaining dialogs.

Would you like to enter the basic configuration dialog (yes/no): y
Create another login account (yes/no) [n]: n
Configure read-only SNMP community string (yes/no) [n]: n
Configure read-write SNMP community string (yes/no) [n]: n
Enter the switch name: dc5548ax
Continue with Out-of-band (mgmt0) management configuration? (yes/no) [y]: y
  Mgmt0 IPv4 address: 10.10.63.10
  Mgmt0 IPv4 netmask: 255.255.255.128
Configure the default gateway? (yes/no) [y]: y
  IPv4 address of the default gateway: 10.10.63.1
Enable the telnet service? (yes/no) [n]: n
Enable the ssh service? (yes/no) [y]: y
  Type of ssh key you would like to generate (dsa/rsa): rsa
  Number of key bits <768-2048>: 2048
Configure the ntp server? (yes/no) [n]: y
  NTP server IPv4 address: 10.10.48.17
Enter basic FC configurations (yes/no) [n]: n
The following configuration will be applied:
  switchname dc5548ax
  interface mgmt0
    ip address 10.10.63.10 255.255.255.128
    no shutdown
    exit
  vrf context management
    ip route 0.0.0.0/0 10.10.63.1
    exit
      no telnet server enable
      ssh key rsa 2048 force

ssh server enable
ntp server 10.10.48.17 use-vrf management
Would you like to edit the configuration? (yes/no) [n]: n
Use this configuration and save it? (yes/no) [y]: y
[########################################] 100%
dc5548ax login:

The only change to the setup script for the second Cisco Nexus 5500UP switch will be the system name and the Mgmt0 address, which will be 10.10.63.11.

Step 3: Enable system features.

Due to the modular nature of Cisco NX-OS, processes are only started when a feature is enabled. As a result, commands and command chains only show up once the feature has been enabled. For licensed features, the feature-name command can only be used once the appropriate license is installed. The Cisco Nexus 5500UP Series requires a license for Layer 3 operation, Fiber Channel storage protocols, and FCoE NPV operation. For more information on licensing, consult the Cisco NX-OS Licensing Guide on www.cisco.com.

Configure common required features in the NXOS software. The example configurations shown in this guide use the following features:

  feature udld
  feature interface-vlan
  feature lacp
  feature vpc
  feature eigrp
  feature fex
  feature hsrp
  feature pim
  feature fcoe
Although not used in this design, if the Fiber Channel–specific feature N-Port Virtualization (NPV) is required for your network it should be enabled prior to applying any additional configuration to the switch. It should be enabled prior to applying any additional configuration to the switch. The NPV feature is the only feature that when enabled or disabled will erase your configuration and reboot the switch, requiring you to re-apply any existing configuration commands to the switch.

**Tech Tip**

Although not used in this design, if the Fiber Channel–specific feature N-Port Virtualization (NPV) is required for your network it should be enabled prior to applying any additional configuration to the switch. It should be enabled prior to applying any additional configuration to the switch. The NPV feature is the only feature that when enabled or disabled will erase your configuration and reboot the switch, requiring you to re-apply any existing configuration commands to the switch.

**Step 4:** Configure port operation mode. In this example, enable ports 28 through 32 on a Cisco Nexus 5548UP switch as Fiber Channel ports.

```plaintext
slot 1
  port 28-32 type fc
```

The Cisco Nexus 5500UP switch has universal ports that are capable of running Ethernet+FCoE or Fiber Channel on a per port basis. All switch ports are by default enabled for Ethernet operation. Fiber channel ports must be enabled in a contiguous range and be the high numbered ports of the switch baseboard and/or the high numbered ports of a Universal Port expansion module.

**Step 5:** Enable jumbo frame support. Jumbo frames can be enabled on a per class of service (CoS) basis on the Cisco Nexus 5500UP. This example shows jumbo frame operation enabled on the default CoS.

```plaintext
policy-map type network-qos jumbo
  class type network-qos class-default
    mtu 9216
  system qos
    service-policy type network-qos jumbo
```

**Tech Tip**

Jumbo frames can improve data throughput between key end nodes in the data center that are able to negotiate larger packet sizes, such as iSCSI based storage systems and their associated servers. If your iSCSI traffic flows are routed between subnets, you can increase the mtu to 9216 on Layer 3 interfaces as well.

**Step 6:** (Optional) Save your configuration, and then reload the switch. Since the Nexus switch requires a reboot to recognize ports configured for Fiber Channel operation, this is a good point to reload the switch.

```plaintext
copy running-config startup-config
reload
```

**Step 7:** On the second Cisco Nexus 5500UP Series switch, repeat all of the steps of this procedure (Procedure 2). Use a unique device name (`dc5548bx`) and IP address (`10.10.63.11`) for the mgmt0 interface. Otherwise, all configuration details are identical.

**Tech Tip**

Changing port type to fc requires a reboot in Cisco Nexus 5500UP NX-OS version 5.1(3)N1(1) software to recognize the new port operation. This is subject to change in later releases of software. Ports will not show up in the configuration as “fc” ports if you did not enable the feature fcoe in the previous step.
Procedure 3  Configure virtual port channel

Before you can add port channels to the switch in virtual port channel (vPC) mode, basic vPC peering must be established between the two Cisco Nexus 5500UP Series switches. The vPC peer link provides a communication path between the data center core switches that allows devices that connect to each core switch for resiliency to do so over a single Layer 2 EtherChannel.

Step 1: Define a vPC domain number to identify the vPC domain to be common between the switches in the pair.

```text
vpc domain 10
```

Step 2: Define a lower role priority for the vPC primary switch.

```text
role priority 16000
```

The vPC secondary switch will be left at the default value of 32667. The switch with lower priority will be elected as the vPC primary switch. If the vPC primary switch is alive, and the vPC peer link goes down, the vPC secondary switch will suspend its vPC member ports to prevent potential looping while the vPC primary switch keeps all of its vPC member ports active. If the peer link fails, the vPC peer will detect the peer switch’s failure through the vPC peer keepalive link.

Step 3: Configure vPC peer keepalive on both Cisco Nexus 5500s:

- On the first Cisco Nexus 5500UP, configure the peer-keepalive destination and source addresses.

  ```text
  peer-keepalive destination 10.10.63.11 source 10.10.63.10
  ```

- Change destination and source addresses and configure accordingly on the second Cisco Nexus 5500UP.

  ```text
  peer-keepalive destination 10.10.63.10 source 10.10.63.11
  ```

The peer-keepalive is ideally an alternate physical path between the two Cisco Nexus 5500UP switches running vPC to ensure that they are aware of one another’s health even in the case where the main peer link fails. The peer-keepalive source IP address should be the address being used on the mgmt0 interface of the switch currently being configured. The destination address is the mgmt0 interface on the vPC peer.

Step 4: Configure the following vPC commands, in the vPC domain configuration mode. This will increase resiliency, optimize performance, and reduce disruptions in vPC operations.

```text
delay restore 360
auto-recovery
graceful consistency-check
peer-gateway
```

The auto-recovery command has a default timer of 240 seconds. This time can be extended by adding the reload-delay variable with time in seconds. The auto-recovery feature for vPC recovery replaces the need for the original peer-config-check-bypass feature.

Step 5: Create a port channel interface to be used as the peer link between the two vPC switches. The peer link is the primary link for communications and for forwarding of data traffic to the peer switch if required.

```text
interface port-channel 10
switchport mode trunk
vpc peer-link
spanning-tree port type network
```
Step 6: Configure the physical interfaces that connect the two Cisco Nexus 5500s together to the port channel. A minimum of two physical interfaces is recommended for link resiliency.

**Tech Tip**

Different 10-Gigabit Ethernet ports (as required by your specific implementation) may replace the interfaces shown in the example.

```
interface Ethernet1/17
  description vpc peer link
  switchport mode trunk
  channel-group 10 mode active

interface Ethernet1/18
  description vpc peer link
  switchport mode trunk
  channel-group 10 mode active
```

Step 7: On the second Cisco Nexus 5500UP switch, repeat Step 4 through Step 6.

Step 8: Ensure that the vPC peer relationship has formed successfully by using the show vpc command.

```
dc5548ax# show vpc
Legend:
  (*) - local vPC is down, forwarding via vPC peer-link

vPC domain id : 10
Peer status : peer adjacency formed ok
vPC keep-alive status : peer is alive
Configuration consistency status: success
```

Per-vlan consistency status : success
Type-2 consistency status : success
vPC role : primary
Number of vPCs configured : 55
Peer Gateway : Enabled
Dual-active excluded VLANs : -
Graceful Consistency Check : Enabled

vPC Peer-link status
-------------------------------------------------------------
<table>
<thead>
<tr>
<th>id</th>
<th>Port</th>
<th>Status</th>
<th>Active vlans</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Po10</td>
<td>up</td>
<td>1</td>
</tr>
</tbody>
</table>

Step 9: Verify successful configuration by looking for the peer status of “peer adjacency formed ok” and the keep-alive status of “peer is alive”. If the status does not indicate success, double-check the IP addressing assigned for the keep-alive destination and source addresses, as well as the physical connections.

**Tech Tip**

Do not be concerned about the “(*) - local vPC is down, forwarding via vPC peer-link” statement at the top of the command output at this time. Once you have vPC port channels defined, and if one of its member links is down or not yet configured, this information becomes a legend that shows the meaning of an asterisk next to your port channel in the listing.
The data center core requires basic core operational configuration beyond the setup script.

### IP Subnet and VLAN Assignment

The IP Subnet and VLAN assignment follow the same guidance as the Cisco SBA for Midsize Borderless Networks—Foundation Deployment Guide. As you review configuration guidance, you may notice differences in the second octet. The second octet’s address is assigned based on which design the configuration was developed in:

- 8 and 9 are part of the midsize-1000 design
- 10 and 11 are part of the midsize-2500 design

The third octet is duplicated from one design to the next. For instance, the 10.x.48.0 subnet is a server-farm or data center subnet. For the LAN segments, matching the VLAN number to the IP subnet simplifies VLAN configuration. In this deployment guide, we have used the third octet of the IP address and added 100 to determine the VLAN number for easier reference. Adding 100 prevents a VLAN number from being one or zero, which can be a problem on some devices, while still making the VLAN ID easy to remember.

#### Table 1 - Data center VLANs

<table>
<thead>
<tr>
<th>VLAN Number</th>
<th>Purpose</th>
<th>Midsize-2500</th>
<th>Midsize-1000</th>
</tr>
</thead>
<tbody>
<tr>
<td>148</td>
<td>Servers_1</td>
<td>10.10.48.0/24</td>
<td>10.8.48.0/24</td>
</tr>
<tr>
<td>149</td>
<td>Servers_2</td>
<td>10.10.49.0/24</td>
<td>10.8.49.0/24</td>
</tr>
<tr>
<td>150</td>
<td>Servers_3</td>
<td>10.10.50.0/24</td>
<td>10.8.50.0/24</td>
</tr>
<tr>
<td>153</td>
<td>FW_Outside</td>
<td>10.10.53.0/24</td>
<td>10.8.53.0/24</td>
</tr>
<tr>
<td>154</td>
<td>FW_Inside_1</td>
<td>10.10.54.0/24</td>
<td>10.8.54.0/24</td>
</tr>
<tr>
<td>155</td>
<td>FW_Inside_2</td>
<td>10.10.55.0/24</td>
<td>10.8.55.0/24</td>
</tr>
<tr>
<td>156</td>
<td>PEERING_VLAN</td>
<td>10.10.56.0/24</td>
<td>10.8.56.0/24</td>
</tr>
<tr>
<td>159</td>
<td>1kv-Packet</td>
<td></td>
<td></td>
</tr>
<tr>
<td>160</td>
<td>1kv-Control</td>
<td></td>
<td></td>
</tr>
<tr>
<td>161</td>
<td>VMotion</td>
<td></td>
<td></td>
</tr>
<tr>
<td>162</td>
<td>iSCSI</td>
<td></td>
<td></td>
</tr>
<tr>
<td>163</td>
<td>DC-Management</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Step 1:** Create the necessary VLANs for the data center operation.

```bash
vlan [vlan number]
name [vlan name]
```

**Step 2:** Configure spanning tree.

Rapid Per-VLAN Spanning-Tree (PVST+) provides an instance of RSTP (802.1w) per VLAN. Rapid PVST+ greatly improves the detection of indirect failures or linkup restoration events over classic spanning tree (802.1D). The Cisco Nexus 5500UP runs Rapid PVST+ by default.

While this architecture is built without any Layer 2 loops, it is a good practice to assign spanning tree root to the core switches.

- Configure the primary Cisco Nexus 5500UP as the spanning-tree root.
  ```bash
  spanning-tree vlan 148-151,153-157,159-163 root primary
  ```
- Configure the second Cisco Nexus 5500UP as the spanning-tree secondary.
  ```bash
  spanning-tree vlan 148-151,153-157,159-163 root secondary
  ```

**Step 3:** Configure the name server command with the IP address of the DNS server for the network. At the command line of a Cisco IOS device, it is helpful to be able to type a domain name instead of the IP address.

```bash
ip name-server 10.10.48.10
```

**Step 4:** Set local time zone for the device location. The Network Time Protocol (NTP) is designed to synchronize time across all devices in a network for troubleshooting. In the initial setup script you set the NTP server address. Now set the local time for the device location.

```bash
clock timezone PST -8 0
clock summer-time PDT 2 Sunday march 02:00 1 Sunday nov 02:00 60
```

**Step 5:** Define a read-only and a read-write SNMP community for network management. In this example, the read-only community is “cisco” and the read write community is “cisco123”.

```bash
snmp-server community cisco group network-operator
snmp-server community cisco123 group network-admin
```
Step 6: Configure an inband management interface. This examples uses an IP address out of the data center core addressing with a 32-bit address (host) mask.

```plaintext
interface loopback 1
ip address 10.10.63.254/32
ip pim sparse-mode
```

The loopback interface is a logical interface that is always reachable as long as the device is powered on and any IP interface is reachable to the network. Because of this capability, the loopback address is the best way to manage the switch in-band and provides an additional management point to the out-of-band management interface. Layer 3 process and features are also bound to the Loopback interface to ensure process resiliency.

The loopback interface for the second Cisco Nexus 5500UP will be 10.10.63.253/32.

Step 7: Configure EtherChannel port-channels to use Layer 3 IP address and Layer 4 port number for load balance hashing. This optimizes load balancing on EtherChannel links and improves throughput to the Layer 3 routing engine in the Cisco Nexus 5500UP switch.

```plaintext
port-channel load-balance ethernet source-dest-port
```

Cisco NX-OS routing configuration follows an interface-centric model. Instead of adding networks to be advertised via network statements, EIGRP is enabled on a per-interface basis. Each Layer 3 interface that carries a network that may be advertised via EIGRP requires the `ip router eigrp` statement.

Step 3: Configure the core Layer 3 peering link.

```plaintext
Interface Vlan 156
ip address 10.10.56.1/30
ip router eigrp 1
ip pim sparse-mode
no shutdown
```

To pass EIGRP routing updates between routing peers, EIGRP must be enabled on each end of a Layer 3 link. To avoid unnecessary EIGRP peering between the core data center switches across all data center VLAN switched virtual interfaces, a single link will be used for active EIGRP peering in the data center core.

The peer Cisco Nexus 5500UP switch will use ip address 10.10.56.2/30.

---

**Procedure 5** Configure IP routing protocol

Step 1: Configure EIGRP as the IP routing protocol.

```plaintext
router eigrp 1
router-id 10.10.63.254
```

The router-id for the second Cisco Nexus 5500UP will be 10.10.63.253/32.

EIGRP is the IP routing protocol used in the midsize data center to be compatible with the midsize foundation LAN core and WAN. This example uses the same routing process ID so that routes can be exchanged with the LAN core.

In this configuration the only parameter configured under the EIGRP process (router eigrp 1) is the router-ID. The loopback 1 IP address is used for the EIGRP router ID.

Step 2: Configure EIGRP on Layer 3 interfaces.

```plaintext
interface loopback 1
ip router eigrp 1
```

**Procedure 6** Configure IP routing for VLANs

Every VLAN that needs Layer 3 reachability between VLANs or to the rest of the network requires a Layer 3 switched virtual interface (SVI) to route packets to and from the VLAN.

Step 1: Configure the SVI.

```plaintext
interface Vlan [vlan number]
```

Step 2: Configure the IP address for the SVI interface.

```plaintext
ip address [ip address]/mask
```

Step 3: Configure the EIGRP process number on the interface. This advertises the subnet into EIGRP.

```plaintext
ip router eigrp [router process + number]
```

Step 4: Configure passive mode EIGRP operation. To avoid unnecessary EIGRP peer processing, server VLANs are configure passive.

```plaintext
ip passive-interface [router process + number]
```
Step 5: Configure Hot Standby Routing Protocol (HSRP). The Nexus 5500UP switches use HSRP to provide a resilient default gateway in a vPC environment. For ease of use, number the HSRP process number the same as the SVI VLAN number. Configure a priority greater than 100 for the primary HSRP peer, leave the second switch at default priority of 100.

```
hsrp [process number]
priority [priority]
ip [ip address of default gateway]
```

### Tech Tip

Both data center core Cisco Nexus 5500UP switches can process packets for the assigned ip address of their SVI and for the HSRP address. In a vPC environment a packet to either switch destined for the default gateway (HSRP) address is locally switched and there is no need to tune aggressive HSRP timers to improve convergence time.

- The following is an example configuration for the first Nexus 5500UP switch.

```
interface Vlan148
no ip redirects
ip address 10.10.48.2/24
ip router eigrp 1
ip passive-interface eigrp 1
ip pim sparse-mode
hsrp 148
  priority 110
  ip 10.10.48.1
no shutdown
description Servers_1
```

- This is an example configuration for the peer Nexus 5500UP switch.

```
interface Vlan148
no ip redirects
ip address 10.10.48.3/24
ip router eigrp 1
ip passive-interface eigrp 1
```

### Procedure 7 Configure IP Multicast routing

The Cisco SBA Midsize Foundation network enables IP Multicast routing for the organization by using pim sparse-mode operation. The configuration of IP Multicast for the rest of the network can be found in the *Cisco SBA for Midsize Organizations—Borderless Networks Foundation Deployment Guide*.

Step 1: Configure the IP Multicast rendezvous point (RP) for the network as the **rp-address** and the IP Multicast subnet that it is serving with the **group-list**.

```
ip pim rp-address 10.10.15.252 group-list 239.1.0.0/16
```

Step 2: Configure an unused VLAN for IP Multicast replication synchronization between the core Cisco Nexus 5500UP switches.

```
vpc bind-vrf default vlan 900
```

### Tech Tip

The VLAN used for the IP Multicast bind-vrf cannot appear any place else in the configuration of the Cisco Nexus 5500UP switches. It must not be defined in the VLAN data base commands, and does not get included in the VLAN allowed list for the vPC core. It will automatically program packet replication across the vPC peer link trunk when needed.

Step 3: Configure IP Multicast to only be replicated across the vPC peer link when there is an orphan port of a vPC.

```
no ip igmp snooping mrouter vpc-peer-link
```
Step 4: Configure all Layer 3 interfaces for IP Multicast operation with the `pim sparse-mode` command.

```
ip pim sparse-mode
```

It is not necessary to configure `ip multicast` on the management VLAN interface(`interface vlan 163`).

### Procedure 8: Configure connectivity to SBA core

Virtual Port Channel does not support peering to another Layer 3 router across a vPC. This design will use dual-homed point-to-point Layer 3 interfaces between each data center core Cisco Nexus 5500UP switch to each Cisco Catalyst 6500 VSS core LAN switch for data to and from the data center to the rest of the network. If your design has a single resilient Cisco Catalyst 4500 with redundant supervisors and redundant line cards, you will instead connect each data center Cisco Nexus 5500UP switch to each of the redundant line cards.

It is recommended you have at least two physical interfaces from each switch connected to the network core, for a total port channel of four resilient physical 10-Gigabit Ethernet links and 40 Gbps of throughput.

**Step 1:** On the first data center core Cisco Nexus 5500UP, configure two point-to-point Layer 3 interfaces.

```
interface Ethernet1/19
  description Core Ten1/4/6
  no switchport
  ip address 10.10.24.2/30
  ip router eigrp 1
  ip pim sparse-mode

interface Ethernet1/20
  description Core Ten2/4/6
  no switchport
  ip address 10.10.24.6/30
  ip router eigrp 1
  ip pim sparse-mode
```

**Step 2:** On the second data center core Cisco Nexus 5500UP switch, configure two point-to-point Layer 3 interfaces.

```
interface Ethernet1/19
  description Core Ten1/4/8
  no switchport
  ip address 10.10.24.10/30
  ip router eigrp 1
  ip pim sparse-mode

interface Ethernet1/20
  description Core Ten2/4/8
  no switchport
  ip address 10.10.24.14/30
  ip router eigrp 1
  ip pim sparse-mode
```

**Step 3:** On the Cisco SBA Midsize Core 6500 VSS Switch, configure the four corresponding point-to-point Layer 3 links.

```
interface TenGigabitEthernet1/4/6
  description DC5548a Eth1/19
  no switchport
  ip address 10.10.24.1 255.255.255.252
  ip pim sparse-mode
```
Ethernet Infrastructure

February 2012 Series

For resiliency the Ethernet out-of-band management switch will be dual-homed to each of the data center core switches by using a vPC port channel.

Configure the following steps on each data center core Cisco Nexus 5500UP switch.

**Step 1:** Configure vPC port channel to the Ethernet management switch.

```plaintext
interface port-channel 21
  description Link to Management Switch for VLAN 163
  switchport mode trunk
  switchport trunk allowed vlan 163
  speed 1000
  vpc 21
```

**Step 2:** Configure the physical ports to belong to the port channel.

```plaintext
interface Ethernet 1/21
  switchport mode trunk
  switchport trunk allowed vlan 163
  speed 1000
  channel-group 21 mode active
```

**Step 3:** Configure an SVI interface for VLAN 163.

- Configure the first data center core Cisco Nexus 5500UP switch.

```plaintext
interface Vlan 163
  description DC-Management
  no ip redirects
  ip address 10.10.63.2/25
  ip router eigrp 1
```
Procedure 10 Configure Fabric Extender connections

Cisco Fabric Extender (FEX) ports are designed to support end host connectivity. There are some design rules to be aware of when connecting devices to Cisco FEX ports:

- Cisco FEX ports do not support connectivity to LAN switches that generate spanning tree Bridge Protocol Data Unit (BPDU) packets. If a Cisco FEX port receives a BPDU packet, it will shut down with an Error Disable status.
- Cisco FEX ports do not support connectivity to Layer 3 routed ports where routing protocols are exchanged with the Layer 3 core, they are only for Layer 2 connected end hosts or appliances.
- The Cisco Nexus 5500UP running Layer 3 routing supports a maximum of 8 connected Cisco FEX on a switch.

Additionally:

- Cisco Fabric Extender connections are also configured as port channel connections on the Cisco Nexus 5500 Series.
- If the Cisco FEX is to be single-homed to only one member of the switch pair, it is configured as a standard port channel.
- If the Cisco FEX is to be dual-homed to both members of the vPC switch pair to support single-homed servers, it is configured as a vPC port channel.

**Step 1:** Assign physical interfaces to the port channels that are supporting Cisco FEX attachment.

```plaintext
interface Ethernet1/13
  channel-group 102

interface Ethernet1/25
  channel-group 103

interface Ethernet1/26
  channel-group 103
```
Step 2: Configure port channel interfaces to support the Cisco FEX attachment. The switchport mode fex-fabric command informs the Cisco Nexus 5500UP Series switch that a fabric extender should be at the other end of this link.

```
interface port-channel 102
  description dual-homed 2248
  switchport mode fex-fabric
  vpc 102
  fex associate 102

interface port-channel 103
  description single-homed 2232
  switchport mode fex-fabric
  fex associate 103
```

Step 3: Once these configuration steps are completed, you can verify the status of the fabric extender modules by using the show fex command, and then looking for the state of “online” for each unit.

```
dc5548ax# show fex
FEX  FEX  FEX
Number Description  State  Model            Serial
-----------------------------------------------
 102     FEX0102     Online  N2K-C2248TP-1GE  SSI14140643
 103     FEX0103     Online  N2K-C2232PP-10GE  SSI142602QL
```

Tech Tip

It may take a few minutes for the Cisco FEX to come online once programmed because the initial startup of the Cisco FEX downloads operating code from the connected Cisco Nexus switch.

Procedure 11 Configure end node ports

Step 1: When connecting single-homed servers to a dual-homed Cisco FEX, assign physical interfaces to support servers or devices that belong in a single VLAN as access ports. Setting the spanning-tree port type to edge allows the port to provide immediate connectivity on the connection of a new device.

**Example**

```
interface Ethernet 102/1/1
  switchport access vlan 163
  spanning-tree port type edge
```

Tech Tip

You must assign the Ethernet interface configuration on both data center core Cisco Nexus 5500UP switches as the host is dual homed because it is on a dual-homed Cisco FEX.

Step 2: When connecting a single-homed server to a dual-homed Cisco FEX, assign physical interfaces to support servers or devices that require a VLAN trunk interface to communicate with multiple VLANs. Most virtualized servers will require trunk access to support management access, plus user data for multiple virtual machines. Setting the spanning-tree port type to edge allows the port to provide immediate connectivity on the connection of a new device.

**Example**

```
interface Ethernet 102/1/2
  switchport mode trunk
  switchport trunk allowed vlan 148-151,154-163
  spanning-tree port type edge trunk
```
Step 3: When connecting a dual-homed server that is using IEEE 802.3ad EtherChannel from the server to a pair of single-homed Cisco FEX, you must configure the Ethernet interface on the Cisco FEX as a port channel and assign a vPC interface as well to talk EtherChannel to the attached server. Since the server is dual-homed using vPC EtherChannel, this configuration must be done on both Cisco Nexus 5500UP data center core switches.

Example

```
interface ethernet103/1/1
  switchport mode trunk
  switchport trunk allowed vlan 148-151,154-163
  spanning-tree port type edge trunk
  channel-group 600
  no shutdown
interface port-channel 600
  vpc 600
  no shutdown
```

Tech Tip

When connecting ports via vPC, the Cisco NX-OS does consistency checks to make sure that the VLAN list, spanning-tree mode, and other characteristics match between the ports configured on each switch that make up a vPC. If the configuration for each port is not identical with the other, the port will not come up.

Summary

The configuration procedures provided in this section allow you to deploy a resilient Ethernet switching fabric for your midsize data center environment. This allows you to immediately take advantage of the high performance, low latency, and high availability characteristics inherent in the Cisco Nexus 5500UP and 2000 Series products. To investigate more advanced features for your configuration, please refer to the Cisco Nexus 5500 Series configuration guide series on cisco.com.
Business Overview

There is a constant demand for more storage in organizations today. Storage for servers can be physically attached directly to the server or connected over a network. Direct attached storage (DAS) is physically attached to a single server and is difficult to use efficiently because it can be used only by the host attached to it. Storage area networks (SANs) allow multiple servers to share a pool of storage over a Fibre Channel or Ethernet network. This capability allows storage administrators to easily expand capacity for servers supporting data-intensive applications.

Technology Overview

IP-based Storage Options

Many storage systems provide the option for access using IP over the Ethernet network. This approach allows a growing organization to gain the advantages of centralized storage without needing to deploy and administer a separate Fibre Channel network. Options for IP-based storage connectivity include Internet Small Computer System Interface (iSCSI) and network attached storage (NAS).

iSCSI is a protocol that enables servers to connect to storage over an IP connection and is a lower-cost alternative to Fibre Channel. iSCSI services on the server must contend for CPU and bandwidth along with other network applications, so you need to ensure that the processing requirements and performance are suitable for a specific application. iSCSI has become a storage technology that is supported by most server, storage, and application vendors. iSCSI provides block-level storage access to raw disk resources, similar to Fibre Channel. Network interface cards also can provide support to offload iSCSI to a separate processor to increase performance.

Network attached storage (NAS) is a general term used to refer to a group of common file access protocols, the most common implementations use common Internet file system (CIFS) or network file system (NFS). CIFS originated in the Microsoft network environment and is a common desktop file sharing protocol. NFS is a multi-platform protocol that originated in the UNIX environment and is a protocol that can be used for shared hypervisor storage. Both NAS protocols provide file-level access to shared storage resources.

Most organizations will have applications for multiple storage access technologies. For example, Fibre Channel for the high performance database and production servers and NAS for desktop storage access.

Fibre Channel Storage

Fibre Channel allows servers to connect to storage across a fiber-optic network, across a data center, or even across a WAN by using Fiber Channel over IP. Multiple servers can share a single storage array.

This Cisco SBA midsize data center architecture uses the Cisco Nexus 5500UP series switches as the core that provides Fibre Channel and Fibre Channel over Ethernet (FCoE) SAN switching. The Cisco Nexus 5500UP offers the density required for collapsed Fibre Channel connectivity requirements by supporting both Fibre Channel and FCoE servers and storage arrays. The Cisco MDS 9148 Multilayer Fabric Switch is ideal for a larger SAN fabric with up to 48 Fibre Channel ports, providing 48 line-rate 8-Gbps Fibre Channel ports and cost-effective scalability. The Cisco MDS family of Multilayer SAN Fabric Switches also offer options like hardware-based encryption services, tape acceleration, and Fibre Channel over IP for longer distance SAN extension.

In a SAN, a fabric consists of servers and storage connected to a Fibre Channel switch (Figure 12). It is standard practice in SANs to create two completely separate physical fabrics, providing two distinct paths to the storage. Fibre Channel fabric services operate independently on each fabric so when a server needs resilient connections to a storage array, it connects to two separate fabrics. This design prevents failures or misconfigurations in one fabric from affecting the other fabric.
Each server or host on a SAN connects to the Fibre Channel switch with a multi-mode fiber cable from a host bus adapter (HBA). For resilient connectivity, each host connects a port to each of the fabrics.

Each port has a port worldwide name (pWWN), which is the port’s address that uniquely identifies it on the network. An example of a pWWN is: 10:00:00:00:c9:87:be:1c. In data networking this would compare to a MAC address for an Ethernet adapter.

Virtual Storage Area Networks

The virtual storage area network (VSAN) is a technology created by Cisco that is modeled after the virtual local area network (VLAN) concept in Ethernet networks. VSANs provide the ability to create many logical SAN fabrics on a single Cisco MDS 9100 Family switch. Each VSAN has its own set of services and address space, which prevents an issue in one VSAN from affecting other VSANs. In the past, it was a common practice to build physically separate fabrics for production, backup, lab, and departmental environments. VSANs allow all of these fabrics to be created on a single physical switch with the same amount of protection provided by separate switches.

Zoning

The terms target and initiator will be used throughout this section. Targets are disk or tape devices. Initiators are servers or devices that initiate access to disk or tape.

Zoning provides a means of restricting visibility and connectivity between devices connected to a SAN. The use of zones allows an administrator to control which initiators can see which targets. It is a service that is common throughout the fabric and any changes to a zoning configuration are disruptive to the entire connected fabric.

Initiator-based zoning allows for zoning to be port-independent by using the world wide name (WWN) of the end host. If a host’s cable is moved to a different port, it will still work if the port is a member of the same VSAN.

Device Aliases

When configuring features such as zoning, quality of service (QoS), and port security on a Cisco MDS 9000 Family switch, WWNs must be specified. The WWN naming format is cumbersome and manually typing WWNs is error prone. Device aliases provide a user-friendly naming format for WWNs in the SAN fabric (for example: “p3-c210-1-hba0-a” instead of “10:00:00:00:c9:87:be:1c”).

Use a naming convention that makes initiator and target identification easy. An example is below.

p3-c210-1-hba0-a in this setup identifies:
- Rack location: P3
- Host type: C210
- Host number: 1
- HBA number: hba0
- Port on HBA: a

Storage Array Tested

The storage arrays used in the testing and validation of this deployment guide are the EMC™ CX4-120 and the NetApp™ FAS3140. The specific storage array configuration may vary. Please consult the installation instructions from the specific storage vendor. The Cisco interoperability support matrix for Fibre Channel host bus adapters and storage arrays can be found at: http://www.cisco.com/en/US/docs/switches/datacenter/mds9000/interop-erability/matrix/intmatrix.html
Deployment Details

Deployment examples documented in this section include:

- Configuration of a Cisco Nexus 5500UP-based SAN network to support Fiber Channel based storage.
- Configuration of a Cisco MDS SAN switch for larger Fiber Channel environments.
- FCoE access to storage from Cisco UCS C-Series servers using the Cisco Nexus 5500.

Process

Configuring Fibre Channel SAN on Cisco Nexus 5500UP Switch

1. Configure Fibre Channel operation
2. Configure VSANs
3. Configure Fibre Channel ports
4. Configure device aliases
5. Configure zoning
6. Verify the configuration

Complete each of the following procedures to configure the Fibre Channel SAN on the data center core Cisco Nexus 5500UP switches.

Procedure 1 Configure Fibre Channel operation

The Nexus 5500UP switch has universal ports that are capable of running Ethernet+FCoE or Fiber Channel on a per port basis. All switch ports are by default enabled for Ethernet operation. Fiber channel ports must be enabled in a contiguous range and be the high numbered ports of the switch baseboard and/or the high numbered ports of a universal port expansion module.

Reader Tip

The first part of this procedure was outlined in the previous Ethernet section of this deployment guide. If you have already configured ports for Fibre Channel operation, you can skip Step 1 through Step 3 of this procedure.

Tech Tip

In this design we will enable ports 28 through 32 on the Cisco Nexus 5548UP switch as Fiber Channel ports.

Step 1: Configure universal port mode for Fibre Channel.

```
slot 1
port 28-32 type fc
```

Tech Tip

Changing port type to fc requires a reboot in Cisco Nexus 5500UP version 5.1(3)N1(1) software to recognize the new port operation. This is subject to change in later releases of software. Ports will not show up in the configuration as “fc” ports if you did not enable the feature fcoe in the previous step.
Step 2: If you are changing the port type at this time, save your configuration and reboot the switch so that the switch recognizes the new ‘fc’ port type operation. If you have already done this there is no need to reboot.

Step 3: If you have not done so, enable fcoe operation, which enables both native Fibre Channel and FCoE operation.

```plaintext
feature fcoe
```

Reader Tip

In the previous Ethernet section of this deployment guide we showed enabling feature fcoe.

Step 4: Enable san port-channel trunking operation and fiber channel N port Interface virtualization for connecting to Cisco UCS fabric interconnects.

```plaintext
feature npiv
feature fport-channel-trunk
```

More detail for connecting to a Cisco UCS B-Series fabric interconnect for Fibre Channel operation can be found in the Cisco SBA for Midsized Organizations— Data Center Unified Computing System Deployment Guide.

Procedure 2 Configure VSANs

The Cisco MDS Device Manager provides a graphical interface to configure Cisco Nexus switch capable of Fibre Channel switching or a Cisco MDS 9100 Family switch. To access the Device Manager, connect to the management address via HTTP or access it directly through Cisco Fabric Manager.

The CLI can also be used to configure Fibre Channel operation.

```plaintext
feature npiv
feature fport-channel-trunk
```

Tech Tip

Java runtime environment (JRE) is required to run Cisco Fabric Manager and Device Manager and should be installed on your desktop before accessing either application.

Cisco DCNM for SAN Essentials Edition is a no cost application available for download from Cisco.com to configure SAN devices. Managing more than one switch at the same time requires a licensed version.

By default, all ports are assigned to VSAN 1 at initialization of the switch. It is a best practice to create a separate VSAN for production and to leave VSAN 1 for unused ports. By not using VSAN 1, you can avoid future problems with merging of VSANs when combining other existing switches that may be set to VSAN 1.

Fibre Channel operates in a “SAN A” and “SAN B” approach, where you create two separate SAN fabrics. Fibre Channel hosts and targets connect to both fabrics for redundancy. The SAN fabrics operate in parallel.

The example below describes creating two VSANs, one on each data center core Nexus 5500UP switch.
You can use the command-line interface (CLI) or Device Manager to create a VSAN.

**Step 1:** Using Device Manager, click **FC > VSANS**. The Create VSAN General window appears.

**Step 2:** Set the VSAN id at 4 and the name as **General-Storage**.

**Step 3:** Next to the Interface Members box, click the ellipsis (…) button.

**Step 4:** Select the interface members by clicking the port numbers you want.

**Step 5:** Click **Create**. The VSAN is created. You can add additional VSAN members in the Membership tab of the main VSAN window.

The preceding steps apply this configuration in CLI.

```bash
vsan database
vsan 4 name "General-Storage"
vsan 4 interface fc1/28
```

**Step 6:** Repeat the steps in this procedure to create a VSAN 5 on the second Cisco Nexus 5500UP switch. Use the same VSAN name.

**Procedure 3** Configure Fibre Channel ports

By default, the ports are configured for port mode **Auto** and this setting should not need to be changed for most devices that are connected to the fabric. However, you will have to assign a VSAN to the port.

**Step 1:** If you want to change the port mode by using Device Manager, right-click the port you want to configure.
The General tab appears.

You can see in this figure that the PortVSAN assignment is listed in the top left of the General panel.

**Step 2:** Click **up** for Status Admin to enable the port.

**Step 3:** Assign VSAN 4 or VSAN 5 to the port from the drop down list, depending on which switch you are working on, and then click **Apply** to change the VSAN and activate the ports.

The preceding steps apply this configuration in CLI.

```
vsan database
vsan 4 interface fc1/28
```

This step assigns ports to a vsan similar to Step 3 in the previous procedure of “Configure VSANs”. If you have already created vsans, this is another way to assign a port to a vsan.

**Step 4:** Connect Fibre Channel devices to ports.

For more information about preparing Cisco UCS B-Series and C-Series servers for connecting to the Fibre Channel network see the Cisco SBA for Midsize Organizations—Data Center Unified Computing System Deployment Guide.

**Step 5:** Display fabric login by entering the **show flogi database** on the switch CLI.

**Tech Tip**

When the initiator or target is plugged in or starts up, it automatically logs into the fabric. Upon login, the initiator or target WWN is made known to the fabric. Until you have storage arrays or servers with active host bus adapters plugged into the switch on fibre channel ports you will not see entries in the flogi database.

**Example**

dc5548ax# show flogi database

```
+-------------------+-------------------+-------------------+-------------------+
| INTERFACE | VSAN | FCID       | PORT NAME          | NODE NAME          |
|-----------+------|------------+-------------------+-------------------|
| fc1/29    | 4     | 0x0bc0002  | 20:41:00:05:73:a2:b2:40 | 20:04:00:05:73:a2:b2:41 |
| fc1/29    | 4     | 0x0bc0005  | 20:00:00:25:b5:77:77:9f | 20:00:00:25:b5:00:77:9f |
| fc1/30    | 4     | 0x0bc0004  | 20:42:00:05:73:a2:b2:40 | 20:04:00:05:73:a2:b2:41 |
| vfc1      | 4     | 0x0bc0000  | 20:00:58:8d:09:0e:e0:d2 | 10:00:58:8d:09:0e:e0:d2 |
| vfc27     | 4     | 0x0bc0006  | 50:0a:09:81:89:3b:63:be | 50:0a:09:80:89:3b:63:be |

Total number of flogi = 5.
```
**Procedure 4 Configure device aliases**

Device aliases map the long WWNs for easier zoning and identification of initiators and targets. An incorrect device name may cause unexpected results. Device aliases can be used for zoning, port-security, QoS, and show commands.

You can configure device aliases via Device Manager or CLI.

**Option 1. Configure device aliases by using Device Manager**

**Step 1:** In Device Manager, access the Device Alias window by navigating to FC > Advanced > Device Alias.

**Step 2:** Click Create.

**Step 3:** Enter a device alias name, and paste in or type the WWN of the host, and then click **Create**.

**Step 4:** Once you have created your devices aliases, click **CFS > Commit**. The changes are written to the database.

**Option 2. Configure device aliases by using CLI**

**Step 1:** Enter device alias database configuration mode.

```
device-alias database
```

**Step 2:** Enter device alias names mapping to a PWWN from the flogi database above. As an example:

```
device-alias name emc-a0-fc pwwn 50:06:01:61:3c:e0:30:59
device-alias name emc-2-a0-fc pwwn 50:06:01:61:3c:e0:60:e2
device-alias name Netapp-e2a-FCOE pwwn 50:0a:09:82:89:ea:df:b1
device-alias name NetApp2-e2a-FCOE pwwn 50:0a:09:81:89:3b:63:be
device-alias name p12-c210-27-vhba3 pwwn 20:00:58:8d:09:0e:e0:d2
```

**Step 3:** Type **exit**. This exits device-alias configuration mode.

```
exit
```

**Step 4:** Commit the changes.

```
device-alias commit
```
**Step 5:** Enter the show flogi database command. Aliases are now visible.

```
dc5548ax# sh flogi database
```

<table>
<thead>
<tr>
<th>INTERFACE</th>
<th>VSAN</th>
<th>FCID</th>
<th>PORT NAME</th>
<th>NODE NAME</th>
</tr>
</thead>
<tbody>
<tr>
<td>fc1/29</td>
<td>4</td>
<td>0xbc00002</td>
<td>20:41:00:05:73:a2:b2:40</td>
<td>20:00:00:05:73:a2:b2:40</td>
</tr>
<tr>
<td>fc1/29</td>
<td>4</td>
<td>0xbc0005</td>
<td>20:00:00:25:57:77:77:9f</td>
<td>20:00:00:25:57:00:77:9f</td>
</tr>
<tr>
<td>fc1/30</td>
<td>4</td>
<td>0xbc0004</td>
<td>20:42:00:05:73:a2:b2:40</td>
<td>20:04:00:05:73:a2:b2:40</td>
</tr>
<tr>
<td>vfc1</td>
<td>4</td>
<td>0xbc0000</td>
<td>20:00:58:8d:09:0e:e0:d2</td>
<td>10:00:58:8d:09:0e:e0:d2</td>
</tr>
<tr>
<td>vfc27</td>
<td>4</td>
<td>0xbc0006</td>
<td>50:0a:09:81:89:3b:63:be</td>
<td>50:0a:09:80:89:3b:63:be</td>
</tr>
</tbody>
</table>

**Tech Tip**

A zoneset is a collection of zones. Zones are members of a zone-set. After you add all the zones as members, you must activate the zoneset. There can only be one active zoneset per VSAN.

**Procedure 5  Configure zoning**

Leading practices for zoning:

- Configure zoning between a single initiator and a single target per zone.
- A single initiator can also be configured to multiple targets in the same zone.
- Zone naming should follow a simple naming convention of `initiator_x_target_x`:
  - `p12-ucs-b-fc0-vhba1_emc-2`
- Limiting zoning to a single initiator with a single target or multiple targets helps prevent disk corruption and data loss.

Zoning can be configured from the CLI and from Fabric Manager.

**Option 1. Configure a zone by using CLI**

**Step 1:** In configuration mode, enter the zone name and vsan number.

```
zone name p12-ucs-b-fc0-vhba1_emc-2 vsan 4
```

**Step 2:** Specify device members by WWN or device alias.

```
member device-alias emc-2-a0-fc
member pwwn 20:00:00:25:57:77:77:9f
```

**Step 3:** Create and activate a zoneset.

```
zoneset name FCOE_4 vsan 4
```

**Step 4:** Add members to the zoneset.

```
member p12-ucs-b-fc0-vhba1_emc-2
member p12-c210-27-vhba3_netapp-2-e2a
```

**Step 5:** Once all the zones for VSAN 4 are created and added to the zone-set, activate the configuration.

```
zoneset activate name FCOE_4 vsan 4
```

**Step 6:** Distribute the zone database to other switches in the SAN. This prepares for expanding your Fibre Channel SAN beyond a single switch.

```
zoneset distribute full vsan 4
```
**Option 2. Configure a zone by using Data Center Network Manager**

**Step 1:** Install Cisco Data Center Network Manager for SAN Essentials.

**Reader Tip**

Cisco DCNM-SAN Essentials edition is available at no charge to manage Cisco Nexus and MDS SAN switches and can be downloaded from [http://www.cisco.com](http://www.cisco.com). DCNM-SAN Essentials replaces the previous Cisco Fabric Manager product.

**Step 2:** Log into DCNM-SAN manager. The default username and password is admin/password.

**Step 3:** Choose a seed switch by entering the IP address of the first Cisco Nexus 5500UP (for example, 10.10.63.10), and then choosing Cisco Nexus 5500UP from the list.

**Step 4:** From the DCNM-SAN menu, click **Zone**, and then click **Edit Local Full Zone Database**.

**Step 5:** In the Zone Database window, on the left side, right-click **Zones**, and then click **Insert**. This creates a new zone.

**Step 6:** In the Zone Name box, enter the name of the new zone, and then click **OK**.
Step 7: Select the new zone, and then, from the bottom of the right-hand side of the database window, choose initiator or targets you want to add to the zone. Click Add to Zone.

Step 8: Right-click Zoneset to insert a new zoneset.

Step 9: Drag the zones you just created from the zone box to the zoneset folder that you created.

Step 10: Click Activate. This activates the configured zoneset.

Step 11: In the Save Configuration dialog box, select Save Running to Startup Configuration, and then click Continue Activation.

Step 12: Configure SAN B the same way by using the procedures in this process to create VSAN 5 on the second data center core Cisco Nexus 5500UP switch.

Procedure 6 Verify the configuration

Step 1: Verify the Fibre Channel login.

In a Fibre Channel fabric, each host or disk requires a Fibre Channel ID (FC ID). When a fabric login (FLOGI) is received from the device, this ID is assigned by the fabric. If the required device is displayed in the FLOGI table, the fabric login is successful.

```
dc5548ax# show flogi database
```

<table>
<thead>
<tr>
<th>INTERFACE</th>
<th>VSAN</th>
<th>FCID</th>
<th>PORT NAME</th>
<th>NODE NAME</th>
</tr>
</thead>
<tbody>
<tr>
<td>fc1/29</td>
<td>4</td>
<td>0xbc0002</td>
<td>20:41:00:05:73:a2:b2:40</td>
<td>20:04:00:05:73:a2:b2:41</td>
</tr>
<tr>
<td>fc1/29</td>
<td>4</td>
<td>0xbc0005</td>
<td>20:00:00:25:b5:77:77:9f</td>
<td>20:00:00:25:b5:00:77:9f</td>
</tr>
<tr>
<td>fc1/30</td>
<td>4</td>
<td>0xbc0004</td>
<td>20:42:00:05:73:a2:b2:40</td>
<td>20:04:00:05:73:a2:b2:41</td>
</tr>
<tr>
<td>vfc1</td>
<td>4</td>
<td>0xbc0000</td>
<td>20:00:58:8d:09:0e:e0:d2</td>
<td>10:00:58:8d:09:0e:e0:d2</td>
</tr>
</tbody>
</table>

Total number of flogi = 5.
Step 2: Verify Fibre Channel Name Server (FCNS) attributes.

The FCNS database shows the same PWWN login along with vendor specific attributes and features. Check that your initiators and targets have logged in and show `FC4-TYPE:FEATURE` attributes as highlighted below. If the feature attributes do not show then you may have a part of the configuration on the end host or storage device misconfigured or a device driver issue.

dc5548ax# show fcns database

VSAN 4:

```
+-------------------+---------+----------------+-----------------+------------------+
<table>
<thead>
<tr>
<th>FCID</th>
<th>TYPE</th>
<th>PWWN</th>
<th>(VENDOR)</th>
<th>FC4-TYPE:FEATURE</th>
</tr>
</thead>
<tbody>
<tr>
<td>0xb90100</td>
<td>N</td>
<td>50:06:01:61:3c:e0:60:e2</td>
<td>(Clariion)</td>
<td>scsi-fcp:target</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>[emc-2-a0-fc]</td>
<td></td>
</tr>
<tr>
<td>0xbc0000</td>
<td>N</td>
<td>20:00:58:8d:09:e0:e0:d2</td>
<td></td>
<td>scsi-fcp:init fc-gs</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>[p12-c210-27-vhba3]</td>
<td></td>
</tr>
<tr>
<td>0xbc0002</td>
<td>N</td>
<td>20:41:00:05:73:a2:b2:40</td>
<td>(Cisco)</td>
<td>npv</td>
</tr>
<tr>
<td>0xbc0004</td>
<td>N</td>
<td>20:42:00:05:73:a2:b2:40</td>
<td>(Cisco)</td>
<td>npv</td>
</tr>
<tr>
<td>0xbc0005</td>
<td>N</td>
<td>20:00:00:25:b5:77:77:9f</td>
<td></td>
<td>scsi-fcp:init fc-gs</td>
</tr>
<tr>
<td>0xbc0006</td>
<td>N</td>
<td>50:0a:09:81:89:3b:63:be</td>
<td>(NetApp)</td>
<td>scsi-fcp:target</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>[NetApp2-e2a-FCOE]</td>
<td></td>
</tr>
</tbody>
</table>
```

Total number of entries = 6

Step 3: Verify active zoneset.

Check the fabric configuration for proper zoning by using the `show zoneset active` command, which displays the active zoneset. Each zone that is a member of the active zoneset is displayed with an asterisk (*) to the left of the member. If there is not an asterisk to the left, the host is either down and not logged into the fabric or there is a misconfiguration of the port VSAN or zoning. Use the `show zone` command to display all configured zones on the Cisco Fibre Channel switches.

dc5548ax# show zoneset active

```
zoneset name FCOE_4 vsan 4
zone name p12-ucs-b-fc0-vhba1_emc-2 vsan 4
  * fcid 0xb90100 [pwwn 50:06:01:61:3c:e0:60:e2] [emc-2-a0-fc]
  * fcid 0xbc0005 [pwwn 20:00:00:25:b5:77:77:9f]

zone name p12-c210-27-vhba3_netapp-2-e2a vsan 4
  * fcid 0xbc0006 [pwwn 50:0a:09:81:89:3b:63:be] [NetApp2-e2a-FCOE]
  * fcid 0xbc0000 [pwwn 20:00:58:8d:09:e0:e0:d2] [p12-c210-27-vhba3]
```

Step 4: Test Fibre Channel reachability by using the `fcping` command, and then trace the routes to the host by using the `fctrace` command.

Tech Tip

Cisco created these commands to provide storage networking troubleshooting tools that are familiar to individuals who use ping and traceroute.
If your Fibre Channel SAN environment requires a higher density of Fibre Channel port connectivity, you may choose to use Cisco MDS 9100 series SAN switches.

The following procedures describe how to deploy a Cisco MDS 9124 or 9148 SAN switch to connect to the data center core Cisco Nexus 5500UP switches.

### Procedure 1: Perform initial setup for MDS switch

The following is required to complete this procedure:
- Setting a management IP address
- Configuring console access
- Configuring a secure password

When initially powered on, a new Cisco MDS 9148 switch starts a setup script when accessed from the console.

**Step 1:** Follow the prompts in the setup script to configure login, out-of-band management, SSH, Network Time Protocol, switch port modes, and default zone policies.

```
---- System Admin Account Setup ----
Do you want to enforce secure password standard (yes/no) [y]: y
Enter the password for “admin”:
Confirm the password for “admin”:
---- Basic System Configuration Dialog ----
This setup utility will guide you through the basic configuration of the system. Setup configures only enough connectivity for management of the system. *Note: setup is mainly used for configuring the system initially, when no configuration is present. So setup always assumes system defaults and not the current system configuration values.*
Press Enter at anytime to skip a dialog. Use ctrl-c at anytime to skip the remaining dialogs.
Would you like to enter the basic configuration dialog (yes/no): y
Create another login account (yes/no) [n]:
Configure read-only SNMP community string (yes/no) [n]:
Configure read-write SNMP community string (yes/no) [n]:
Enter the switch name: mds9148ax
```
Continue with Out-of-band (mgmt0) management configuration? (yes/no) [y]: y

Mgmt0 IPv4 address: 10.10.63.12
Mgmt0 IPv4 netmask: 255.255.255.128

Configure the default gateway? (yes/no) [y]: y
IPv4 address of the default gateway: 10.10.63.1

Configure advanced IP options? (yes/no) [n]:
Enable the ssh service? (yes/no) [y]: y
Type of ssh key you would like to generate (dsa/rsa): rsa
Number of rsa key bits <768-2048> [1024]: 2048

Enable the telnet service? (yes/no) [n]:
Configure clock? (yes/no) [n]:
Configure timezone? (yes/no) [n]:
Configure summertime? (yes/no) [n]:
Configure the ntp server? (yes/no) [n]: y
NTP server IPv4 address: 10.10.48.17

Configure default switchport interface state (shut/noshut): noshut
Configure default switchport trunk mode (on/off/auto) [on]:
Configure default switchport port mode F (yes/no) [n]:
Configure default zone policy (permit/deny) [deny]:
Enable full zoneset distribution? (yes/no) [n]:
Configure default zone mode (basic/enhanced) [basic]:

The following configuration will be applied:
password strength-check
switchname mds9148ax
interface mgmt0
  ip address 10.10.63.12 255.255.255.128
  no shutdown
  ip default-gateway 10.10.63.1
  ssh key rsa 2048 force
  feature ssh
  no feature telnet
  feature http-server
  ntp server 10.10.48.17

system default switchport shutdown
system default switchport trunk mode on
system default zone default-zone permit
system default zone distribute full
system default zone mode enhanced

Would you like to edit the configuration? (yes/no) [n]: n
Use this configuration and save it? (yes/no) [y]: y
[########################################] 100%

Network Time Protocol (NTP) is critical to troubleshooting and should not be overlooked.

Step 2: Run the setup script for the second Cisco MDS 9100 switch using a unique switch name, and 10.10.63.13 for the Mgmt0 IPv4 address.

Step 3: Set the SNMP strings in order to enable managing MDS switches with Device Manager. Set both the read-only (network-operator) and read-write (network-admin) SNMP strings:

- snmp-server community cisco group network-operator
- snmp-server community cisco123 group network-admin

Step 4: Configure the clock. In the setup mode, you configured the NTP server address. In this step, configuring the clock enables the clock to use the NTP time for reference and makes the switch output match the local timezone.

clock timezone PST -8 0

Step 6: Configure the clock. In the setup mode, you configured the NTP server address. In this step, configuring the clock enables the clock to use the NTP time for reference and makes the switch output match the local timezone.

clock timezone PST -8 0

clock summer-time PDT 2 Sunday march 02:00 1 Sunday nov 02:00 60
Procedure 2  Configure VSANs

To configure the Cisco MDS switches to expand the Fibre Channel SAN that you built on the Cisco Nexus 5500UP switches, use the same VSAN numbers for SAN A and SAN B, respectively. The CLI and GUI tools work the same way for Cisco MDS as they do with the Cisco Nexus 5500UP.

Step 1: In Device Manager, click FC > VSANS.

The Create VSAN General window appears.

Step 2: In the VSAN id list, choose 4, and then, in the Name box, enter General-Storage.

Step 3: Click Create.

The preceding steps apply this configuration in CLI.

    vsan database
    vsan 4 name "General-Storage"

Step 4: Configure the second MDS SAN switch for vsan 5 and vsan name General-Storage using steps 1 through 3 above.

Procedure 3  Configure trunk for SAN interconnect

Connect the Cisco MDS switch to the existing Nexus 5500UP core Fibre Channel SAN.

Step 1: In Device Manager, navigate to Cisco MDS switch.

Step 2: In the Device Manager screen, click Interfaces > Port Channels, and then click Create to configure the trunk ports on the Cisco MDS.
Step 3: Choose the port channel Id number, select **trunk**, select **Mode E**, and then select **Force**.

Step 4: In the Allowed VSANs box, enter **1,4**. For the Cisco MDS switch for SAN Fabric B, the VSANs to enter would be **1** and **5**.

Step 5: To the right of the Interface Members box, click **...** and then select the **Interface Members** that will belong to this port channel.

Step 6: Click **Create**. The new port channel is created.

The preceding steps apply this Cisco MDS 9100 configuration to the MDS SAN-A switch:

```
interface port-channel 1
  switchport mode E
  switchport trunk allowed vsan 1
  switchport trunk allowed vsan add 4
  switchport rate-mode dedicated

interface fc1/13
  switchport mode E
  channel-group 1 force
  switchport rate-mode dedicated

interface fc1/14
  switchport mode E
  channel-group 1 force
  switchport rate-mode dedicated
```

The preceding steps apply this Cisco MDS 9100 configuration to the MDS SAN-B switch:

```
interface port-channel 1
  switchport mode E
  switchport trunk allowed vsan 1
  switchport trunk allowed vsan add 5
  switchport rate-mode dedicated

interface fc1/13
  switchport mode E
  channel-group 1 force
  switchport rate-mode dedicated

interface fc1/14
  switchport mode E
  channel-group 1 force
  switchport rate-mode dedicated
```
Step 7: Create the corresponding SAN port channel to connect to the Cisco MDS switch for the Cisco Nexus 5500UP by following the preceding steps in this procedure (Procedure 3).

The resulting Cisco Nexus 5500UP CLI for this SAN port channel is the following for the SAN-A switch.

```text
interface san-port-channel 31
    switchport trunk allowed vsan 1
    switchport trunk allowed vsan add 4

interface fc1/31
    switchport description Link to dcmds9148ax port fc-1/13
    channel-group 31 force
    no shutdown

interface fc1/32
    switchport description Link to dcmds9148ax port fc1/14
    channel-group 31 force
    no shutdown
```

The resulting Cisco Nexus 5500UP CLI for this SAN port channel is the following for the SAN-B switch.

```text
interface san-port-channel 31
    switchport trunk allowed vsan 1
    switchport trunk allowed vsan add 4

interface fc1/31
    switchport description Link to dcmds9148bx port fc-1/13
    channel-group 31 force
    no shutdown

interface fc1/32
    switchport description Link to dcmds9148bx port fc1/14
    channel-group 31 force
    no shutdown
```

Step 8: Distribute the zone database created on the Cisco Nexus 5500UP switch to new MDS 9100 switch.

Configure the Cisco Nexus 5500UP CLI for SAN-A to distribute the zone database to the new MDS9100 switch.

```text
zoneset distribute full vsan 4
```

Configure the Cisco Nexus 5500UP CLI for SAN-B to distribute the zone database to the new MDS9100 switch.

```text
zoneset distribute full vsan 5
```
Cisco UCS C-series rack servers ship with onboard 10/100/1000 Ethernet adapters and a Cisco Integrated Management Controller (CIMC), which uses a 10/100 Ethernet port. To get the most out of the rack servers and minimize cabling in the SBA Unified Computing architecture, the Cisco UCS C Series rack-mount server is connected to a unified fabric. The Cisco Nexus 5500UP Series switch that connects the Cisco UCS 5100 Series Blade Server Chassis to the network can also be used to extend Fibre Channel traffic over 10-Gigabit Ethernet. The Cisco Nexus 5500UP Series switch consolidates I/O onto one set of 10-Gigabit Ethernet cables, eliminating redundant adapters, cables, and ports. A single converged network adapter (CNA) card and set of cables connects servers to the Ethernet and Fibre Channel networks by using Fibre Channel over Ethernet (FCoE). It also allows the use of a single cabling infrastructure within server racks.

In the Cisco SBA midsize data center architecture, the Cisco UCS C Series rack-mount server is configured with a dual-port CNA. Cabling the Cisco UCS C Series with a CNA limits the cables to three, one for each port on the CNA and the CIMC connection.

### Tech Tip

A server connecting to the Cisco Nexus 5500UP that is running FCoE consumes a Fibre Channel port license. If you are connecting the FCoE attached servers to a Cisco FEX model 2232PP, then only the 5500UP ports connected to the Cisco FEX require a Fibre Channel port license for each port connecting to the Cisco FEX. This way you could connect up to 32 FCoE servers to a Cisco FEX 2232PP and only use Fibre Channel port licenses for the Cisco FEX uplinks.

A standard server without a CNA could have a few Ethernet connections or multiple Ethernet and Fibre Channel connections. The following figure shows a topology with mixed unified fabric, standard Ethernet and Fibre Channel connections, and the optional Cisco MDS 9100 Series for Fibre Channel expansion.

### Process

Configuring for FCoE Host Connectivity

1. Configure FCoE QoS
2. Configure host facing FCoE ports
3. Verify FCoE connectivity
The Cisco UCS C Series is connected to both Cisco Nexus 5500UP Series switches from the CNA with twinax or fiber optic cabling. The Cisco UCS server running FCoE can also attach to a single-homed Cisco FEX model 2232PP.

**Tech Tip**

At this time FCoE connected hosts can only connect over 10-Gigabit Ethernet and must use a fiber optic or twinax connection.

The recommended approach is to connect the CIMC 10/100 management port(s) to an Ethernet port on the out-of-band management switch. Alternatively, you can connect the Cisco IMC management port(s) to a Cisco Nexus 2248 fabric extender port in the management VLAN (163).

**Nexus 5500UP Configuration for FCoE**

In previous sections we have enabled the Cisco Nexus 5500UP Series FCoE functionality. In this section we will configure the following items to allow a Cisco C-Series server to connect using FCoE:

- Creating a virtual Fibre Channel interface
- Assigning the VSAN to a virtual Fibre Channel interface
- Configuring the Ethernet port and trunking

**Procedure 1**  **Configure FCoE QoS**

Configuration is the same across both of the Cisco Nexus 5500UP Series switches with the exception of the VSAN configured for SAN fabric A and for SAN fabric B.

The Cisco Nexus 5500UP, unlike the Cisco Nexus 5010, does not preconfigure QoS for FCoE traffic.

**Step 1:** Configure FCoE QoS by entering the following commands in global configuration mode.

```
Tech Tip

There are four lines of QoS statements that map the existing system QoS policies for FCoE. Without these commands, the virtual Fibre Channel interface will not come up when activated.

system qos
service-policy type qos input fcoe-default-in-policy
service-policy type queuing input fcoe-default-in-policy
service-policy type queuing output fcoe-default-out-policy
service-policy type network-qos fcoe-default-nq-policy
```

**Procedure 2**  **Configure host facing FCoE ports**

On the Cisco Nexus 5500UP switch, configure the Ethernet ports connected to the CNA in the host.

**Step 1:** Create a VLAN that will carry FCoE traffic to the host.

- In this example, VLAN 304 is mapped to VSAN 4. VLAN 304 carries all VSAN 4 traffic to the CNA over the trunk for the first Cisco Nexus 5500UP.
  ```
  vlan 304
  fcoe vsan 4
  exit
  ```
- On the second Cisco Nexus 5500UP, VLAN 305 is mapped to VSAN 5.
  ```
  vlan 305
  fcoe vsan 5
  exit
  ```
Step 2: Create a virtual Fibre Channel (vfc) interface for Fiber Channel traffic, and then bind it to the corresponding host Ethernet interface. You need to do this in order to be able to map an FCoE interface to Fiber Channel.

This example shows binding to a Cisco FEX 2232PP Ethernet interface. This command will be the same on both Cisco Nexus 5500UP switches.

```
interface vfc1
  bind interface Ethernet 103/1/3
  no shutdown
exit
```

Step 3: Add the vfc interface to the VSAN database.

- In this example, on the first Nexus 5500UP switch, the vfc is mapped to VSAN 4.
  ```
  vsan database
  vsan 4 interface vfc 1
  exit
  ```
- On the second Nexus 5500UP switch the vfc is mapped to VSAN 5.
  ```
  vsan database
  vsan 5 interface vfc 1
  exit
  ```

Step 4: Configure the Ethernet interface to operate in trunk mode, configure the interface with the FCoE VSAN and any data VLANs required by the host, and configure the spanning-tree port type as trunk edge.

- This example shows the configuration of the first Nexus 5500UP switch.
  ```
  interface Ethernet 103/1/3
  switchport mode trunk
  switchport trunk allowed vlan 148,304
  spanning-tree port type edge trunk
  no shut
  ```
- This example shows the configuration of the second Nexus 5500UP switch.
  ```
  interface Ethernet 103/1/3
  switchport mode trunk
  switchport trunk allowed vlan 148,305
  spanning-tree port type edge trunk
  no shut
  ```

Step 5: Configure VSAN on a C-Series server.

The C-Series server using the Cisco P81E CNA must have the FCoE VSANs configured for virtual host bus adapter (vHBA) operation to connect to the Fibre Channel fabric. For more information on configuring the C-Series server for FCoE connectivity, please see the Cisco SBA for Midsize Organizations—Data Center Unified Computing System Deployment Guide.

**Tech Tip**

**Procedure 3** Verify FCoE connectivity

Step 1: On the Cisco Nexus 5500UP switches, use the `show interface` command to verify the status of the virtual Fibre Channel interface. The interface should now be up as seen below if the host is properly configured to support the CNA.

**Reader Tip**

Host configuration is beyond the scope of this guide. Please see CNA documentation for specific host drivers and configurations.
Step 2: On the Cisco Nexus 5500UP switches, display the FCoE addresses.

dc5548ax# show fcoe database

<table>
<thead>
<tr>
<th>INTERFACE</th>
<th>FCID</th>
<th>PORT NAME</th>
<th>MAC ADDRESS</th>
</tr>
</thead>
<tbody>
<tr>
<td>vfc1</td>
<td>0xbc0000</td>
<td>20:00:58:8d:09:0e:e0:d2</td>
<td>58:8d:09:0e:e0:d2</td>
</tr>
</tbody>
</table>

Step 3: Show flogi database for FCoE login. The vfc1 addresses appear in the current Fiber Channel login database on the Nexus 5500 switch.

dc5548ax# show flogi database

<table>
<thead>
<tr>
<th>INTERFACE</th>
<th>VSAN</th>
<th>FCID</th>
<th>PORT NAME</th>
<th>NODE NAME</th>
</tr>
</thead>
<tbody>
<tr>
<td>vfc1</td>
<td>4</td>
<td>0xbc0000</td>
<td>20:00:58:8d:09:0e:e0:d2</td>
<td>10:00:58:8d:09:0e:e0:d2</td>
</tr>
</tbody>
</table>

Step 4: Show fcns database for FCoE login. The Fiber Channel name server database shows the FCoE host logged in and the FC-4 TYPE:FEATURE information.

dc5548ax# show fcns database

VSAN 4:

<table>
<thead>
<tr>
<th>FCID</th>
<th>TYPE</th>
<th>PWWN</th>
<th>(VENDOR)</th>
<th>FC4-TYPE:FEATURE</th>
</tr>
</thead>
<tbody>
<tr>
<td>0xbc0000</td>
<td>N</td>
<td>20:00:58:8d:09:0e:e0:d2</td>
<td>scsi-fcp:init fc-gs</td>
<td></td>
</tr>
</tbody>
</table>

Now you can configure zoning and device aliases per the previous Fibre Channel configuration section.

Tech Tip

Much of the configuration of the Cisco Nexus 5500UP Series switch can also be done from within Device Manager; however, Device Manager for SAN Essentials cannot be used to configure VLANs or Ethernet Trunks on the Cisco Nexus 5500UP Series switches.
Business Overview

As a midsize organization grows, the number and type of servers required to handle the information processing tasks of the organization grows as well. This imposes several challenges:

- Increased data center square footage and rack space.
- More power and cooling, particularly in light of the fact that every new CPU generation increases wattage dissipation as core speeds increase.
- Increased complexity of data-networking cable plant to provide adequate capacity and capability for increasing server counts.
- More hardware capital expense to buy server platforms and spares, and greater operational expense to administer and maintain diverse hardware and OS platforms.
- Migration from existing servers and applications to newer platforms and connection methods requires a flexible architecture that accommodates both legacy and new servers and applications.
- Increased resilience and migration-path challenges, as appliance-centric or server-centric application platforms tend to be platform-centric and may not lend themselves well to being load-balanced or moved to disparate platforms.

Organizations frequently need to optimize the use of the investment in server resources, so that the organization can add new applications while controlling costs as they move from a small server room environment into a midsized data center.

Scaling a data center with conventional servers, networking equipment, and storage resources can pose a significant challenge to a growing organization. Multiple hardware platforms and technologies must be integrated to deliver the expected levels of performance and availability to application end users. These components in the data center also need to be managed and maintained, typically with a diverse set of management tools with different interfaces and approaches.

Technology Overview

Server virtualization offers the capability to run multiple application servers on a common hardware platform, allowing an organization to focus on maximizing the application capability of the data center while minimizing costs. Increased capability and reduced costs are realized through multiple aspects:

- Multiple applications can be combined in a single hardware chassis, reducing the number of boxes that must be accommodated in data-center space.
- Simplified cable management, due to fewer required cable runs and greater flexibility in allocating network connectivity to hosts on an as-needed basis.
- Improved resilience and application portability as hypervisors allow workload resilience and load-sharing across multiple platforms, even in geographically dispersed locations.
- Applications that are deployed on standardized hardware platforms, which reduces platform-management consoles and minimizes hardware spare stock challenges.
- Minimized box count reduces power and cooling requirements, as there are fewer lightly-loaded boxes idling away expensive wattage.

The ability to virtualize server platforms to handle multiple operating systems and applications with Hypervisor technologies building virtual machines (VMs) allows the organization to lower capital and operating costs by collapsing more applications onto fewer physical servers. The Hypervisor technology also provides the ability to cluster many virtual machines into a domain where workloads can be orchestrated to move around the data center to provide resiliency and load balancing, and to allow new applications to be deployed in hours versus days or weeks.

The ability to move VMs or application loads from one server to the next, whether the server is a blade server in a chassis-based system or a stand-alone rackmount server, requires the network to be flexible and scalable, allowing any VLAN to appear anywhere in the data center. Cisco Virtual Port Channel and Fabric Extender technologies are used extensively in the Cisco SBA midsized data center architecture to provide flexible Ethernet connectivity to VLANs distributed across the data center in a scalable and resilient manner.
Streamlining the management of server hardware and its interaction with networking and storage equipment is another important component of using this investment in an efficient manner. Cisco offers a simplified reference model for managing a small server room as it grows into a full-fledged data center. This model benefits from the ease of use offered by the Cisco Unified Computing System (UCS). Cisco UCS provides a single graphical management tool for the provisioning and management of servers, network interfaces, storage interfaces, and their immediately attached network components. Cisco UCS treats all of these components as a cohesive system, which simplifies these complex interactions and allows a midsize organization to deploy the same efficient technologies as larger enterprises, without a dramatic learning curve.

The primary computing platforms targeted for the Cisco SBA Unified Computing reference architecture are Cisco UCS B-Series Blade Servers and Cisco UCS C-Series Rack-Mount Servers. The Cisco UCS Manager graphical interface provides ease of use that is consistent with the goals of the Cisco Smart Business Architecture. When deployed in conjunction with the Cisco SBA data center network foundation, the environment provides the flexibility to support the concurrent use of the Cisco UCS B-Series Blade Servers, Cisco UCS C-Series Rack-Mount Servers, and third-party servers connected to 1 and 10-Gigabit Ethernet connections.

Prior to connecting servers to the data center network, an explanation of some of the features like Cisco Nexus Virtual Port Channel and Cisco Nexus Fabric Extender which enhance connectivity options is in order.

**Cisco Nexus Virtual Port Channel**

As described in the Ethernet Infrastructure module, Virtual Port Channel (vPC) allows links that are physically connected to two different Cisco Nexus switches to appear to a third downstream device to be coming from a single device and as part of a single Ethernet Port Channel. The third device can be a server, switch, or any other device or appliance that supports IEEE 802.3ad Port Channels. For Cisco EtherChannel technology, the term “multichassis EtherChannel” (MCEC) refers to this technology. MCEC links from a device connected to the data center core that provides spanning tree loop-free topologies allowing VLANs to be extended across the midsize data center while maintaining a resilient architecture.

vPCs consist of two vPC peer switches connected by a peer link. Of the vPC peers, one is primary and one is secondary. The system formed by the switches is referred to as a vPC domain. The vPC peer link between the two Cisco Nexus switches is the most important connectivity element in the system. This link is used to create the illusion of a single control plane between the two switches, and carries critical control plane packets as well as data packets when devices are single homed due to design or EtherChannel link failure. For a VLAN to be forwards on a vPC, that VLAN must exist on the peer link and both vPC peer switches.

The vPC peer-keepalive link is used to resolve dual-active scenarios in which the peer link connectivity is lost. If the vPC peer link connectivity is lost, the secondary vPC peer will shut down all vPC member links, and the primary vPC switch will continue forwarding packets providing a resilient architecture.

A vPC port is a port that is assigned to a vPC channel group. The ports that form the virtual port channel are split between the vPC peers, must be defined identically on both vPC switches, and are referred to as vPC member ports. A non-vPC port, also known as an orphaned port, is a port that belongs to a VLAN that is part of a vPC, but is not programmed as a vPC member. The following figure illustrates vPC ports and orphan ports:

**Figure 13 - vPC member and non-member ports**
The important point to remember about vPC orphan ports is that if the vPC peer link is lost and the secondary vPC shuts down vPC ports, it will not shut down vPC orphan ports unless programmed to do so with the vpc orphan-port suspend command on the switch interface.

Example

```
interface Ethernet103/1/2
description to_teamed_adapter
switchport mode access
switchport access vlan 50
vpc orphan-port suspend

interface Ethernet104/1/2
description to_teamed_adapter
switchport mode access
switchport access vlan 50
vpc orphan-port suspend
```

Reader Tip

The fundamental concepts of vPC are described in detail in the whitepaper titled “Cisco NX-OS Virtual PortChannel: Fundamental Design Concepts with NXOS 5.0” on www.cisco.com.

Cisco Nexus Fabric Extender

As described earlier in the Ethernet Infrastructure module of this document, the Cisco Fabric Extender (FEX) acts as a remote line card to the attached Cisco Nexus 5500UP switch that it is connected to. This allows for central configuration of all switch ports on the data center core switches, and provides fan out to higher density Fast Ethernet, Gigabit Ethernet, and 10-Gigabit Ethernet for top of rack server connectivity. Because the Cisco FEX acts as a line card on the Cisco Nexus 5500UP switch, extending VLANs to server ports on different Cisco FEXs does not create spanning tree loops across the data center.

The Cisco FEX can be single-homed to a data center core switch (also called straight-through mode) or dual-homed using vPC (also called Active/Active mode).

Figure 14 - Cisco Nexus FEX connectivity to data center core

The dual-homed (Active/Active) Cisco FEX uses vPC to provide resilient connectivity to both data center core switches for single attached host servers. Each host is considered vPC connected through the associated connectivity to a vPC dual-homed Cisco FEX. The Cisco FEX to core connectivity ranges from 4-8 uplinks depending on the Cisco FEX type in use, and the Cisco FEX uplinks can be configured as a port channel as well.
The host connected to a pair of single-homed Cisco FEXs can be configured for port channel operation to provide resilient connectivity to both data center core switches through the connection to each Cisco FEX. The Cisco FEX to core connectivity ranges from 4-8 uplinks depending on the Cisco FEX type in use, and the Cisco FEX uplinks are typically configured as a port channel as well.

**Tech Tip**

Devices such as LAN switches that generate spanning tree BPDUs should not be connected to Cisco FEXs. The Cisco FEX is designed for host connectivity and will error disable a port that receives a BPDU packet.

The complete Cisco FEX connectivity programming to the Cisco Nexus 5500UP data center core switches and Ethernet port configuration for server connection is detailed in the Ethernet Infrastructure module of this document.

**Cisco UCS System Network Connectivity**

Both Cisco UCS B-Series Blade Servers and C-Series Rack Mount Servers integrate cleanly into the Cisco SBA Midsize Data Center Architecture. The Cisco Nexus 5500UP data center core provides 1-Gigabit Ethernet, 10-Gigabit Ethernet, and Fibre Channel SAN connectivity in a single platform.

**Cisco UCS B-Series Blade Chassis System Components**

The Cisco UCS Blade Chassis system has a unique architecture that integrates compute, data network access, and storage network access into a common set of components under a single-pane-of-glass management interface. The primary components included within this architecture are as follows:

- **Cisco UCS 6100 Series Fabric Interconnects**—Provide both network connectivity and management capabilities to the other components in the system.
- **Cisco UCS 2100 Series Fabric Extenders**—Logically extend the fabric from the fabric interconnects into each of the enclosures for Ethernet, FCoE, and management purposes.

- **Cisco UCS 5100 Series Blade Server Chassis**—Provides an enclosure to house up to eight half-width or four full-width blade servers, their associated fabric extenders, and four power supplies for system resiliency.
- **Cisco UCS B-Series Blade Servers**—Available in half-width or full-width form factors, with a variety of high-performance processors and memory architectures to allow customers to easily customize their compute resources to the specific needs of their most critical applications.
- **Cisco UCS B-Series Network Adapters**—A variety of mezzanine adapter cards that allow the switching fabric to provide multiple interfaces to a server.

The following figure shows an example of the physical connections required within a UCS Blade Chassis system to establish the connection between the fabric interconnects and a single blade chassis. The links between the blade chassis and the fabric interconnects carry all server data traffic, centralized storage traffic, and management traffic generated by Cisco UCS Manager.

**Figure 15 - Cisco UCS Blade System component connections**

Cisco UCS Manager

Cisco UCS Manager is embedded software resident on the fabric interconnects, providing complete configuration and management capabilities for all of the components in the UCS system. This configuration information is replicated between the two fabric interconnects, providing a highly available solution for this critical function. The most common way to access Cisco UCS Manager for simple tasks is to use a web browser to open the Java-based GUI. For command-line or programmatic operations against the system, a CLI and an XML API are also included with the system.
Cisco UCS B-Series System Network Connectivity

The Cisco UCS 6100 Series Fabric Interconnects provide connectivity for Cisco UCS Blade Server systems. The following figure shows a detailed example of the connections between the fabric interconnects and the Cisco Nexus 5500UP Series data center core.

The default and recommended configuration for the fabric interconnects is end-host mode, which means they do not operate as full LAN switches, and rely on the upstream data center switching fabric. In this way, the Cisco UCS system appears to the network as a virtualized compute cluster with multiple physical connections. Individual server traffic is pinned to specific interfaces, with failover capability in the event of loss of the primary link. The Ethernet traffic from the fabric interconnects shown in Figure 16 uses vPC links to the data center core for resilience and traffic load sharing. The Fibre Channel links to the core use SAN port channels for load sharing and resilience as well.

*Figure 16 - UCS fabric interconnect to core*

---

Cisco UCS C-Series Network Connectivity


The Cisco Nexus switching fabric provides connectivity for 10-Gigabit or 1-Gigabit Ethernet attachment for Cisco UCS C-Series servers, depending on the throughput requirements of the applications or virtual machines in use and the number of network interface cards installed per server. Figure 17 shows some examples of dual-homed connections from Cisco UCS C-Series servers to single-homed Cisco FEXs providing 10-Gigabit and 10-Gigabit Ethernet connections. 10-Gigabit Ethernet connections capable of supporting Ethernet and FCoE are available either through the Cisco Nexus 2232PP Fabric Extender or by using 10-Gigabit ports directly on the Cisco Nexus 5500UP Series switch pair. Connections for Fast Ethernet or 1-Gigabit Ethernet can also use the Cisco Nexus 2248TP Fabric Extender.

*Figure 17 - Example Cisco UCS C-Series FEX Connections*
The Cisco UCS C-Series Server connectivity to Cisco FEX options in Figure 17 above all make use of vPC connections by using IEEE 802.3ad EtherChannel from the host to single-homed Cisco Nexus 2232PP FEXs. When using vPC for server connections, each server interface must be identically configured on each data center core Cisco Nexus 5500UP switch. The Cisco FEX to data center core uplinks use a port channel to load balance server connections over multiple links and provide added resilience.

The Cisco UCS C-Series Server with 10-Gigabit Ethernet and FCoE connectivity uses a converged network adapter (CNA) in the server and must connect to either a Cisco Nexus 2232PP FEX or directly to the Cisco Nexus 5500UP switch just as FCoE uplinks must use a fiber optic or twinax connection to maintain bit error rate (BER) thresholds for Fibre Channel transport. Cisco supports FCoE on 10-Gigabit Ethernet only at this time. If used with vPC, the Ethernet traffic is load balanced across the server links with EtherChannel and Fibre Channel runs up each link to the core, with SAN-A traffic on one link to the connected Cisco FEX and data center core switch, and SAN-B traffic on the other link to the connected Cisco FEX and data center core switch, as is typical of Fibre Channel SAN traffic.

The Cisco UCS C-Series Server with 10-Gigabit Ethernet without FCoE can connect to a Cisco Nexus 2232 FEX or directly to the Cisco Nexus 5500UP switch. These server connections can be fiber optic, copper, or twinax depending on the Cisco FEX and server combination used. If used with vPC, the Ethernet traffic is load balanced across the server links with EtherChannel.

The Cisco UCS C-Series Server with multiple 1-Gigabit Ethernet uses vPC to load balance traffic over multiple links using EtherChannel. The use of vPC is not a requirement. In a non-vPC server connection where independent server interfaces are desired, connecting to a dual-homed Cisco FEX may be preferable for resilience unless the server operating system provides resilient connectivity.

Detailed configuration for the Cisco Nexus FEX to Cisco Nexus 5500UP switch connections can be found in the Ethernet Infrastructure module earlier in this guide. Detailed configuration for Cisco UCS C-Series deployment can be found in the Cisco SBA for Midsize Organizations—Data Center Unified Computing System Deployment Guide.

---

**Single-Homed Server Connectivity**

As an organization grows many legacy servers and appliances with a single Fast Ethernet or Gigabit Ethernet may need connectivity in the data center. To provide added resilience for these servers, a dual-homed Cisco FEX using vPC for the Cisco FEX connection to the data center is recommended as shown in the figure below.

**Figure 18 - Single-homed server to dual-homed Cisco FEX**

The vPC connection from the Cisco Nexus 2248TP FEX provides both control plane and data plane redundancy for servers connected to the same Cisco FEX. This topology provides resiliency for the attached servers in the event of a fabric uplink or Nexus 5500UP core switch failure, however there is no resilience in the event of a Nexus 2248TP failure. All servers connected to the vPC dual-homed Cisco FEX are vPC connections and must be configured on each data center core Nexus 5500UP switch. While this approach does provide added resiliency, single-homed servers hosting important applications should be migrated to dual-homed connectivity to provide sufficient resilience.
Server with Teamed Interface Connectivity

Server network interface card (NIC teaming) comes in many options and features. NIC adapters and operating systems capable of using IEEE 802.3ad EtherChannel from servers to a Cisco FEX would use the vPC option covered in the UCS C-Series connectivity section. NIC adapters and operating systems using an active/standby method for connecting to the Cisco FEX are best served by a dual-homed Cisco FEX as shown in the figure below.

Figure 19 - Server with active/standby NIC to Cisco FEX connection

The vPC connection from the Cisco Nexus 2248TP FEX provides both control plane and data plane redundancy for servers connected to each Cisco FEX. This topology provides resiliency for the attached servers in the event of a fabric uplink or Nexus 5500UP core switch failure. In the event of a Cisco FEX failure, the NIC teaming would switch to the standby interfaces.

Third-Party Blade Server System Connectivity

Blade server systems are available from manufacturers other than Cisco. In the event you have a non-Cisco blade server system to connect to your data center there are multiple options for connecting to your Cisco SBA midsize data center architecture.

The first option is using a blade server system with a pass-through module that extends server interfaces directly out of the blade server chassis without using an internal switch fabric in the blade server system. When using pass-through modules, the server NIC connections can use the Cisco Nexus Fabric Extender for high-density port fan out and resilient connections as shown in the figure below.

Figure 20 - Third-party blade server system with pass-through module
A second option for connecting a non-Cisco blade server system to the Cisco SBA midsize data center architecture involves a blade server system that has an integrated Ethernet switch. In this scenario the integrated switch in the blade server chassis would generate spanning tree BPDUs and therefore cannot be connected to fabric extenders. Another consideration is that a blade server with an integrated switch generally uses a few high speed 10-Gigabit Ethernet uplinks where direct connection to the Cisco Nexus 5500UP switch core, as shown in Figure 21, is recommended.

*Figure 21 - Third party blade server system with integrated switch*

**Summary**

The compute connectivity options outlined in this section show how the Cisco SBA midsize data center foundation architecture integrates with the Cisco Unified Computing System to build a flexible and scalable compute connectivity. The data center architecture also provides support for resilient non-Cisco server and blade system connectivity. For further detail on deploying the Cisco UCS Server systems, please refer to the *Cisco SBA for Midsize Organizations—Data Center Unified Computing System Deployment Guide.*
**Business Overview**

In today’s business environment, the data center contains some of the organization’s most valuable assets. Customer and personnel records, financial data, email stores, and intellectual property must be maintained in a secure environment to assure confidentiality and availability. Additionally, portions of networks in specific business sectors may be subject to industry or government regulations that mandate specific security controls to protect customer or client information.

To protect the valuable electronic assets located in the data center, network security ensures the facility is protected from automated or human-operated snooping and tampering, and it prevents compromise of hosts by resource-consuming worms, viruses, or botnets.

While worms, viruses, and botnets pose a substantial threat to centralized data, particularly from the perspective of host performance and availability, servers must also be protected from employee snooping and unauthorized access. Statistics have consistently shown that the majority of data loss and network disruptions have occurred as the result of human-initiated activity (intentional or accidental) carried out within the boundaries of the business’s network.

**Technology Overview**

To minimize the impact of unwanted network intrusions, firewalls and intrusion prevention systems (IPSs) should be deployed between clients and centralized data resources.

*Figure 22 - Deploy firewall inline to protect data resources*

Because everything else outside the protected VLANs hosting the data center resources can be a threat, the security policy associated with protecting those resources has to include the following potential threat vectors.

Data center threat landscape:

- Internet
- Remote access and teleworker VPN hosts
- Remote office/branch networks
- Business partner connections
- Campus networks
- Unprotected data center networks
- Other protected data center networks

The data center security design employs a pair of Cisco Adaptive Security Appliance (ASA) 5585-X with SSP-20 firewall modules and matching IPS Security Service Processors (SSP) installed. This configuration provides up to 10 Gbps of firewall throughput. The IPS and firewall SSPs deliver 3 Gbps of concurrent throughput.
All of the ports on modules installed in the Cisco ASA chassis are available to the firewall SSP, which offers a very flexible configuration. The Cisco ASA firewalls are dual-homed to the data center core Nexus 5500UP switches using two 10Gigabit Ethernet links for resiliency. The pair of links on each Cisco ASA is configured as an EtherChannel, which provides load balancing as well as rapid and transparent failure recovery. The Cisco NX-OS Virtual Port Channel (vPC) feature on the Nexus 5500UP data core switches allow the firewall EtherChannel to span the two data center core switches (Multi-Chassis EtherChannel) but appear to be connected to a single upstream switch. This EtherChannel link is configured as a VLAN trunk in order to support access to multiple secure VLANs in the data center. One VLAN on the data center core acts as the outside VLAN for the firewall and any hosts or servers that reside in that VLAN are outside the firewall and therefore receive no protection from the Cisco ASA for attacks originating from anywhere else in the organization’s network. Other VLANs on the EtherChannel trunk will be designated as being firewall from all the other data center threat vectors or firewall with additional IPS services.

The pair of Cisco ASAs is configured for firewall active-standby high availability operation to ensure that access to the data center is minimally impacted by outages caused by software maintenance or hardware failure. When Cisco ASA appliances are configured in active-standby mode, the standby appliance does not handle traffic, so the primary device must be sized to provide enough throughput to address connectivity requirements between the core and the data center. While the IPS modules do not actively exchange state traffic, they participate in the firewall appliances’ active/standby status by way of reporting their status to the firewall’s status monitor. A firewall failover will occur if either the Cisco ASA itself has an issue or the IPS module becomes unavailable.

The Cisco ASAs are configured in routing mode; as a result, the secure network must be in a separate subnet from the client subnets. IP subnet allocation would be simplified if the Cisco ASA were deployed in transparent mode; however, hosts might inadvertently be connected to the wrong VLAN, where they would still be able to communicate with the network, incurring an unwanted security exposure.

The data center IPSs monitor for and mitigate potential malicious activity that is contained within traffic allowed by the security policy defined on the Cisco ASAs. The IPS sensors can be deployed in promiscuous intrusion detection system (IDS) mode so that they only monitor and alert for abnormal traffic. The IPS modules can be deployed inline in IPS mode to fully engage their intrusion prevention capabilities, wherein they will block malicious traffic before it reaches its destination. The choice to have the sensor drop traffic or not is one that is influenced by several factors: risk tolerance for having a security incidence, risk aversion for inadvertently dropping valid traffic, and other possibly externally driven reasons like compliance requirements for IPS. The ability to run in IDS mode or IPS is highly configurable to allow the maximum flexibility in meeting a specific security policy.

**Security Topology Design**

The Cisco SBA secure data center design provides two secure VLANs in the data center. The number of secure VLANs is arbitrary; the design is an example of how to create multiple secured networks to host services that require separation. High-value applications, such as Enterprise Resource Planning and Customer Relationship Management, may need to be separated from other applications in their own VLAN.

*Figure 23 - Example design with secure VLANs*

As another example, services that are indirectly exposed to the Internet (via a web server or other application servers in the Internet demilitarized zone) should be separated from other services, if possible, to prevent Internet-borne compromise of some servers from spreading to other services that are not exposed. Traffic between VLANs should be kept to a minimum, unless your security policy dictates service separation. Keeping traffic between servers intra-VLAN will improve performance and reduce load on network devices.

For this deployment, open VLANs without any security policy applied are configured physically and logically on the data center core switches. For devices that need an access policy, they will be deployed on a VLAN behind the firewalls. Devices that require both an access policy and IPS traffic inspection will be deployed on a different VLAN that exists logically behind
the Cisco ASAs. Because the Cisco ASAs are physically attached only to the data center core Nexus switches, these protected VLANs will also exist at Layer 2 on the data center core switches. All protected VLANs are logically connected via Layer 3 to the rest of the network through the Cisco ASA and therefore reachable only by traversing the Cisco ASA.

**Security Policy Development**

A business should have an IT security policy as a starting point in defining its firewall policy. If there is no companywide security policy, it will be very difficult to define an effective policy for the business while maintaining a secure computing environment.

To effectively deploy security between the various functional segments of a business’s network, you should seek the highest level of detail possible regarding the expected network behaviors. If you have greater detail of the expectations, you will be better positioned to define a security policy that enables a business’s application traffic and performance requirements while optimizing security.

A detailed examination of regulatory compliance considerations exceeds the scope of this document; you should include industry regulation in your network security design. Noncompliance may result in regulatory penalties such as fines or business-activity suspension.

Network security policies can be broken down into two basic categories: “whitelist” policies and “blacklist” policies. A whitelist security policy offers a higher implicit security posture, blocking all traffic except that which must be allowed (at a sufficiently granular level) to enable applications. Whitelist policies are generally better positioned to meet regulatory requirements because only traffic that must be allowed to conduct business is allowed. Other traffic is blocked and does not need to be monitored to assure that unwanted activity is not occurring. This reduces the volume of data that will be forwarded to an IDS or IPS, and also minimizes the number of log entries that must be reviewed in the event of an intrusion or data loss.

Inversely, a blacklist policy only denies traffic that specifically poses the greatest risk to centralized data resources. A blacklist policy is simpler to maintain and less likely to interfere with network applications. A whitelist policy is the best-practice option if you have the opportunity to examine the network’s requirements and adjust the policy to avoid interfering with desired network activity.
Cisco ASA Firewalls implicitly end access lists with a deny-all rule. Blacklist policies include an explicit rule, prior to the implicit deny-all rule, to allow any traffic that is not explicitly allowed or denied.

Whether you choose a whitelist or blacklist policy basis, consider IDS or IPS deployment for controlling malicious activity on otherwise trustworthy application traffic. At a minimum, IDS or IPS can aid with forensics to determine the origin of a data breach. Ideally, IPS can detect and prevent attacks as they occur and provide detailed information to track the malicious activity to its source. IDS or IPS may also be required by the regulatory oversight to which a network is subject (for example, PCI 2.0).

A blacklist policy that blocks high-risk traffic offers a lower-impact but less-secure option (compared to a whitelist policy) in cases where a detailed study of the network’s application activity is impractical, or if the network availability requirements prohibit application troubleshooting. If identifying all of the application requirements is not practical, you can apply a blacklist policy with logging enabled, so that a detailed history of the policy is generated. With network-behavior details in hand, development of a whitelist policy is much easier and more effective.
Deployment Details

Data center security deployment is addressed in three discrete processes:

- Cisco ASA Firewall connectivity, which establishes network connections between the Cisco ASA Firewalls and the Cisco Nexus 5500UP data center core.
- Cisco ASA Firewall policy discussion and configuration, which outlines the process needed to identify security policy needs and apply a configuration to meet requirements.
- Cisco IPS connectivity and policy configuration, which integrates connectivity and policy configuration in one process.

Process

Configuring Cisco ASA Firewall Connectivity

1. Configure port channels on Nexus 5500s
2. Initial ASA configuration
3. Configure firewall connectivity
4. Configure routing
5. Configure Cisco ASAs for high availability

Complete the following procedures to configure connectivity between the Cisco ASA chassis and the core. Note that this design describes a configuration wherein the Cisco ASAs are connected to the Nexus 5500UP data center core switches by using a pair of 10-gigabit Ethernet interfaces in an EtherChannel. The Cisco ASA will connect between the data center core routed interface and the protected VLANs that also reside on the switches.

Procedure 1

The Cisco ASA firewalls protecting applications and servers in the data center will be dual-homed to each of the data center core Cisco Nexus 5500UP switches by using EtherChannel links.

Dual-homed or multi-chassis EtherChannel connectivity to the Cisco Nexus 5500UP switches uses vPCs, which allow a Cisco ASA to connect to both of the data center core switches with a single logical EtherChannel.
Step 1: Configure the physical interfaces that will make up the port channels on the two Cisco Nexus 5500UP data center core switches.

- Configure the first Cisco Nexus 5500UP switch.
  ```
  interface Ethernet1/1
  description DC5585a Ten0/8
  channel-group 53 mode active
  ```

  ```
  interface Ethernet1/2
  description DC5585b Ten0/8
  channel-group 54 mode active
  ```

- Configure the second Cisco Nexus 5500UP switch.
  ```
  interface Ethernet1/1
  description DC5585a Ten0/9
  channel-group 53 mode active
  ```

  ```
  interface Ethernet1/2
  description DC5585b Ten0/9
  channel-group 54 mode active
  ```

When you assign the channel group to a physical interface, it creates the logical EtherChannel (port-channel) interface that will be configured in the next step.

Step 2: Configure the logical port-channel interfaces for both data center core switches. The physical interfaces tied to the port-channel will inherit the settings from the logical port-channel interface.

```
interface port-channel53
  switchport mode trunk
  switchport trunk allowed vlan 153-155
  vpc 53
```

```
interface port-channel54
  switchport mode trunk
  switchport trunk allowed vlan 153-155
  vpc 54
```

The port channels are created as vPC port channels since the fabric interfaces are dual-homed EtherChannels to both Nexus 5500UP data center core switches.

---

**Procedure 2**  
**Initial ASA configuration**

Connect to the console of the Cisco ASA firewall and perform the following global configuration.

Step 1: Configure the Cisco ASA hostname to make it easy to identify.
  ```
  hostname DC5585ax
  ```

Step 2: Disable the dedicated management port. This design does not use the dedicated management port.
  ```
  interface Management0/0
  shutdown
  ```

Step 3: Configure local user authentication.
  ```
  Username [username] password [password]
  ```

Step 4: Configure enable password.
  ```
  enable password [password]
  ```

Step 5: Configure domain name.
  ```
  domain-name cisco.local
  ```

Step 6: Configure management access.
  ```
  http server enable
  http 10.0.0.0 255.0.0.0 outside
  ```

Step 7: Configure a Network Time Protocol (NTP) server address. NTP is designed to synchronize time across all devices in a network, for troubleshooting.
  ```
  ntp server 10.10.48.17
  ```
Procedure 3 Configure firewall connectivity

Two 10-gigabit Ethernet links connect each Cisco ASA chassis to the two core Cisco Nexus switches. The two interfaces are paired in a port channel group. Subinterfaces are created on the port channel for the outside VLAN 153 and all the protected VLANs inside (154 and 155). Each interface created will be assigned the correct VLAN, an appropriate name, a security level, and an IP address and netmask.

All interfaces on Cisco ASA have a security-level setting. The higher the number, the more trusted the interface, relative to other interfaces. The inside interface is, by default, assigned 100, the highest security level. The outside interface is assigned 0. By default, traffic can pass from a high-security interface to a lower-security interface. In other words, traffic from an inside network is permitted to an outside network, but not conversely.

**Step 1:** Configure the port channel group by using the two 10-Gigabit Ethernet interfaces.
```
interface Port-channel10
  description ECLB Trunk to 5548 Switches
  no shutdown
!
interface TenGigabitEthernet0/8
  description Trunk to DC5548x TenGigx/x
  channel-group 10 mode passive
  no shutdown
!
interface TenGigabitEthernet0/9
  description Trunk to DC5548x TenGigx/x
  channel-group 10 mode passive
  no shutdown
```

**Step 2:** Configure the subinterfaces for the 3 VLANs: outside VLAN 153, inside the firewall VLAN 154, and inside the firewall with IPS VLAN 155.
```
interface Port-channel10.153
  description DC VLAN Outside the FW
  vlan 153
  nameif outside
  security-level 0
  ip address 10.10.53.126 255.255.255.128 standby 10.10.53.125
  no shutdown
!
interface Port-channel10.154
  description DC VLAN Inside the Firewall
  vlan 154
  nameif DC-InsideFW
  security-level 75
  ip address 10.10.54.1 255.255.255.0 standby 10.10.54.2
  no shutdown
!```
**Procedure 4**  Configure routing

Because the Cisco ASAs are the gateway to the secure VLANs in the server room, the Cisco ASA pair is configured to use a static route to the HSRP address of the Nexus switches on outside VLAN 153.

Static routes also need to be configured on the data center core Cisco Nexus 5500s to route traffic destined to the secure VLANs to the Cisco ASA. These routes also need to be injected into EIGRP to allow them to propagate through the network.

**Step 1:** Configure the static route pointing to the data center core HSRP address on the Cisco ASA pair.

```
route outside 0.0.0.0 0.0.0.0 10.10.53.1 1
```

**Step 2:** On the data center core Nexus 5500s, configure the static routes pointing to the secure subnets behind the firewalls, and redistribute the subnets into the EIGRP routing process.

```
route-map static-to-eigrp permit 10
  match ip address 10.10.54.0/24
route-map static-to-eigrp permit 20
  match ip address 10.10.55.0/24
router eigrp 1
  redistribute static route-map static-to-eigrp
ip route 10.10.54.0/24 Vlan153 10.10.53.126
ip route 10.10.55.0/24 Vlan153 10.10.53.126
```

**Procedure 5** Configure Cisco ASAs for high availability

The Cisco ASA firewalls are configured for active-standby high availability.

**Step 1:** Define the primary firewall’s failover configuration. The two lines of the configuration that begin with ‘failover polltime’ reduce the failover timers from the defaults in order to achieve sub-second failover. Improved failover times reduce application and user impact during outages. Reducing the failover timer intervals below these values is not recommended:

```
interface GigabitEthernet0/1
  description LAN/STATE Failover Interface
  no shutdown
!
failover
failover lan unit primary
failover lan interface failover GigabitEthernet0/1
failover polltime unit msec 200 holdtime msec 800
failover polltime interface msec 500 holdtime 5
failover key [key]
failover replication http
failover link failover GigabitEthernet0/1
failover interface ip failover 10.10.53.130 255.255.255.252
standby 10.10.53.129
```
Step 2: Define the secondary firewall’s failover configuration. The failover key value must match on the two devices that are configured in the active-standby high availability pair. Note that this is not the configuration that exists on the device but instead the configuration that is applied to an unconfigured Cisco ASA to make it the failover secondary device of the pair.

```network
interface GigabitEthernet0/1
  no shutdown
!
failover
failover lan unit secondary
failover lan interface failover GigabitEthernet0/1
failover polltime unit msec 200 holdtime msec 800
failover polltime interface msec 500 holdtime 5
failover key [key]
failover replication http
failover link failover GigabitEthernet0/1
failover interface ip failover 10.10.53.130 255.255.255.252
  standby 10.10.53.129
```

Step 3: Add the configuration so that the active firewall will defer to the standby firewall if connectivity is lost on the DC VLANs.

```network
monitor-interface outside
monitor-interface DC-InsideFW
monitor-interface DC-InsideIPS
```

**Process**

**Evaluating and Deploying Firewall Security Policy**

1. Evaluate security policy requirements
2. Deploy the appropriate security policy

This section describes the steps required to evaluate which type of policy fits an organization’s data center security requirements and provides the procedures necessary to apply these policies.

**Procedure 1**

**Evaluate security policy requirements**

Step 1: Evaluate security policy requirements by answering the following questions.

- What applications will be served from the secure data center?
- Can the applications’ traffic be characterized at the protocol level?
- Is a detailed description of application behavior available to facilitate troubleshooting if the security policy interferes with the application?
- What is the network’s baseline performance expectation between the controlled and uncontrolled portions of the network?
- What is the peak level of throughput that security controls will be expected to handle, including bandwidth-intensive activity such as workstation backups or data transfers to a secondary data replication site?

Step 2: For each datacenter VLAN, determine which security policy enables application requirements. Each VLAN that requires firewall will need either a permissive (blacklist) or restrictive (whitelist) security policy.
**Procedure 2** Deploy the appropriate security policy

Network security policy configuration is fairly arbitrary to suit the policy and management requirements of an organization. Thus, examples here should be used as a basis for security policy configuration.

**Option 1. Deploy a whitelist security policy**

A basic whitelist data-service policy can be applied to allow common business services such as HTTP, HTTPS, DNS, and other services typically seen in Microsoft-based networks.

**Step 1:** Enter the following configuration to control access so only specific hosts may be accessed.

```plaintext
object network BladeWeb1Secure
host 10.10.54.100
object network BladeWeb2Secure
host 10.10.55.100
object network Secure-Subnets
 subnet 10.10.54.0 255.255.255.0
object network SecureIPS-Subnets
 subnet 10.10.55.0 255.255.255.0
object-group network Application-Servers
description HTTP, HTTPS, DNS, MSExchange
 network-object object BladeWeb1Secure
 network-object object BladeWeb2Secure
!
object-group service MS-App-Services
 service-object tcp destination eq domain
 service-object tcp destination eq www
 service-object tcp destination eq https
 service-object tcp destination eq netbios-ssn
 service-object udp destination eq domain
 service-object udp destination eq nameserver
 service-object udp destination eq netbios-dgm
 service-object udp destination eq netbios-ns
!
 access-list global_access extended permit object-group MS-App-Services any object-group Application-Servers
```

**Step 2:** You can specify which resources certain users (for example, IT management staff or network users) can use to access management resources. In this example, management hosts in the IP address range 10.10.48.224-255 are allowed SSH and SNMP access to Data Center subnets.

```plaintext
object network Mgmt-host-range
 range 10.10.48.224 10.10.48.254
object-group network DC_Secure_Subnet_List
 network-object object Secure-Subnets
 network-object object SecureIPS-Subnets
object-group service Mgmt-Traffic
 service-object tcp destination eq ssh
 service-object udp destination eq snmp
 access-list global_access extended permit object-group Mgmt-Traffic

Step 3: (Optional) A bypass rule allows wide-open access to hosts that are added to the appropriate network object group. The bypass rule must be carefully defined to avoid opening access to hosts or services that must otherwise be blocked. In a whitelist policy, the bypass rule is typically disabled, and it is only called into use whenever firewall policy troubleshooting is required to allow access to an application.

The following policy defines two hosts and applies them to the bypass rule

```plaintext
object-group network Bypass-Rule
description Open Policy for Server Access
 network-object object BladeWeb1Secure
 network-object object BladeWeb2Secure
 access-list global_access extended permit ip any object-group Bypass-Rule

This disables the Bypass rule:

```plaintext
access-list global_access extended permit ip any object-group Bypass-Rule inactive
```
The bypass rule group is useful for troubleshooting or providing temporary access to services on the host that must be opened for maintenance or service migration. It is typically disabled unless being used for troubleshooting.

**Tech Tip**

The bypass rule group is useful for troubleshooting or providing temporary access to services on the host that must be opened for maintenance or service migration. It is typically disabled unless being used for troubleshooting.

**Step 4:** Save your Cisco ASA firewall configuration.

```bash
copy running-config startup-config
```

**Option 2. Deploy a blacklist security policy**

If an organization does not have the desire or resources to maintain a granular, restrictive policy to control access between centralized data and the user community, a simpler, easy-to-deploy policy that limits only the highest-risk traffic may be more attractive. This policy is typically configured such that only specific services' access is blocked; all other access is handled by the bypass rule discussed in the previous section.

**Step 1:** Allow SNMP queries and SSH requests for a specific address range that will be allocated for IT staff. Network administrative users may need to issue SNMP queries from desktop computers to monitor network activity and SSH to connect to devices.

```plaintext
object network Mgmt-host-range
  range 10.10.48.224 10.10.48.254
object-group network DC_Secure_Subnet_List
  network-object object Secure-Subnets
  network-object object SecureIPS-Subnets
object-group service Mgmt-Traffic
  service-object tcp destination eq ssh
  service-object udp destination eq snmp

access-list global_access extended permit object-group Mgmt-Traffic
  object Mgmt-host-range object-group DC_Secure_Subnet_List
```

**Step 2:** Block Telnet, SSH and SNMP to all other hosts.

```plaintext
access-list global_access extended deny object-group Mgmt-Traffic any any
```

**Step 3:** Configure a bypass rule to allow any application traffic through that was not specifically denied. Note that logging is disabled on this policy to prevent the firewall from having to log all accesses to the server network.

```plaintext
access-list global_access extended permit ip any object-group Bypass-Rule log disable
```

**Step 4:** Save your Cisco ASA firewall configuration.

```bash
copy running-config startup-config
```

**Process**

Deploying Cisco Intrusion Protection System (IPS)

1. Apply initial configuration
2. Complete basic configuration
3. Configure signature updates

From a security standpoint, intrusion detection systems (IDS) and intrusion prevention systems (IPS) are complementary to firewalls because firewalls are generally access-control devices and are built to block access to an application or host. In this way, a firewall can be used to remove access to a large number of application ports, reducing the threat to the servers. IDS and IPS sensors watch network and application traffic that is permitted to go through the firewall looking for attacks. If it detects an attack, the IDS sensor generates an alert to inform the organization about the activity. IPS is similar in that it generates alerts due to malicious activity, and additionally, it can apply an action to block the attack before it reaches the destination.
Promiscuous versus Inline

There are two primary deployment modes when using IPS sensors: promiscuous (IDS) or inline (IPS). There are specific reasons for each deployment model based on risk tolerance and fault tolerance. In promiscuous mode (IDS), the sensor inspects copies of packets, which prevents it from being able to stop a malicious packet when it sees one.

An IDS sensor must utilize another inline enforcement device in order to stop malicious traffic. This means that for activity such as single-packet attacks (for example, slammer worm over user datagram protocol), an IDS sensor could not prevent the attack from occurring. However, an IDS sensor can offer great value when identifying and cleaning up infected hosts.

In an IPS deployment, because the packet flow is sent through the sensor and returned to the Cisco ASA, the sensor inspects the actual data packets. The advantage IPS mode offers is that when the sensor detects malicious behavior, the sensor can simply drop it. This allows the IPS device a much greater capacity to actually prevent attacks.

Use IDS when you do not want to impact the availability of the network or create latency issues. Use IPS when you need higher security than IDS and the ability to drop packets.

The secure data center design using a Cisco ASA 5585-X with IPS implements a policy for IPS, which sends all traffic to the IPS module inline. An organization may choose an IPS or IDS deployment, depending on regulatory and application requirements. It is very easy to start with an IDS or promiscuous design for initial deployment and then move to IPS once the traffic and performance profile of the network is known and you are comfortable that production traffic will not be affected.

Procedure 1  Apply initial configuration

Use the sensor’s command-line interface in order to set up basic networking information, specifically, the IP address, gateway address, and access lists that allow remote access. Once these critical pieces of data are entered, the rest of the configuration is accomplished by using IPS Device Manager (IDM), the embedded GUI console. Unlike the Cisco ASA firewalls used in the Cisco SBA design, IPS modules use an out-of-band management connection for configuration and monitoring. The sensor’s management port is connected to the data center management VLAN where the sensors can route to or directly reach the management station.

Step 1: Connect to the IPS Silicon Switch Processor (SSP) console through the serial console on the IPS SSP module on the front panel of the 5585.

Tech Tip

You can also gain access to the console on the IPS SSP by using the session 1 command from the Cisco ASA SSP’s CLI.

Step 2: Log in to the IPS device. The default username and password are both cisco. You will be prompted to change the login password for the “cisco” user.

Step 3: At the IPS module’s command-line interface, launch the System Configuration Dialogue by typing Setup.

sensor# setup

The IPS module enters the interactive setup.

Step 4: Define the IPS module’s hostname.

--- Basic Setup ---
--- System Configuration Dialog ---
At any point you may enter a question mark ‘?’ for help. Use ctrl-c to abort configuration dialog at any prompt. Default settings are in square brackets ‘[]’.
Current time: Mon Oct 12 23:31:38 2009
Enter host name [sensor]: IPS-SSP20-A

Step 5: Define the IP address and gateway address for the IPS module’s external management port.

Enter IP interface [192.168.1.62/24,192.168.1.250]: 10.10.63.21/24,10.10.63.1
**Step 6:** Define the access list, and then press Enter. This controls management access to the IPS module. For the Midsize-2500 network, all addresses in the HQ subnet (10.10.0.0/16) will be allowed. Hit Enter at a blank Permit prompt to go to the next step.

- Modify current access list?[no]: yes
- Current access list entries:
  - No entries
- Permit: 10.10.0.0/16

**Step 7:** Accept the default answer (no) for the next three questions.

- Use DNS server for Global Correlation? [no]:
- Use HTTP proxy server for Global Correlation? [no]:
- Modify system clock settings?[no]:

Note the following:

- Global correlation is disabled until later in the configuration process.
- An HTTP proxy server address is not needed for a network that is configured according to the Cisco SBA for Midsize Organizations—Borderless Networks Foundation Deployment Guide.
- You will configure time details in the sensor’s GUI console.

**Step 8:** Accept the default answer (off) for the option to participate in the SensorBase Network.

Participation in the SensorBase Network allows Cisco to collect aggregated statistics about traffic sent to your IPS.

- SensorBase Network Participation level? [off]:

The IPS SSP displays your configuration and a brief menu with four options.

**Step 9:** In the System Configuration dialog, save your configuration and exit setup by entering 2.

The following configuration was entered.

- [removed for brevity]
- exit
- [0] Go to the command prompt without saving this configuration.
- [1] Return to setup without saving this configuration.
- [2] Save this configuration and exit setup.
- [3] Continue to Advanced setup.

Enter your selection [3]: 2

Warning: DNS or HTTP proxy is required for global correlation inspection and reputation filtering, but no DNS or proxy servers are defined.

--- Configuration Saved ---

Complete the advanced setup using CLI or IDM.

To use IDM, point your web browser at https://<sensor-ip-address>.

**Step 10:** Repeat Procedure 1, Step 1 through Step 9 for the IPS sensor installed in the other Cisco ASA chassis. Be sure to use a different IP address on the other sensor’s management interface.

--- Procedure 2: Complete basic configuration ---

Once the basic setup in the System Configuration Dialogue is complete, you will use the startup wizard in the integrated management tool, Cisco Adaptive Security Device Manager (ASDM), to complete the remaining tasks in order to configure a basic IDS configuration:

- Configure time settings
- Configure DNS and NTP servers
- Define a basic IDS configuration
- Configure inspection service rule policy
- Assign interfaces to virtual sensors
Step 1: Connect to the sensor by navigating to the IPS tab in Cisco ASDM and entering the required connection information.

Step 2: Navigate to Sensor Setup > Startup Wizard, and then click Launch Startup Wizard.

Step 3: Review the Startup Wizard Introduction, and then click Next.

Step 4: On the Sensor Setup page, configure the DNS server address, time zone, and NTP server address.

Tech Tip
NTP is particularly important for security event correlation if you use a Security Event Information Manager product to monitor security activity on your network.

Step 5: If necessary for your time zone, select Enable Summertime. Ensure that Authenticated NTP is not selected, and then click Next.
Step 6: In the Traffic Allocation window, click Add.

Step 7: In the Specify traffic for IPS Scan window, next to Traffic Inspection Mode, select Inline, and then click OK. Note that if the Cisco ASA already had a default Traffic Allocation policy, IDM displays a warning that “The Service Rule Policy you are trying to create already exists.” You can cancel the window and proceed to the next step if you receive this warning.

Step 8: On the Traffic Allocation page, in the Packet Flow Diagram for the selected Rule panel, verify the traffic allocation configuration by clicking Start. The animation will illustrate a packet being copied to the IPS module and the egress interface. The animation may display an incorrect platform compared to the one you are configuring.

Step 9: On the Startup Wizard screen, click Finish, and then click Yes when you are prompted if you want to commit your changes to the sensor.

Step 10: Reboot the sensor and apply the changes by clicking OK.
Step 11: After the IPS module reboots, reconnect and navigate to IPS > Policies > IPS Policies.

On the main panel, note that there is an Event Action Override to Deny Packet Inline for all High Risk events.

Step 12: In the main panel, click the Risk Category for information about what High Risk means.

In the default case, High Risk means events that have a Risk Rating from 90 to 100. To reduce the risk of dropping non-malicious traffic, edit the Deny Packet action such that it triggers only when the Risk Rating is 100. This means that the sensor will now use the Deny Packet action only on events with a Risk Rating equal to 100, which only occurs when the most accurate, highest risk signatures fire.

Step 13: In the Virtual Sensor panel, right-click the vs0 entry, and then select Edit.

Step 14: Click the Deny Packet Inline Override, and then click Delete.

Step 15: Click Add to add a new override, enter a value of 100-100 for the Risk Rating, select Deny Packet Inline, click OK, and then click Apply.

Note: PIX/ASA devices do not support Connection Blocks. Use Request Block Host instead.
Step 16: Repeat these steps for the IPS module installed in the other Cisco ASA chassis. There is no configuration synchronization between the two sensors.

Reader Tip
Cisco IME is a standalone application that can configure and monitor activity for up to 10 sensors (as of IME 7.1.1). Cisco IME is available at no extra cost on Cisco.com in the same web location as Cisco IPS software updates and upgrades.

Procedure 3 Configure signature updates
(Optional)
IDS and IPS devices are generally only as good as their last update, and because of this, keeping the sensors updated is important. To this end, the easiest solution is to configure each sensor to retrieve signature updates directly from Cisco.com. Use Cisco ASDM to program the following steps.

Step 1: Access IPS > Sensor Management > Auto/Cisco.com Update, select Enable Signature and Engine Updates from Cisco.com, and then expand the Cisco.com Server Settings panel.

Step 2: Provide a valid cisco.com username and password that holds entitlement to download IPS software updates.

Step 3: Select Daily, enter a time between 12:00 a.m. and 4:00 a.m. for the Start Time, and then select each day.

Tech Tip
Using the auto update feature from Cisco.com will update only the sensor’s engine files and signature files. Major and minor code versions and service packs are not updated with this mechanism.
Application Resiliency

**Business Overview**

The network is playing an increasingly important role in the success of a business. Key applications such as enterprise resource planning, e-commerce, email, and portals must be available around the clock to provide uninterrupted business services. However, the availability of these applications is often threatened by network overloads as well as server and application failures. Furthermore, resource utilization is often out of balance, resulting in the low-performance resources being overloaded with requests while the high-performance resources remain idle. Application performance, as well as availability, directly affects employee productivity and the bottom line of a company. As more users work more hours while using key business applications, it becomes even more important to address application availability and performance issues to ensure achievement of business processes and objectives.

There are several factors that make applications difficult to deploy and deliver effectively over the network.

**Inflexible Application Infrastructure**

Application design has historically been done on an application-by-application basis. This means the infrastructure used for a particular application is often unique to that application. This type of design tightly couples the application to the infrastructure and offers little flexibility. Because the application and infrastructure are tightly coupled, it is difficult to partition resources and levels of control to match changing business requirements.

**Server Availability and Load**

The mission-critical nature of applications puts a premium on server availability. Despite the benefits of server virtualization technology, the number of physical servers continues to grow based on new application deployments, which in turn increases power and cooling requirements.

**Application Security and Compliance**

Many of the new threats to network security are the result of application- and document-embedded attacks that compromise application performance and availability. Such attacks also potentially cause loss of vital application data, while leaving networks and servers unaffected.

One possible solution to improve application performance and availability is to rewrite the application completely to make it network-optimized. However, this requires application developers to have a deep understanding of how different applications respond to things such as bandwidth constraints, delay, jitter, and other network variances. In addition, developers need to accurately predict each end-user’s foreseeable access method. This is simply not feasible for every business application, particularly traditional applications that took years to write and customize.
Technology Overview

The idea of improving application performance began in the data center. The Internet boom ushered in the era of the server load balancers (SLBs). SLBs balance the load on groups of servers to improve their response to client requests, although they have evolved and taken on additional responsibilities such as application proxies and complete Layer 4 through 7 application switching.

Cisco Application Control Engine (ACE) is the latest SLB offering from Cisco. Its main role is to provide Layer 4 through 7 switching, but Cisco ACE also provides an array of acceleration and server offload benefits, including TCP processing offload, Secure Socket Layer (SSL) offload, compression, and various other acceleration technologies. Cisco ACE sits in the data center in front of the application servers and provides a range of services to maximize server and application availability, security, and asymmetric (from server to client browser) application acceleration. As a result, Cisco ACE gives IT departments more control over application and server infrastructure, which enables them to manage and secure application services more easily and improve performance.

Cisco’s Application Control Engine is the next-generation Application Delivery Controller that provides server load-balancing, SSL offload, and application acceleration capabilities. There are four key benefits provided by Cisco ACE:

- **Scalability**—Cisco ACE scales the performance of a server-based program, such as a web server, by distributing its client requests across multiple servers, known as a server farm. As traffic increases, additional servers can be added to the farm. With the advent of server virtualization, application servers can be staged and added dynamically as capacity requirements change.

- **High Availability**—Cisco ACE provides high availability by automatically detecting the failure of a server and repartitioning client traffic among the remaining servers within seconds, while providing users with continuous service.

- **Application Acceleration**—Cisco ACE improves application performance and reduces response time by minimizing latency and compressing data transfers for any HTTP-based application, for any internal or external end user.

- **Server Offload**—Cisco ACE offloads TCP, SSL processing, and compression from the server, which allows more users to be served and handle more requests, and reduce bandwidth requirements by up to 90% without increasing the number of servers.

Cisco ACE hardware is always deployed in pairs for highest availability: one primary and one secondary. If the primary Cisco ACE fails, the secondary Cisco ACE takes control. Depending on how session state redundancy is configured, this failover may take place without disrupting the client-to-server connection.

Cisco ACE uses both active and passive techniques to monitor server health. By periodically probing servers, the ACE will rapidly detect server failures and quickly reroute connections to available servers. A variety of health-checking features are supported, including the ability to verify web servers, SSL servers, application servers, databases, FTP servers, streaming media servers, and a host of others.

Cisco ACE can be used to partition components of a single web application across several application server clusters. For example: The two URLs www.mycompany.com/quotes/getquote.jsp and www.mycompany.com/trades/order.jsp could be located on two different server clusters even though the domain name is the same. This partitioning allows the application developer to easily scale the application to several servers without numerous code modifications. Furthermore, it maximizes the cache coherency of the servers by keeping requests for the same pages on the same servers.

Additionally, Cisco ACE may be used to push requests for cacheable content such as image files to a set of caches that can serve them more cost-effectively than the application servers.

Running SSL on the web application servers is a tremendous drain on server resources. By offloading SSL processing, those resources can be applied to traditional web application functions. In addition, because persistence information used by the content switches is inside the HTTP header, this information is no longer visible when carried inside SSL sessions. By terminating these sessions before applying content switching decisions, all the persistence options previously discussed become available for secure sites.

There are several ways to integrate Cisco ACE into the data center network. Logically, the Cisco ACE is deployed in front of the application cluster. Requests to the application cluster are directed to a virtual IP address (VIP) configured on the Cisco ACE. The Cisco ACE receives connections and HTTP requests and routes them to the appropriate application server based on configured policies.

Physically, the network topology can take many forms. One-armed mode is the simplest deployment method, where the Cisco ACE is connected off to the side of the layer 2/layer 3 infrastructure. It is not directly in the path of traffic flow and only receives traffic that is specifically intended for it. Traffic, which should be directed to it, is controlled by careful design of VLANs, virtual server addresses, server default gateway selection, or policy routes on the layer 2/layer 3 switch.
Deployment Details

Process

Configuring Connectivity to the Data Center Core Switches
1. Configure port channels on Nexus 5500s

Procedure 1 Configure port channels on Nexus 5500s

The Cisco ACE server load balancers serving applications and servers in the data center will each connect to one of the data center core Cisco Nexus 5500UP switches by using EtherChannel links.

The use of EtherChannel links for connectivity to the core provides a resilient connection, load balances traffic over the links, and makes it easier to add bandwidth in the future.

The data center core Cisco Nexus 5500UP switches use Virtual Port Channel (vPC) for many dual-homed EtherChannel devices. If the vPC peer link between the data center core switches fails, one of the switches will go into error recovery and shut down interfaces associated with VLANs that are part of vPC connections to prevent any loops in the infrastructure. Since the Cisco ACEs are single homed to each data center core switch and not using a vPC for connectivity, but are using a VLAN that is part of other vPC connections, they are non-vPC ports or “vPC orphan ports”. Use the vpc orphan-port suspend command to shut down the EtherChannel interfaces to the attached Cisco ACE on each switch in the event that the vPC peer link is broken between the data center core switches and a switch goes into error recovery mode. The active Cisco ACE on the switch that remains in service will continue operating and provides the resiliency in the design.

The Cisco ACE does support EtherChannel but does not support Link Aggregation Control Protocol (LACP). Therefore the channel-group mode will be forced on.

Step 1: Configure physical interfaces to the port channels as follows on the two Cisco Nexus 5500UP data center core switches. Use the speed 1000 command to set the ports connected to the Cisco ACE from the default of 10-Gigabit Ethernet to 1-Gigabit Ethernet.

Tech Tip

When configuring the interfaces, the vpc orphan-port suspend command must be entered before the channel-group command. If you enter the channel-group command on the interface first, the switch will not let you enter the vpc orphan-port suspend command on the interface.

• Configure the first Cisco Nexus 5500UP switch.

interface Ethernet1/3
description ACE 1 Gig 1/1
speed 1000
vpc orphan-port suspend
channel-group 13 mode on
interface Ethernet1/4
  description ACE 1 Gig 1/2
  speed 1000
  vpc orphan-port suspend
  channel-group 13 mode on

- Configure the second Cisco Nexus 5500UP switch.
  interface Ethernet1/3
    description ACE 2 Gig 1/1
    speed 1000
    vpc orphan-port suspend
    channel-group 13 mode on

  interface Ethernet1/4
    description ACE 2 Gig 1/2
    speed 1000
    vpc orphan-port suspend
    channel-group 13 mode on

When you assign the channel-group to a physical interface, it creates the logical EtherChannel (port-channel) interface. In the next step, configure the logical port-channel interfaces on both data center core switches and the physical interfaces tied to the port-channel will inherit the settings.

Step 2: Configure the logical port-channel interfaces.
  interface port-channel
    switchport mode trunk
    switchport trunk allowed vlan 148,912
    spanning-tree port type edge trunk

Step 3: On each Cisco Nexus 5500UP switch, configure an unused VLAN for the Cisco ACE fault tolerant heartbeat VLAN.
  vlan 912
  name ACE-Heartbeat

Process

Configuring Cisco ACE Appliance Network
1. Perform initial setup
2. Configure high availability

Procedure 1 Perform initial setup

Step 1: Connect to the Cisco ACE appliance via the console, perform the initial configuration, and then exit from the initial configuration dialog box at the prompt.

  switch login: admin
  Password: admin
  Admin user is allowed to log in only from console until the default password is changed.
  www user is allowed to log in only after the default password is changed.

  Enter the new password for user “admin”: password
  Confirm the new password for user “admin”: password
  admin user password successfully changed.
  Enter the new password for user “www”: password
  Confirm the new password for user “www”: password
  www user password successfully changed.

  ACE>Would you like to enter the basic configuration dialog (yes/no) [y]: n
  switch/Admin#
Step 2: Set up the basic network security policies. This allows for management access into the Cisco ACE.

```
access-list ALL line 8 extended permit ip any any
class-map type management match-any remote_access
  2 match protocol xml-https any
  3 match protocol icmp any
  4 match protocol telnet any
  5 match protocol ssh any
  6 match protocol http any
  7 match protocol https any
  8 match protocol snmp any
policy-map type management first-match remote_mgmt_allow_policy
  class remote_access
  permit
```

Step 3: Configure port channel and trunking on the gigabit Ethernet interfaces.

```
interface gigabitEthernet 1/1
  channel-group 1
  no shutdown
interface gigabitEthernet 1/2
  channel-group 1
  no shutdown
interface port-channel 1
  switchport trunk native vlan 1
  switchport trunk allowed vlan 148
  no shutdown
```

This configuration provisions a 2-Gbps port channel and is sufficient for a Cisco ACE 4710 with up to a 2-Gbps license. If a 4-Gbps license is being used, include gigabit Ethernet ports 1/3 and 1/4 for a total of 4 Gbps of throughput.

Step 4: Configure the VLAN 148 interface on the Cisco ACE for management access and general network connectivity.

```
interface vlan 148
  ip address 10.10.48.119 255.255.255.0
  access-group input ALL
  service-policy input remote_mgmt_allow_policy
  no shutdown
```

Step 5: Configure the default route.

```
ip route 0.0.0.0 0.0.0.0 10.10.48.1
```

The Cisco ACE should now be reachable via the network. Repeat Step 1 to Step 5 on the second Cisco ACE, replacing the IP address in Step 4 with 10.10.48.120.

---

**Procedure 2** Configure high availability

Next, you configure the Cisco ACE appliances as an active standby failover pair. Once you configure high availability, the devices will be synchronized and further configuration is only necessary on the primary Cisco ACE. Start with the Cisco ACE appliance that you want to be primary. In this example, the primary is 10.10.48.119.

Step 1: To access the Cisco ACE GUI, use a browser, navigate to https://10.10.48.119, and log in as admin, using the password you set in Procedure 1, Step 1.
Step 2: Navigate to Config > Virtual Contexts > High Availability (HA) > Setup, and then click Edit.

Step 3: In the ACE HA Management dialog box, enter the following values, and then click Deploy Now.
- VLAN – 912
- Interface – Port Channel 1
- IP Address – 10.255.255.1
- IP Address Peer Appliance – 10.255.255.2
- Netmask – 255.255.255.0
- Management IP Address – 10.10.48.119
- Management IP Address Peer Appliance – 10.10.48.120

Step 4: In the ACE HA Groups dialog box, click Add.

Step 5: Leave all of the values at their defaults, and then click Deploy Now.

Now high availability is configured on the primary Cisco ACE appliance. For the rest of the high availability configuration, you need to log into the secondary Cisco ACE appliance.

Step 6: Log into the secondary Cisco ACE appliance by navigating to HTTPS://10.10.48.120.

Step 7: Navigate to Config > Virtual Contexts > High Availability (HA) > Setup, and then click Edit.

Now high availability is configured on the primary Cisco ACE appliance.
Step 8: In the ACE HA Management dialog box, enter the following values, and then click Deploy Now.

- VLAN – 912
- Interface – Port Channel 1
- IP Address – 10.255.255.2
- IP Address Peer Appliance – 10.255.255.1
- Netmask – 255.255.255.0
- Management IP Address – 10.10.48.120
- Management IP Address Peer Appliance – 10.10.48.119

Step 9: In the ACE HA Groups dialog box, click Add.

Step 10: Leave all of the values at their defaults and then click Deploy Now.

The two Cisco ACE appliances should be communicating and high availability should be up and active. The device you just finished configuring should show a state of “Standby Hot” and the peer should be “Active”, as shown in the ACE HA Groups dialog box below.

Additional configuration will take place on the primary Cisco ACE appliance, 10.10.48.119, and any changes will be automatically replicated to the standby Cisco ACE.

---

Process

Setting up Load Balancing for HTTP Servers

1. Configure health probes
2. Configure real servers
3. Configure a server farm
4. Configure a NAT pool
5. Configure a virtual server

---

Procedure 1 Configure health probes

Health probes poll the servers or applications to make sure that the server or service is available and to allow the system to remove failed devices. For this configuration, you will build an Internet Control Message Protocol (ICMP) and an HTTP probe.

Step 1: Navigate to Config > Virtual Contexts > Load Balancing > Health Monitoring, and then click the + icon.

Step 2: In the New Health Monitoring dialog box, in the Name box, enter icmp-probe, and then, in the Type list, choose ICMP.
Step 3: Click Deploy Now.

Step 4: Navigate to Config > Virtual Contexts > Load Balancing > Health Monitoring, and then click the + icon.

Step 5: In the New Health Monitoring dialog box, in the Name box, enter http-probe, and then, in the Type list, choose HTTP.

Step 6: Click Deploy Now.

Step 7: Click the Expect Status tab, and then click +.

Step 8: For both the maximum and minimum status codes, enter 200, and then click Deploy Now.

You have now created the ICMP and HTTP probes, which you can use to monitor the real and virtual servers in the load balancing server farm.

---

**Procedure 2** Configure real servers

In this section, you will add the real servers across which the Cisco ACE appliance will load balance client connections.

**Step 1:** Navigate to Config > Virtual Contexts > Load Balancing > Real Servers, and then click Add.

**Step 2:** In the New Real Server dialog box, enter the values below, and then click Deploy Now.

- Name – webserver1
- IP Address – 10.10.48.111
- Probes – icmp-probe

**Step 3:** Navigate to Config > Virtual Contexts > Load Balancing > Real Servers, and then click Add.

**Step 4:** In the New Real Server dialog box, enter the values below, and then click Deploy Now.

- Name – webserver2
- IP Address – 10.10.48.112
- Probes – icmp-probe
This example uses the ICMP probe to monitor the real servers configured in this example, thereby ensuring the server is monitored rather than a specific service. This is the most flexible configuration and allows load balancing for multiple services on a single physical or virtual server.

The two web servers shown in this example are now configured. If you have additional servers that you plan on using, you can configure them now by following the example above.

**Procedure 3  Configure a server farm**

A server farm on the Cisco ACE is a pool of real servers that you can use to connect to the virtual IP address that the clients will use to connect to the HTTP service.

- **Step 1:** Navigate to Config > Virtual Contexts > Load Balancing > Server Farms, and then click **Add**.
- **Step 2:** In the New Server Farm dialog box, enter the values below, and then click **Deploy Now**.
  - Name – webfarm
  - Probes – http-probe
- **Step 3:** Click the **Real Server** tab, and then click **Add**.

**Step 4:** In the New Real Server dialog box, next to Name, select web-server1, and then in the Port box, enter **80** for HTTP.

**Step 5:** Click **Deploy Now**.

**Step 6:** Click the **Real Server** tab, and then click **Add**.

**Step 7:** In the New Real Server dialog box, next to Name, select web-server2, and then in the Port box, enter **80**.

**Step 8:** Click **Deploy Now**.

These steps have created the server farm webfarm with the real server members webserver1 and webserver2 for HTTP on port 80. The http-probe will monitor all the servers in the server farm to ensure that the HTTP service is available.

**Procedure 4  Configure a NAT pool**

- **Step 1:** Navigate to Config > Virtual Contexts > Network > NAT Pools, and then click **Add**.
- **Step 2:** In the New NAT Pool dialog box, enter the following values, and then click **Deploy Now**.
  - Start IP Address – 10.10.48.99
  - End IP Address – 10.10.48.99
  - Netmask – 255.255.255.0
### Procedure 5  Configure a virtual server

**Step 1:** Navigate to **Config > Virtual Contexts > Load Balancing > Virtual Servers**, and then click **Add**.

**Step 2:** In the Properties dialog box, enter the following values.
- Virtual Server Name – **http-vip**
- Virtual IP Address – **10.10.48.100**
- VLAN - **148**

**Step 3:** In the Default L7 Load-Balancing Action dialog box, in the Server Farm list, choose **webfarm**, and then select **Deflate**.

**Step 4:** In the NAT dialog box, click **Add**, click **OK**, and then click **Deploy Now**.

Clients going to the virtual IP 10.10.48.100 on port 80 will be load balanced across the real servers webserver1 and webserver2 in the server farm webfarm.

---

### Process

**Load Balancing and SSL Offloading for HTTPS Servers**

1. Configure real servers
2. Configure a server farm
3. Configure SSL proxy service
4. Configure HTTP cookie sticky service
5. Configure a virtual server
6. Configure an HTTP to HTTPS Redirect

This section describes configuring a group of servers for load balancing with the Cisco ACE appliance performing all the SSL processing, thereby offloading it from the servers.

### Procedure 1  Configure real servers

In this section you will add the real servers across which the Cisco ACE appliance will load balance client SSL connections.

**Step 1:** Navigate to **Config > Virtual Contexts > Load Balancing > Real Servers**, and then click **Add**.

**Step 2:** In the New Real Server dialog box, enter the values below, and then click **Deploy Now**.
- Name – **webserver3**
- IP Address – **10.10.48.113**
- Probes – **icmp-probe**
Step 3: Navigate to Config > Virtual Contexts > Load Balancing > Real Servers, and then click Add.

Step 4: In the New Real Server dialog box, enter the values below, and then click Deploy Now.

- Name – webserver4
- IP Address – 10.10.48.114
- Probes – icmp-probe

This example uses the ICMP probe to monitor the real servers configured in this example, thereby ensuring the server is monitored rather than a specific service. This is the most flexible configuration and allows load balancing multiple services on a single physical or virtual server.

The two web servers shown in this example are now configured. If you have additional servers that you plan on using, you can configure them now by following the example above.

Procedure 2 Configure a server farm

A server farm on the Cisco ACE is a pool of real servers that you can use to connect to the virtual IP address that the clients will use to connect to the HTTP service.

Step 1: Navigate to Config > Virtual Contexts > Load Balancing > Server Farms, and then click Add.

Step 2: In the New Server Farm dialog box, enter the values below, and then click Deploy Now.

- Name – appfarm
- Probes – http-probe

Step 3: Click the Real Server tab, and then click Add.

Step 4: In the New Real Server dialog box, in the Name list, choose webserver3, and then in the Port box, enter 80 for HTTP.

Step 5: Click Deploy Now.
Step 6: Click the **Real Server** tab, and then click **Add**.

Step 7: In the New Real Server dialog box, in the Name list, choose **web-server4**, and then in the Port box, enter **80**.

Step 8: Click **Deploy Now**.

---

**Procedure 3  Configure SSL proxy service**

For the Cisco ACE to offload the SSL processing, you need to configure an SSL proxy service. This example uses the Cisco sample key and certificate. However, in a production deployment, you would most likely purchase a certificate from a trusted certificate authority (CA).

Step 1: Navigate to **Config > Virtual Contexts > SSL > Proxy Service**, and then click **Add**.

Step 2: In the New Proxy Service dialog box, in the Name box, enter **app-ssl-proxy**.

Step 3: Select both **cisco-sample-key** and **cisco-sample-cert**, and then click **Deploy Now**.

---

**Procedure 4  Configure HTTP cookie sticky service**

The HTTP cookie sticky service keeps traffic from a client stuck to a single real server. This is useful for applications where state could be lost if the client connection was balanced across several servers.

Step 1: Navigate to **Config > Virtual Contexts > Load Balancing > Stickiness**, and then click **Add**.

Step 2: In the New Sticky Group dialog box, in the Group Name box, enter **app-sticky**.

Step 3: In the **Type** list, choose **HTTP Cookie**, and then in the Cookie Name box, enter **APPSESSIONID**.

Step 4: Select both **Enable Insert** and **Browser Expire**.

Step 5: Next to Sticky Server Farm, select **appfarm**, click **Deploy Now**.
**Procedure 5**  
Configure a virtual server

Step 1: Navigate to Config > Virtual Contexts > Load Balancing > Virtual Servers, and then click Add.

Step 2: In the Properties dialog box, enter the following values.
- Virtual Server Name – https-vip
- Virtual IP Address – 10.10.48.101
- Application Protocol – HTTPS
- VLAN - 148

Step 3: In the SSL Termination dialog box, in the Proxy Service Name list, choose app-ssl-proxy.

Step 4: In the Default L7 Load-Balancing Action dialog box, in the Primary Action list, choose Sticky, in the Sticky Group list, choose app-sticky (HTTP Cookie), and then select Deflate.

Step 5: In the NAT dialog box, click Add, click OK, and then click Deploy Now.

Clients going to the virtual IP 10.10.48.101 on port 443 will be load balanced across the real servers webserver3 and webserver4 in the server farm appfarm. The Cisco ACE will terminate the SSL session and load balance the connections to the real servers over standard HTTP on TCP port 80.

---

**Procedure 6**  
Configure an HTTP to HTTPS Redirect

(Optional)

It is often preferable to have HTTP traffic redirected to HTTPS to ensure that connections to that service are encrypted. This example describes creating a service that redirects any HTTP traffic directed to 10.10.48.101 to the HTTPS service configured in the steps above.

Step 1: Navigate to Config > Virtual Contexts > Load Balancing > Real Servers, and then click Add.
Step 2: In the New Real Server dialog box, enter the values below, and then click Deploy Now.
- Name – redirect1
- Type - Redirect
- Web Host Redirection – https://%h%p
- Redirection Code - 302

Step 3: Navigate to Config > Virtual Contexts > Load Balancing > Server Farms, and then click Add.

Step 4: In the New Server Farm dialog box, enter the values below, and then click Deploy Now.
- Name – http-redirect
- Type – Redirect

Step 5: Click the Real Server tab, and then click Add.

Step 6: In the New Real Server dialog box, select redirect1.

Step 7: Click Deploy Now.

Step 8: Navigate to Config > Virtual Contexts > Load Balancing > Virtual Servers, and then click Add.

Step 9: In the Properties dialog box, enter the following values.
- Virtual Server Name – http-vip-redirect
- Virtual IP Address – 10.10.48.101
- VLAN - 148

Step 10: In the Default L7 Load-Balancing Action dialog box, in the Server Farm list, choose http-redirect, and then click Deploy Now.
The following products and software version have been validated for the Cisco Smart Business Architecture.

**Table 2 - Products**

<table>
<thead>
<tr>
<th>Functional Area</th>
<th>Product</th>
<th>Part Numbers</th>
<th>Software Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethernet Infrastructure</td>
<td>Nexus 5548UP</td>
<td>N5K-C5548UP-FA</td>
<td>NX-OS 5.1(3)N1(1)</td>
</tr>
<tr>
<td></td>
<td>Nexus 5548 Layer 3 Daughter Card</td>
<td>N55-D160L3</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Nexus 2248TP</td>
<td>N2K-C2248TP-1GE</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Nexus 2232PP</td>
<td>N2K-C2232PP-10GE</td>
<td></td>
</tr>
<tr>
<td>Storage Infrastructure</td>
<td>MDS 9148</td>
<td>DS-C9148D-8G16P-K9</td>
<td>NX-OS 5.0(7)</td>
</tr>
<tr>
<td></td>
<td>MDS 9124</td>
<td>DS-C9124-K9</td>
<td></td>
</tr>
<tr>
<td>Network Security</td>
<td>ASA 5585-X</td>
<td>ASA5585-S40-K9</td>
<td>ASA: 8.4.2</td>
</tr>
<tr>
<td></td>
<td>ASA 5585-X IPS SSP</td>
<td>ASA5585-SSP-IPS20</td>
<td>IPS: 7.1-2-E4</td>
</tr>
<tr>
<td>Application Resiliency</td>
<td>Cisco ACE 4710 Appliance</td>
<td>ACE-4710-0.5-K9</td>
<td>A5(1.0)</td>
</tr>
</tbody>
</table>
Appendix B: Changes

This appendix summarizes the changes to this guide since the previous Cisco SBA series.

- We updated the Ethernet Infrastructure module to use the Cisco Nexus 5500UP Series switch with Layer 2 and Layer 3 to create a standalone routed data center core. We also added details for an Ethernet out-of-band management network.
- We updated the Storage Infrastructure module to use the Cisco Nexus 5500UP Series switch as the Fibre Channel SAN core with MDS 9100 Series deployment for expansion for larger Fibre Channel SAN requirements.
- We updated the Computing Resources module to Compute Connectivity and explained various methods for connecting servers to the data center network.
- We updated the Network Security module to detail the move of the data center firewalls and integrated Cisco IPS to connect to the data center core switches.
- We updated the Application Resiliency module with a more advanced version that details deployment for multiple health probes and resiliency features.
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.