Newer Cisco SBA for Government Guides Available

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

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.

Data Center Deployment Guide

SBA FOR GOVERNMENT

Revision: H2CY10

The Purpose of this Guide

Within the *Cisco Smart Business Architecture (SBA) for Government Midsize Agencies—Borderless Networks Foundation Deployment Guide*, the Server Room module accommodates up to 24 physical servers. That design provides basic computing and storage capability for agency operations.

The Data Center for Midsize Agencies described in this guide can easily replace the server room in the SBA foundation architecture for more advanced agency operations and applications. This will provide an architecture designed to accommodate growth of the server farm up to 250 physical or virtual servers.

Use this guide as an addendum to the *Cisco SBA for Midsize Agencies—Borderless Networks Foundation Deployment Guide* and as a "snap-In" replacement for the Server Room module.

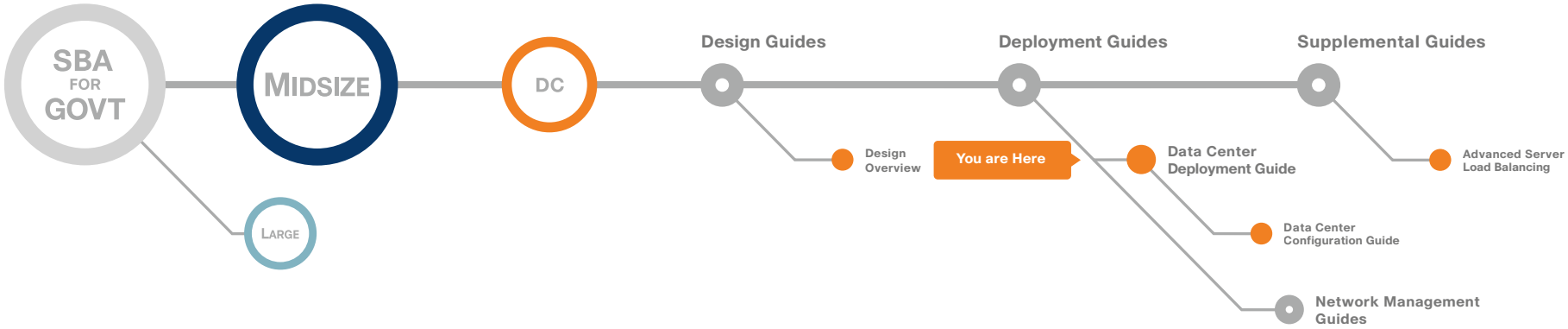
As with the *Cisco SBA for Midsize Agencies—Borderless Networks Foundation Deployment Guide*, this guide is a prescriptive reference design that provides step-by-step instructions for the deployment of the design. It is based on enterprise best practice principles, yet delivered in a design and cost structure for midsize agencies that are growing and expanding. Based on feedback from customers and partners, Cisco has developed a solid network foundation as a flexible platform that does not require reengineering to include additional network or user services.

To reflect our ease-of-use principle, this guide is organized into modules. You can start at the beginning or jump to any module. Each part of the guide is designed to stand alone, so you can deploy the Cisco technology for that section without having to complete the previous module.

The specific products that make up this design are listed at the end of this document for your convenience. A separate document, the *Cisco SBA for Midsize Agencies—Data Center Configuration Files Guide*, contains the specific configuration files from the products used in the Cisco lab testing and can be found on Cisco.com.

Tech Tip

If this design does not scale to meet your needs, please refer to the Cisco Validated Designs (CVD) for larger data center deployment models. CVDs can be found on Cisco.com.



Who Should Read This Guide

This guide is intended for the reader who has any or all of the following:

- Has already read the *Cisco SBA for Midsize Agencies—Borderless Networks Foundation Deployment Guide*
- Has an existing server room and is looking to solve agency problems that require technologies more typically found in a data center
- Uses iSCSI and/or Fibre Channel for storage

The intended reader of this document will be ready to:

- Increase their computing capacity from the Server Room design
- Expand from a few dozen servers to a combination of virtual and physical servers up to 250 servers
- Gain additional storage capacity for their servers
- Improve server utilization with virtual servers
- Ensure availability of applications
- Consolidate and virtualize storage and servers
- Deploy a business continuance/disaster recovery data center solution

Related Documents

Before reviewing this guide

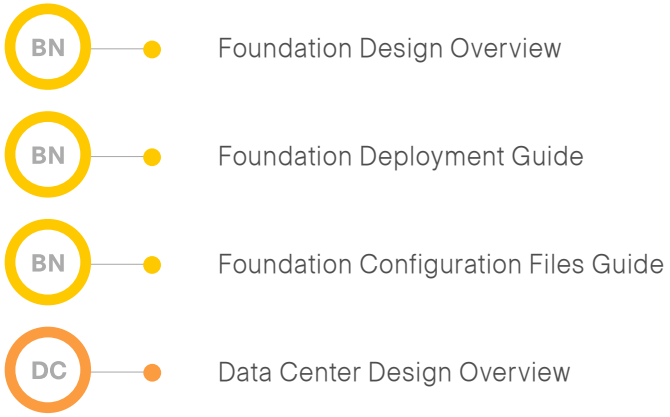


Table of Contents

Introduction

Every agency begins with an idea. Transforming that idea into a agency is an evolution that involves people and processes. In the beginning, most agencies start with a small number of people and processes. As the agency evolves, people are added and new processes developed to support the agency. In the early days of a agency, the processes move quickly from manual to electronic. Today, even in their infancy, agencies rely on computerization and applications.

Email is a ubiquitous application used for the transfer of information, and while there are many public email services available, whether hosted off site or locally, most agencies bring the service in-house. Now, the agency has a server to care for. Other operational processes get added to the server and one server becomes many.

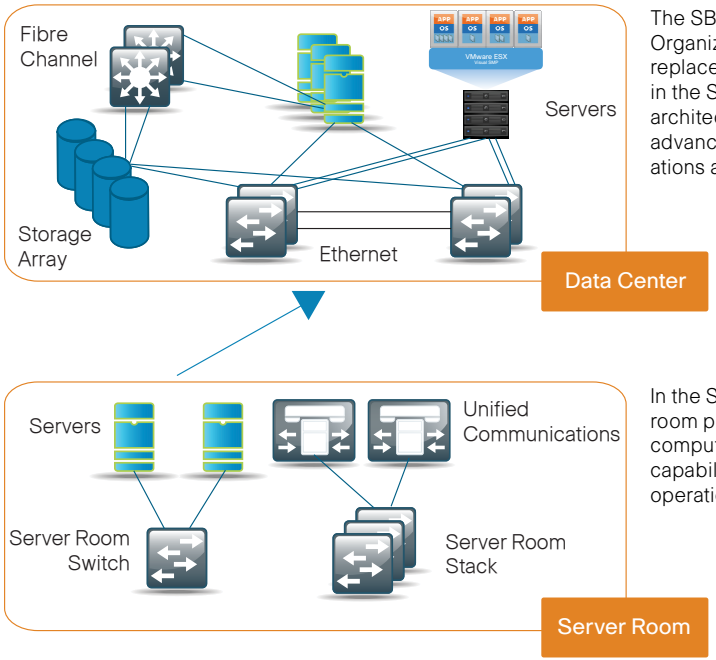
As the number of servers grows, so does the reliance the agency has on the information stored on those servers, at which point, the agency information technology (IT) organization generally forms. Prior to this stage, the servers were purchased as needed with little process; they sat under a desk or in a closet, and the care and feeding was performed ad hoc. When the agency grows and has multiple servers, it is necessary to develop a standard process for the selection and maintenance of the hardware and the viability of the information stored within those computers. This usually includes the consolidation of the servers into a single physical location within the agency and/or sometimes hosted off premises. In either case, the need for a server room or a more scalable data center is born.

For Cisco partners and customers whose server farm will have a combined total of up to 250 physical and virtual servers, Cisco has created a network architecture that is simple, fast to deploy, affordable, scalable, and flexible. We have designed it to be easy. Easy to install, configure, and manage. By taking advantage of the foundation architecture you've already deployed, the SBA Data Center lets you add 50 or 250 servers, or a disaster recovery site, without wasting time and expense reconfiguring the existing network foundation.

The deployment has been architected to make your life a little bit—maybe even a lot—easier. This architecture:

- Provides a solid foundation
- Makes deployment fast and easy
- Avoids the need for reengineering the core network

Figure 1. Server Farm to Data Center Transition



The SBA DC for Midsize Organizations can easily replace the server room in the SBA foundation architecture for more advanced business operations and applications.

In the SBA, the server room provides basic compute and storage capability for business operations.

Agency Requirements

The Cisco SBA Data Center Architecture for Midsize Agencies is designed to address four primary issues encountered by growing agencies:

- Supporting application growth
- Managing data storage requirements
- Optimizing the investment in server processing resources
- Providing for business continuance

Supporting 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 agency often increases. The first phase of the server room evolution is caused when the agency outgrows the capacity of the existing server room. 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 agency to smoothly scale the size of the server farm as application requirements change.

Managing 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 agency grows, the investment in this 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 using storage area network (SAN) technology.

A dedicated storage system provides multiple benefits beyond raw disk capacity, including:

- The ability to increase the reliability of disk storage, which improves application availability.
- Increased capacity can be provided to a given server over the SAN without needing to physically attach new devices to the server itself.
- More sophisticated backup and data replication technologies are available in SAN storage, which helps protect the agency against data loss and application outages.

The design provided in this guide allows easy integration of centralized storage into the server farm with a choice of multiple storage-networking technology options.

Optimizing the Investment in Server Processing Resources

As an agency grows, 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 agency 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 virtual machines on server hardware helps to increase processor utilization levels, while still allowing each VM to be viewed as independent from a security, configuration, and troubleshooting perspective.

Server virtualization and SAN storage technologies complement one another to allow rapid deployment of new servers, and reduce 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 agency great flexibility when rolling out new applications or upgrading server hardware.

The architecture defined in this guide is designed to facilitate easy deployment of server virtualization, while still providing support for the existing installed base of equipment.

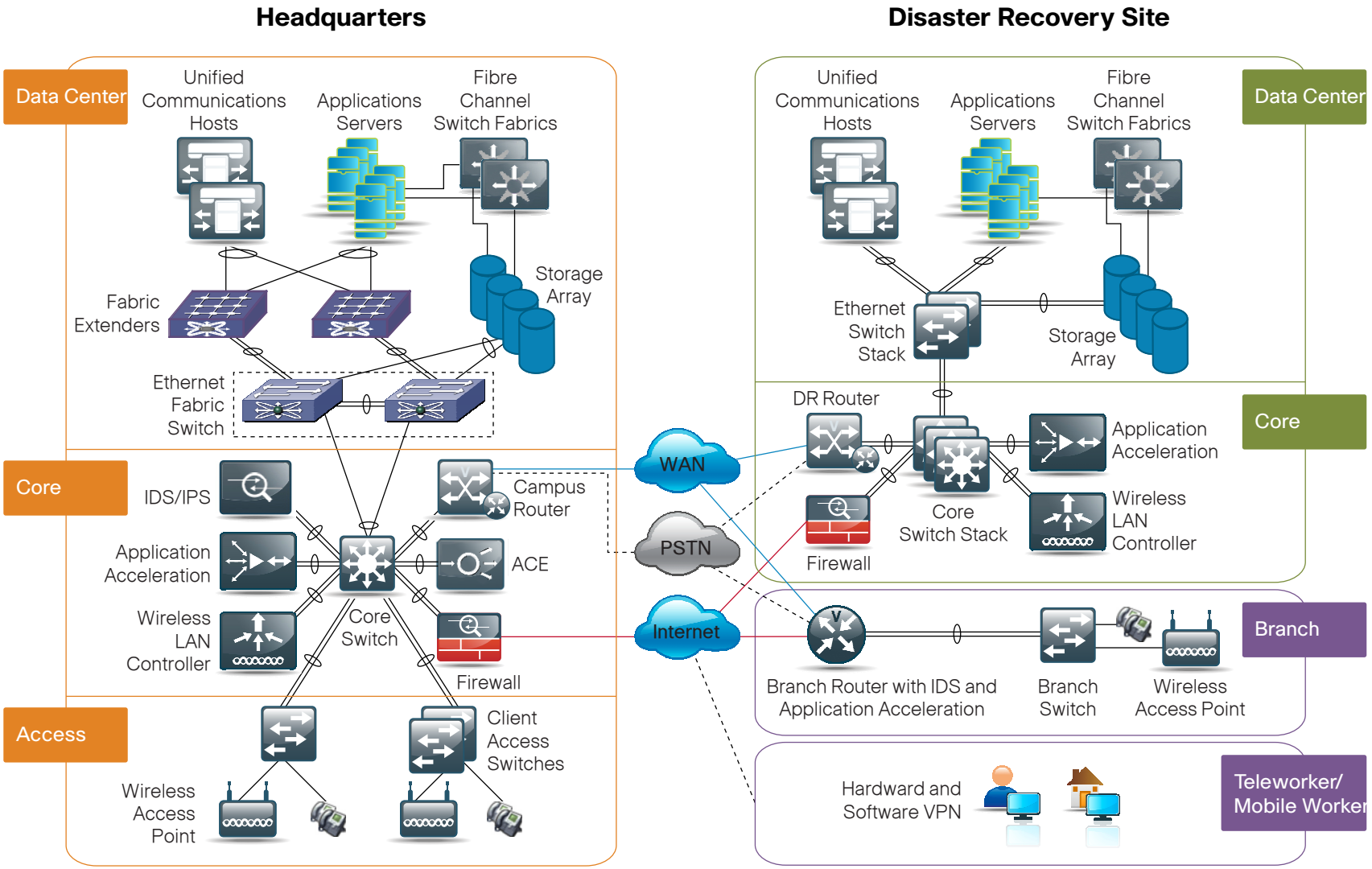
Providing for Business Continuance

The fourth requirement is business continuance. As the agency continues to grow, so too does its reliance on the applications provided by the servers and storage systems. These applications and their associated data need to be accessible even if the primary location experiences a catastrophic event. The resilient design includes a secondary data center or disaster recovery (DR) site. In the event of the primary location becoming unreachable, the DR site is activated. The DR site may be housed in a location owned by the busi¬ness or for cost reasons co-located with a hosting service provider. The inclusion of a DR site in the overall design can help the agency to address multiple types of potential failures, from single wide-area network (WAN) link outages to loss of individual applications or servers.

Some of the sections included in this guide are modifications to the original SBA design to enable DR capability. For example, the remote-site WAN design was modified in this deployment guide to address failing over services to the DR site.

Figure 2 depicts the architecture that will be in place if you deploy all of the modules in the data center design.

Figure 2. Data Center for Midsize Agencies Design



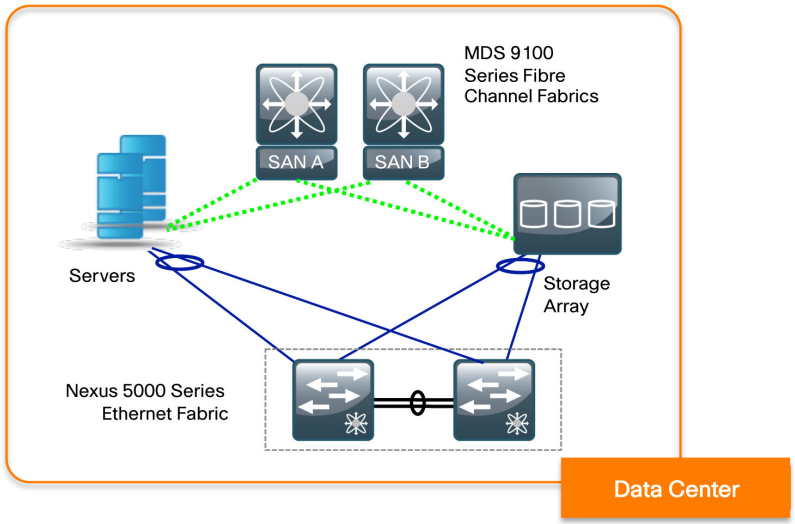
Ethernet Data Center Design

Agency Overview

Your agency resources such as agency and client data, availability, and disaster recovery are key business continuance considerations. Selecting an architecture that can address each of these in a scalable manner is the goal of this section. Drivers that affect your architecture may vary. You may be experiencing rapid growth of data storage, new applications, or application performance. Each of these issues can create a different set of challenges. As each of these problems are addressed, resiliency and high availability become increasingly critical.

In this module, which is the foundation for your new data center for midsize agencies we will explore various options and recommendations to address these requirements.

Figure 3. Ethernet Data Center Design



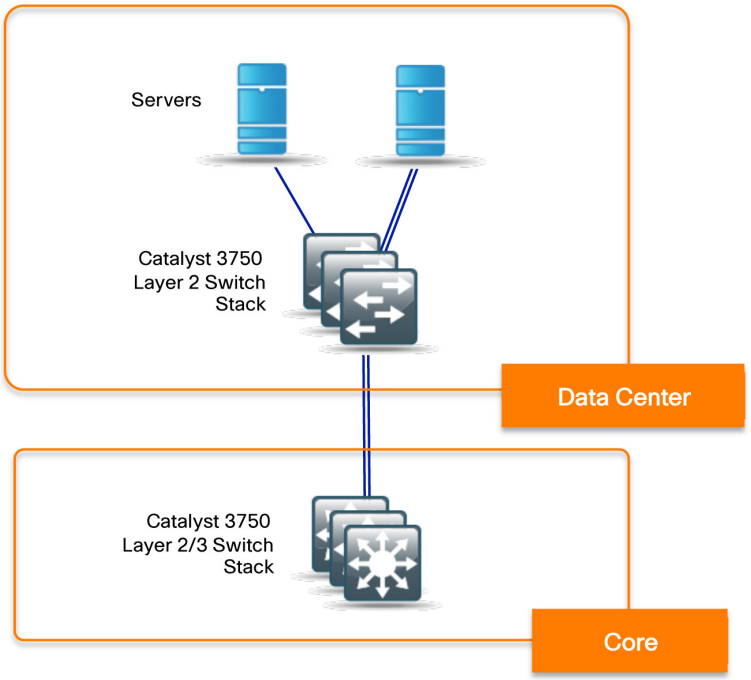
Technology Overview

The Ethernet data center design presented here addresses the availability, performance, and scalability requirements that are at the heart of the evolution from server room to data center (Figure 3).

Small Data Centers

For data centers with one to two racks of servers, the Cisco Catalyst® 3750G switch is a good option. Several Catalyst 3750 Series switches can be stacked together to act as a single switch for simplified configuration and management. The uplinks from the 3750s can be distributed across the stack for high availability and to scale bandwidth from the data center to the network core (Figure 4). This approach also allows the solution to scale as the data center server throughput requirements grow.

Figure 4. Small Data Center Design



Tech Tip

The input/output or total throughput of the server is going to drive the decision of how many connections you have from the server to the network. When you add all of the connections for the servers, do you have enough network ports?

The Cisco Catalyst 3750G can support up to 192 1-Gbps Ethernet ports in the Cisco SBA Data Center for Midsize Agencies design. A basic hardware configuration would be two 3750s stacked together at the top of the rack, that provide either 48 ports of Gigabit Ethernet using the 24-port 3750 switches or 96 ports if using the 48-port 3750 switches.

An additional pair of 3750s can be added to another rack to support an additional 96 Gigabit Ethernet ports if you need to scale up the design. This second pair is connected to the first pair via StackWise cables to make all four switches into a single switch stack for simplified management and high availability.

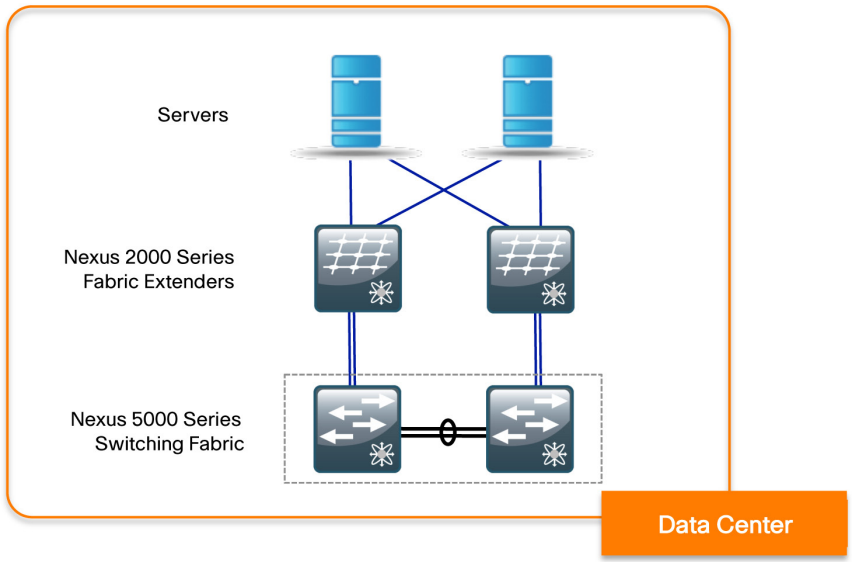
If the data center servers are mostly or entirely made up of blade servers, Cisco offers the Cisco Catalyst Blade Switch 3100 Series Switches. The blade switches slot into the blade server chassis and connect directly to the servers over the chassis midplane. The Cisco Catalyst 3100 Blade Switches are available for Dell, FSC, HP, and IBM blade enclosures. The blade switch operates similarly to a standalone Cisco 3750 switch; they can be stacked with other blade switches and have Ethernet uplink ports that can be attached by way of a port channel to the resilient core.

Medium Data Centers

For medium data centers, the Cisco Nexus™ 5000 Series switches with Cisco® Nexus 2000 Series Fabric Extenders (FEX) allow for higher-performance server connectivity, up to 10-Gigabit Ethernet.

In the SBA design, two Cisco Nexus 5000 Series switches are configured independently, but work together as a resilient pair that is connected to servers via the fabric extenders or attached directly to the Cisco Nexus 5000 Series switches. The fabric extenders can be configured to home to a single Cisco Nexus 5000 Series switch that provides optimal connectivity to dual-attached servers, or to dual-home to both Cisco Nexus 5000 Series switches to provide higher resiliency for single attached servers (Figure 5).

Figure 5. Medium Data Center Design



Design Options

If you plan to have a combination of rack and blade servers, standalone switches and pass-through modules are the best choices. This design provides a single platform for switching multiple types of servers. If the agency is planning to migrate to use blade servers exclusively, the Cisco Catalyst 3100 Series switches provide a clean solution that can help reduce cabling requirements within the data center racks.

If you are choosing between the two designs, choose the Cisco Catalyst 3750G Stack if you:

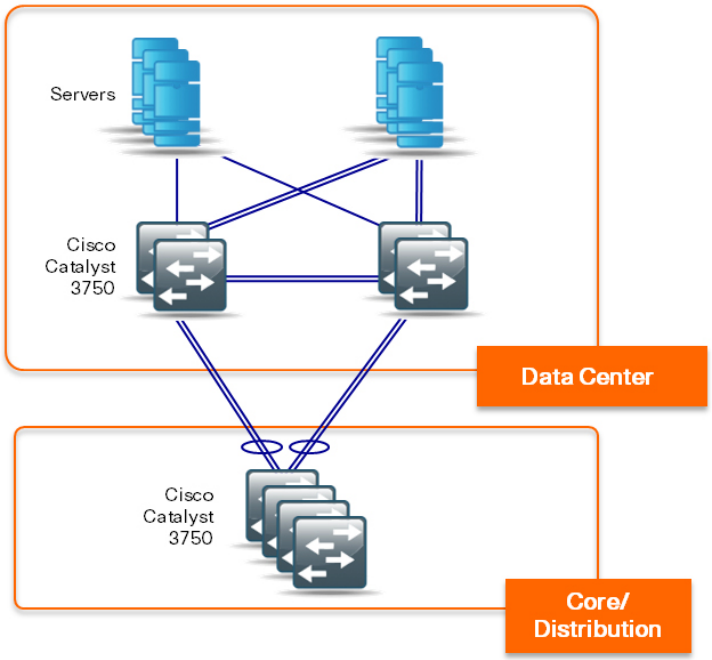
- Want to move from an existing server room model to the SBA Data Center for Midsize Agencies model.
- Have only one or two racks of servers.
- Want to use the same hardware in the data center as in the client access layer for easy sparing.
- Have a combination of 10/100 Mbps and Gigabit Ethernet connected hosts.
- Need the resiliency of a data center, but not the high performance or scalability of the Nexus 5000/2000 design.

Choose the Cisco Nexus 5000/2000 design if you:

- Have devices that all support Gigabit Ethernet.
- Have more than one or two racks of servers.
- Need wire-rate Gigabit Ethernet performance for a large number of ports.
- Plan to migrate some devices to 10 Gigabit Ethernet.
- Need very low latency between devices within the data center.
- Plan to migrate to Fibre Channel over Ethernet (FCoE) and Unified Fabric in the future.

Connectivity to the Core

Figure 6. Connectivity to the Core



The resilient core described in the *Cisco SBA for Midsize Agencies—Borderless Networks Foundation Deployment Guide* provides all the Layer 3 services to the network.

Whether you use a Cisco Catalyst 3750 stack (Figure 6) or a Cisco Nexus 5000 Series resilient pair, the following recommendations can help guard against hardware failure in the data center for Midsize Agencies:

- Each switch has at least one uplink connected to the resilient core.
- The uplinks are connected to different cards or switches depending on the hardware in the core. All of the uplinks are a member of a single port-channel group for simpler configuration (no STP is required).
- When using a Cisco Catalyst 3750 stack, the uplinks are Gigabit and the logical link can scale up to a total of eight physical uplinks distributed among the member switches in the stack. The total throughput is an aggregation of all the links between the data center and network core switches.

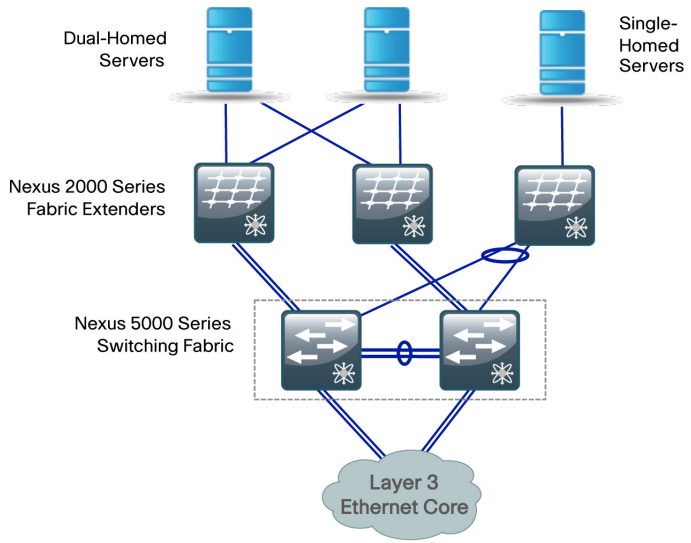
When using a Cisco Nexus 5000 Series resilient pair, the uplinks attached to the Cisco Catalyst 4507RE resilient core are each 10 Gigabit.

Servers with Dual Network Connections

Having multiple paths from the core all the way to the server is a key contributor to service high availability (Figure 7). Server to data center access layer link-level resiliency and load sharing can be achieved when the servers support the 802.3ad Link Aggregation Control Protocol (LACP) or with more basic network interface card (NIC) teaming.

As with the connectivity to the core, to guard against hardware failure in the data center access layer, the server uplinks are connected to different switches.

Figure 7. Server Connectivity



Servers with Single Network Connections

Even in a data center, there are situations where a server may not have dual paths all the way to the core. For example, service resiliency may be built into the application layer, or the service may reside on hardware that cannot be dual-attached.

A single-attached host can be given a level of resiliency by connecting it as a dual-attached access layer switch. The host network connection is still a single point of failure, but the access switch has resilient uplinks to protect against failures.

Jumbo Frames

Jumbo Frames are a common way to improve performance. They are bigger than the standard Ethernet frame size and benchmarks show they can potentially double the throughput and lower server processor load.

Jumbo Frames allow for higher utilization of links with less overhead for a server and the network since fewer packets are being sent.

Flow Control

In a network path that normally consists of multiple hops between source and destination, lack of feedback between transmitters and receivers at each hop is one of the main causes of unreliability. Transmitters can send packets faster than receivers can accept packets. As the receivers run out of available buffer space to absorb incoming flows, they are forced to silently drop all traffic that exceeds their capacity.

For applications that cannot build reliability on upper layers, the addition of flow control functions at Layer 2 can offer a solution. Flow control enables feedback from a receiver to the sender to communicate buffer availability.

EtherChannel—Number of Ports

Port-channel technology (IEEE 802.3ad) provides the capability for multiple physical links between participating devices to be used concurrently to forward traffic as a single logical link. As bandwidth needs increase in the network, more member links can be added to port-channel groups to increase the available bandwidth. This works well for scaling the connection from the data center switches to the core. Servers can use port channels to connect to the data center switches, but it is more common for a server to use more basic NIC teaming.

Process

Configuring the Cisco Nexus 5000/2000 Pair

1. Configure Platform
2. Configure a Virtual Port Channel (vPC)

Complete each of the following procedures to configure the Cisco Nexus 5000/2000 pair.

Procedure 1 Configure Platform

Step 1: The default administration account needs to be configured with a password. Enter the following at the command line:

```
username admin password [password] role network-admin
```

Step 2: The management interface of the Cisco Nexus 5000 Series switch is connected to the core directly because it is used not only to manage the device, but is the link used for keep-alive messages between the vPC peers.

```
interface mgmt0
   ip address [address]/[mask]
!
vrf context management
   ip route 0.0.0.0/0 [gateway]
```

Step 3: Several features are required for normal operations. Enter the following commands to enable normal operation:

```
feature telnet
cfs eth distribute
feature private-vlan
feature udld
feature interface-vlan
```

Step 4: SSH is enabled by default. However, if you need to generate an SSH key, use the following command:

```
ssh key rsa 2048
```

Step 5: If you need to use Telnet to manage the device, you must enable it. Enter the following at the command line:

```
telnet server enable
```

Procedure 2 Configure a Virtual Port Channel (vPC)

A vPC allows a server or switch to connect multiple physical links to two physical switches and use all available bandwidth on those links as if they were connected via an EtherChannel link to a single switch. This makes it possible to eliminate the port blocking behavior of spanning tree and utilize all the available bandwidth while providing dual-path resiliency. The Cisco Nexus 5000 Series switches that work together to form the vPC pair are configured separately. Most of the following commands can be executed without modification on each switch.

Step 1: The vPC domain allows the two Cisco Nexus 5000 Series switches to know that they need to work together as a vPC pair. The keep-alive addresses should be the management interfaces of the Cisco Nexus 5000 Series switches.

```
feature lacp
feature vpc
vpc domain [domain number]
   peer-keepalive destination [ip] source [ip]
```

Step 2: Configure one Cisco Nexus 5000 Series switch to be the secondary switch for the vPC pair.

```
vpc domain [domain number]
   role priority 16000
```

Step 3: Connect the Cisco Nexus 5000 Series switches together via two 10-Gigabit connections to form a port-channel connection for the vPC peer link.

```
interface Ethernet[port number]
   channel-group 10 mode active
interface port-channel[channel number]
   switchport mode trunk
   switchport trunk native vlan [vlan]
   switchport trunk allowed vlan [list]
   vpc peer-link
   spanning-tree port type network
```

Step 4: For each FEX, you need to configure a unique FEX number and associate it to the physical ports that the FEX is connected to on the Cisco Nexus 5000 Series switch.

If you plan on dual-homing the servers to the Cisco Nexus 5000/2000 pair, the following configuration is required:

```
fex [fex number]
   pinning max-links [num of links]
int ethernet [port number]
   channel-group [channel number]
interface port-channel[channel number]
   switchport mode fex-fabric
   fex associate [fex number]
```

Step 5: If you plan on dual-homing the FEX because you have single-homed servers, enter these additional commands at the command line:

```
interface port-channel[channel number]
   vpc [vpc number]
```

Process

Configuring the Cisco 3750G and Cisco Nexus 5000/2000 Pair

1. Configure Basic Virtual Switching
2. Configure Support for iSCSI Storage

Complete each of the following procedures to configure the Cisco 3750G and Cisco Nexus 5000/2000 pair.

Procedure 1 Configure Basic Virtual Switching

Basic switch configuration is covered in the *Cisco SBA for Midsize Agencies—Borderless Networks Foundation Deployment Guide's* Global Configuration module and is not addressed here. Cisco 3750G configuration examples can also be used for the Cisco Catalyst Blade Switch 3100.

This procedure explains the interface configuration for servers that attach to a single VLAN and require no trunking or channeling.

If you are connecting to the Cisco Catalyst 3750G, the server can be connected with no change to multiple ports on the switch for NIC teaming, as long as the server is not tagging traffic with different VLAN IDs. Basic virtual switching can also be configured on the host if virtual machines are being run on the host without modifying the configuration described here.

Step 1: Enter the following at the command line:

For the Cisco Catalyst 3750G:

```
interface GigabitEthernet[port number]
   switchport access vlan [server VLAN]
   switchport mode access
   spanning-tree portfast
   spanning-tree bpduguard enable
```

For the Cisco Nexus 5000/2000:

```
interface Ethernet[port number]
   switchport access vlan [server VLAN]
   spanning-tree port type edge
```

Step 2: Servers that need VLAN trunking and EtherChannel, which are typically servers using virtualization technologies, can use this port configuration. Enter the following at the command line.

For the Cisco Catalyst 3750G:

```
interface GigabitEthernet[port number]
   switchport nonegotiate
   channel-group [channel number] mode on
   spanning-tree portfast trunk
interface Port-channel [channel number]
   switchport trunk encapsulation dot1q
   switchport trunk allowed vlan [list]
   switchport mode trunk
   switchport nonegotiate
```

Tech Tip

The Cisco Catalyst Blade Switch 3130 does not require switch-port trunk encapsulation dot1q.

For the Cisco Nexus 5000/2000:

```
interface Ethernet[port number]
   spanning-tree port type edge
   channel-group [channel number]
interface port-channel[channel number]
   switchport mode trunk
   switchport trunk allowed vlan [list]
   vpc [vpc number]
```

Procedure 2 Configure Support for iSCSI Storage

Step 1: If the server is connecting to storage via Internet Small Computer System Interface (iSCSI), Cisco recommends that you configure a separate VLAN on the switch and configure jumbo frame support as well as flow control. At a global level, jumbo frame support can be enabled with the following commands:

For the Cisco Catalyst 3750G:

```
system mtu jumbo [frame size 1500-9000]
```

For the Cisco Nexus 5000/2000:

```
policy-map jumbo
  class class-default
    mtu 9216
system qos
  service-policy jumbo 1
```

Step 2: iSCSI links can get very close to a full Gigabit per second of traffic and may trigger storm control on the switch. To prevent storm control from activating, enable the following command on all switch ports connecting to devices running iSCSI traffic.

For the Cisco Catalyst 3750G:

```
storm-control unicast level 100
```

Step 3: Flow control allows a congested host to send a pause to the transmitting host to temporarily stop data on the link without shutting down the interface. This allows the congested host to process traffic and catch up without dropping packets. If the server and iSCSI array support 802.3x flow control, the following command should be configured on the switchports with iSCSI traffic:

For the Cisco Catalyst 3750G:

```
flowcontrol receive on
```

For the Cisco Nexus 5000/2000:

```
flowcontrol receive on transmit on
```

Notes

Fibre Channel Data Center Design

Agency Overview

There is a constant demand for more storage in agencies today. Storage for servers can be physically attached or connected over a network. Direct Attached Storage (DAS) is physically attached to a single server and is difficult to use efficiently. Storage Area Networks (SANs) allow servers to share a pool of storage over a Fibre Channel or Ethernet network. This capability allows SAN administrators to easily expand storage capacity for servers supporting data-intensive applications.

Technology Overview

Fibre Channel allows servers to connect to storage across a fiber-optic network. Multiple servers can share a single storage array, and Fibre Channel allows a server to connect to storage across a data center or even a WAN.

The SBA Data Center design uses the Cisco 9124 Multilayer Fabric Switch (or Cisco MDS 9134 Multilayer Fabric Switch).

- The Cisco MDS 9124 switch is ideal for a small SAN fabric with up to 24 Fibre Channel ports.
- The Cisco MDS 9134 swtich can be trunked together with 10-Gbps ISL ports to grow the fabric to 64 ports of Fibre Channel SAN without having the large investment of a director-class switch.

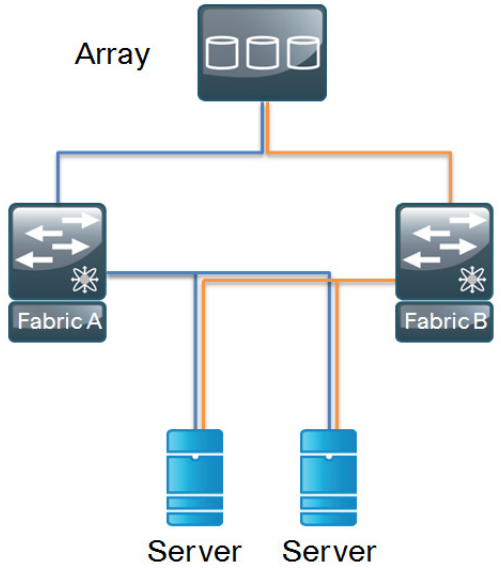
The Cisco MDS 9148 Multilayer Fabric Switch provides 48 line-rate 8-Gbps Fibre Channel ports and offers cost-effective scalability. The Cisco MDS 9148 switch was validated in the *Cisco SBA Data Center For Midsize Agencies Unified Computing Deployment Guide*. Please refer to this guide for more information on the Cisco MDS 9148 switch.

Dual Cisco MDS 9000 Family switches are deployed to create two separate physical fabrics and two distinct paths to storage. In a SAN, a fabric consists of servers and storage connected to a Fibre Channel switch (Figure 8). 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 host on a SAN connects to the Fibre Channel switch with 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

Figure 8. Fibre Channel Overview



iSCSI and Fibre Channel

Internet Small Computer System Interface (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. iSCSI has become a storage technology that is supported by most server, storage, and application vendors.

- The decision to use iSCSI or Fibre Channel depends on the application and performance requirements:
  - iSCSI fits for applications with lower-performance requirements as an access method to inexpensive bulk storage.
  - Fibre Channel provides higher performance and bandwidth to the storage and is good for applications that require a higher level of availability and performance.

Most agencies will have applications for both technologies.

Virtual Storage Area Networks (VSANs)

The 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 9000 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.

There are two types of zoning, initiator-based and port-based. 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. Port-based zoning depends on a physical switch port. If the cable from a host's HBA is moved to another port on the Cisco MDS 9000 switch, the device will no longer be in the correct zone and will not work properly. The SBA Data Center design uses initiator-based zoning because of its inherent ease-of-use benefits.

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: "server1-port1" instead of "10:00:00:00:c9:87:be:1c").

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 will vary with the Cisco MDS 9124 switch or Cisco MDS 9134 switch. Please consult the installation instructions from the specific storage vendor.

Tech Tip

Specific interfaces, addresses, and device aliases are examples from the lab. Your WWN addresses, interfaces, and device aliases will likely be different.

Process

Configuring the Cisco MDS 9124 or 9134 Switch

1. Complete the Initial Setup
2. Configure VSANs
3. Configure Ports
4. Configure Device Aliases
5. Configure Zoning
6. Troubleshoot the Configuration

Complete each of the following procedures to configure the Cisco MDS 9124 switch or MDS 9134 switch.

Procedure 1 Complete the Initial Setup

When initially powered on, a new Cisco MDS 9124 or 9134 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, Telnet, SSH, clock, time zone, Network Time Protocol, switch port modes, and default zone policies.

Tech Tip

When the administrative login is configured, a Simple Network Management Protocol Version 3 (SNMPv3) user is created automatically. This login is used by Cisco Fabric Manager to manage the switch.

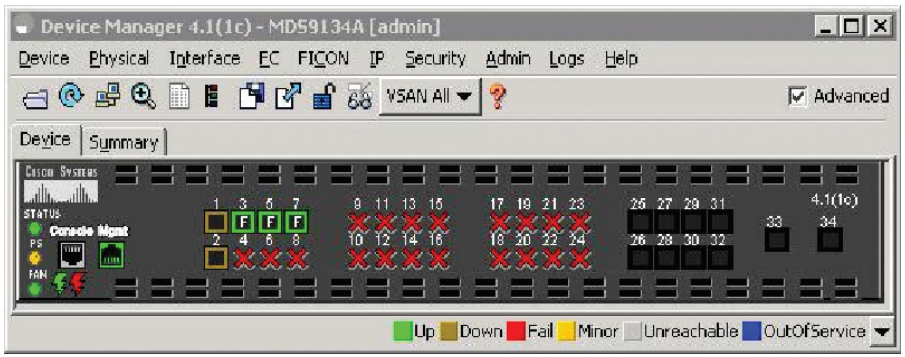
```
Enter the password for "admin":
Confirm the password for "admin":
---- Basic System Configuration Dialog ----
This setup utility will guide you through the basic
configuration of the system. Setup configures only enough
connectivity for management of the system.
Please register Cisco MDS 9000 Family devices promptly with
your supplier. Failure to register may affect response times
for initial service calls. MDS 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]
Configure read-only SNMP community string (yes/no): [n]
Configure read-write SNMP community string (yes/no): [n]
Enter the switch name: dc-1
Continue with Out-of-band (mgmt0) management configuration?
(yes/no): [y]
Mgmt0 IPv4 address: 192.168.128.114
Mgmt0 IPv4 netmask: 255.255.255.0
Configure the default gateway? (yes/no)[y]: [y]
IPv4 address of the default gateway: 192.168.128.1
Configure advanced IP options? (yes/no): [n]
Enable the telnet service? (yes/no): [y]
Enable the ssh service? (yes/no) [n]: y
Type of ssh key you would like to generate (dsa/rsa/rsa1): rsa
Number of key bits <768-2048>: 2048
Configure clock? (yes/no): [n]
Configure timezone? (yes/no) [n]: y
Enter timezone config: PST -8 0
Configure summertime? (yes/no) [n]: y
Sample config: PDT 2 sunday march 02:00 1 sunday november
02:00 59
summer-time config: PDT 2 sunday march 02:00 1 sunday november
02:00 59
Configure the ntp server? (yes/no) [n]: y
NTP server IPv4 address: 192.168.1.1
Configure default switchport interface state (shut/noshut)
[shut]: 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]
```

Tech Tip

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

Step 2: The Cisco MDS Device Manager (Figure 9) provides a graphical interface to configure a Cisco MDS 9000 Family switch. To access the Device Manager, connect to the management address via HTTP or access it directly through Cisco Fabric Manager.

Figure 9. Device Manager



Tech Tip

Cisco Fabric Manager is available for download from Cisco.com or from the CD that ships with the Cisco MDS 9000 Family switch.

Tech Tip

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

Procedure 2 Configure VSANs

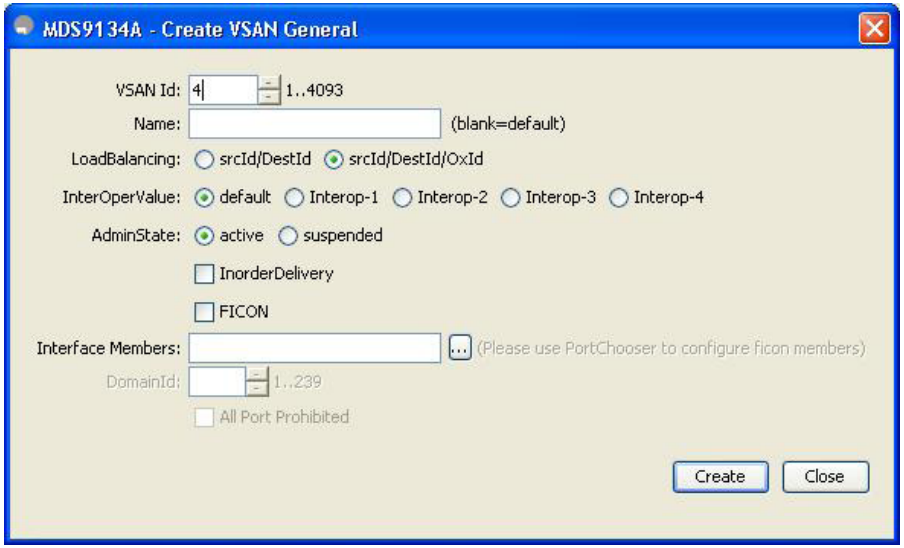
By default, all ports are assigned to VSAN 1 at initialization of the switch. It is a best practice to create a separate VSAN for production and to leave VSAN 1 for unused ports. By not using VSAN 1, you can avoid future problems with merging when combining other existing switches that may be set to VSAN 1. To create a VSAN, use the command-line interface (CLI) or Device Manager.

Step 1: To create VSAN 4 and add it to port FC1/4 with the name Finance, enter the following from the command line:

```
vsan database
   vsan 4 name "Finance"
   vsan 4 interface fc1/4
```

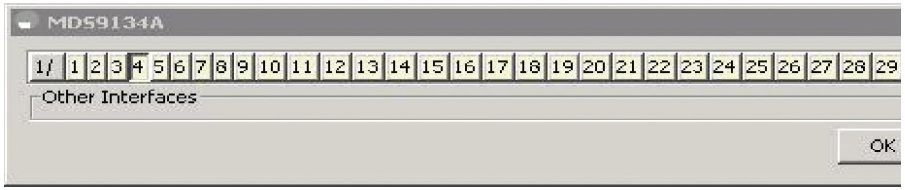
Using Device Manager, select **FC->VSANS**.

Figure 10. Create VSAN General Window



Step 2: Select the interface members by clicking ... after **Interface Members** (Figure 10). Figure 11 illustrates interface fc 1/4 being selected.

Figure 11. Other Interfaces Window



Step 3: Click **Create** to create the VSAN. You can add additional VSAN members in the **Membership** tab of the main VSAN window.

Tech Tip

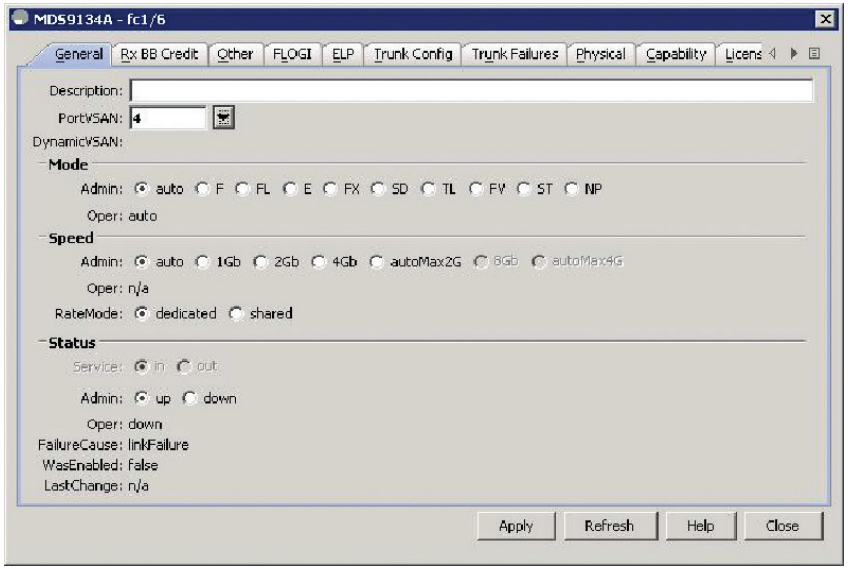
A seperate VSAN should be created for each fabric. Example: Fabric A has the Finance VSAN with the VSAN number 4, Fabric B would have the Finance VSAN number configured as VSAN 5.

Procedure 3 Configure 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.

Step 1: To change the port mode via Device Manager, right-click the selected port.

Figure 12. General Tab



Step 2: Connect devices to the Fibre Channel ports and activate the ports. When the initiator or target starts up, it automatically logs into the fabric. Upon login, the initiator or target WWN is made known to the fabric. To display this fabric login database, enter the following command through the Cisco MDS 9000 switch CLI:

```
show flogi database
--------------------------------------------------------------------------------
INTERFACE VSAN FCID PORT NAME NODE NAME
--------------------------------------------------------------------------------
fc1/3 4 0x830100 10:00:00:00:c9:87:be:1c
20:00:00:00:c9:87:be:1c
fc1/5 4 0x830000 10:00:00:00:c9:87:be:2a
20:00:00:00:c9:87:be:2a
fc1/7 4 0x830200 50:0a:09:82:89:2a:df:b1
50:0a:09:80:89:2a:df:b1
Total number of flogi = 3
```

Step 3: Add device aliases to map the long WWNs for easier zoning and identification of initiators and targets.

Procedure 4 Configure Device Aliases

To configure device aliases using the CLI, complete the following steps:

Step 1: Apply the following configuration:

```
device-alias database
device-alias name esx-12-hba0 pwwn 10:00:00:00:c9:87:be:1c
device-alias name esx-13-hba0 pwwn 10:00:00:00:c9:87:be:2a
device-alias name array0-a pwwn 50:0a:09:82:89:2a:df:b1
exit
device-alias commit
```

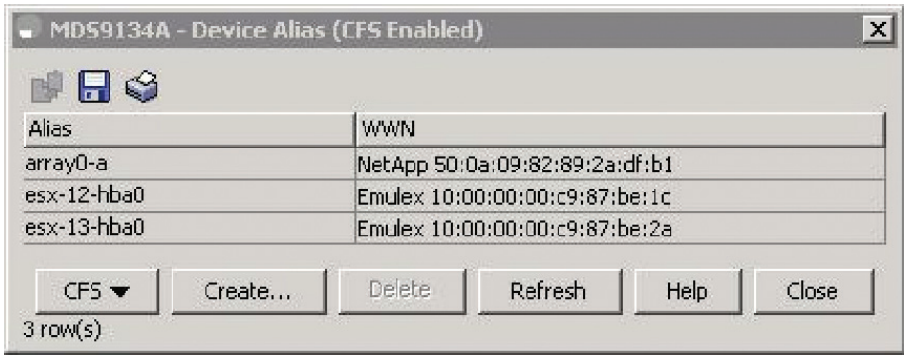
Step 2: Aliases are now visible when you enter the show flogi database command.

```
show flogi database
--------------------------------------------------------------------------------
INTERFACE VSAN FCID PORT NAME NODE NAME
--------------------------------------------------------------------------------
fc1/3 4 0x830100 10:00:00:00:c9:87:be:1c
20:00:00:00:c9:87:be:1c
[esx-12-hba0]
fc1/5 4 0x830000 10:00:00:00:c9:87:be:2a
20:00:00:00:c9:87:be:2a
[esx-13-hba0]
fc1/7 4 0x830200 50:0a:09:82:89:2a:df:b1
50:0a:09:80:89:2a:df:b1
[array0-a]
Total number of flogi = 3.
```

To configure device aliases with Device Manager, complete the following steps:

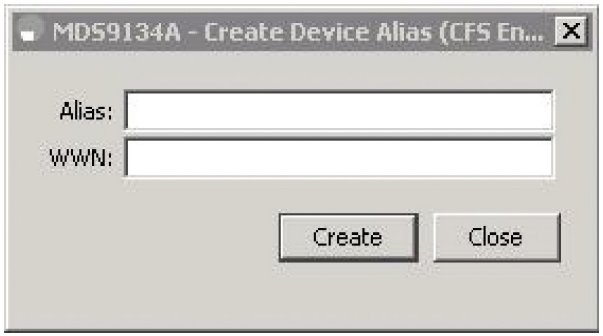
Step 1: Access the Device Aliases window.

Figure 13. Advanced > Device Aliases Window



Step 2: Click **Create**.

Figure 14. Create Device Alias Window



Step 3: Enter a device alias name and paste in or type the WWN of the host.

Step 4: Click **CFS->Commit** when complete.

Procedure 5 Configure Zoning

Zoning should be configured 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.

```
ESX3_HBA0_Array_0
ESX5_HBA1_EMC_B0_FC2
```

Limiting zoning to a single initiator with a single or multiple target helps prevent disk corruption and data loss.

To create a zone with the CLI, complete the following steps:

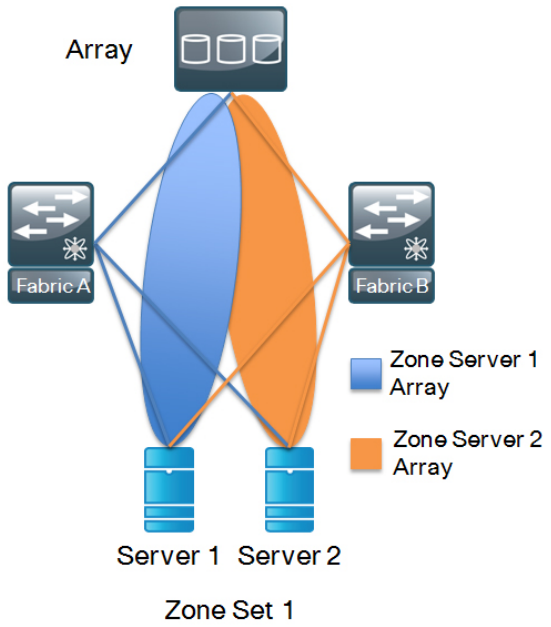
Step 1: Enter configuration mode, enter zone name (zone name), and enter vsan number (vsan number).

```
zone name esx-12-hba0_array0-a vsan 4
```

Device members can be specified by WWN or device alias.

```
member device-alias esx-12-hba0
member pwwn 50:0a:09:82:89:2a:df:b1
```

Figure 15. Zoning



Step 2: Create a zoneset. A zoneset is a collection of zones (Figure 15). Zones are added to the zoneset as members. Once all zones are added, the zoneset must be activated.

There can only be one active zoneset per VSAN.

```
zoneset name zoneset1 vsan 4
```

Step 3: To add members to the zoneset, enter the following commands.

```
member esx-12-hba0-Array0-a
member esx-13-hba0-Array0-a
```

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

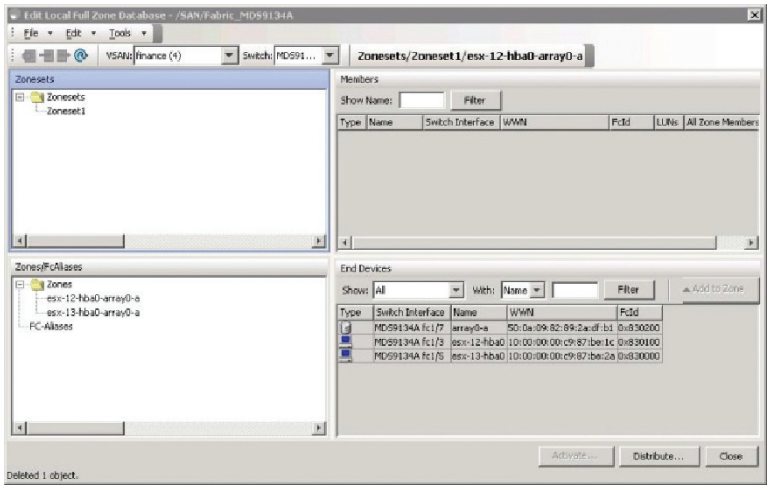
```
zoneset activate name Zone1 vsan 4
```

To configure zones and zoneset via Cisco Fabric Manager, complete the following steps:

Step 1: Select: **Zone Edit Local Full Zone Database** in the Cisco Fabric Manager menu.

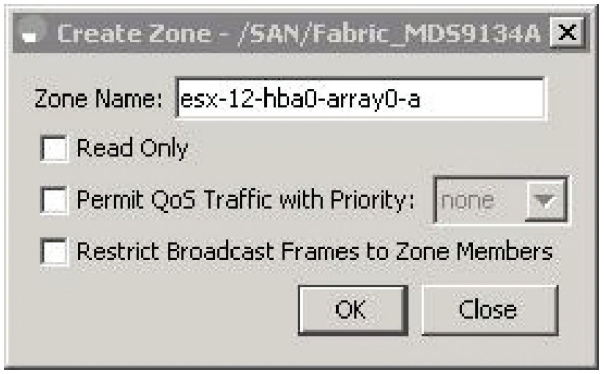
Step 2: On the left side of the zone database window are two sections, Zonesets and Zones. Across the top, the current VSAN and switch are displayed. The two sections on the right side list zones and zone members. To create a zone, right- click the zone folder to insert the zone.

Figure 16. Zone Edit Local Full Zone Database Window



Step 3: On the right pane, highlight initiator ortargets to add to the zone and click **Add to Zone**.

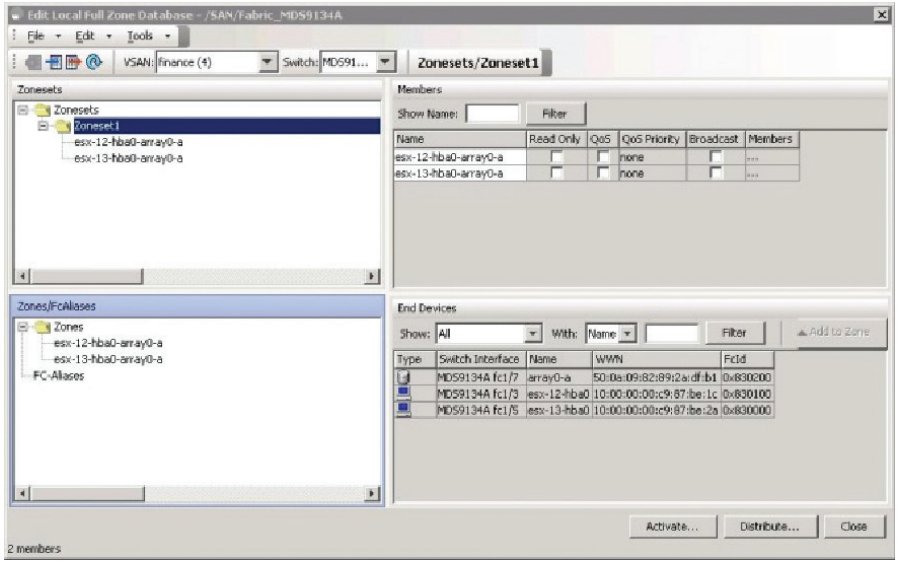
Figure 17. Create Zone Window



Step 4: Highlight the new zone and then add members to it on the right by clicking **Add to Zone**.

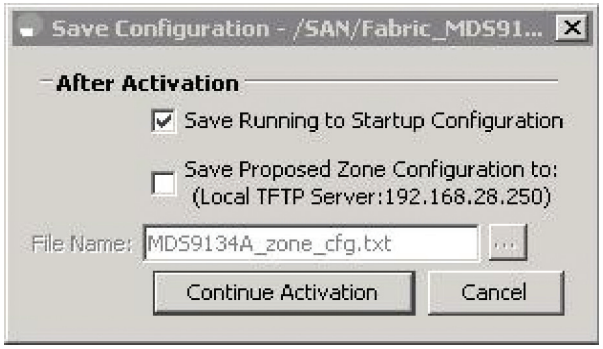
Step 5: Right-click **Zoneset** to insert a new zoneset. Drag zones just created from the zone box to the zoneset.

Figure 18. Zone Edit Local Full Zone Database Window



Step 6: To activate the configured zoneset, click **Activate** in the bottom right of the window.

Figure 19. Save Configuration Window



Procedure 6 Troubleshoot the Configuration

Step 1: To check the fabric configuration for proper zoning, use the **show zoneset active** command to display 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 MDS 9000 Family switch.

Step 2: 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.

```
show zoneset active
zoneset name zoneset1 vsan 4
  zone name esx-13-hba0-array0-a vsan 4
  * fcid 0x830000 [pwwn 10:00:00:00:c9:87:be:2a] [esx-13-hba0]
  * fcid 0x830200 [pwwn 50:0a:09:82:89:2a:df:b1] [array0-a]
zone name esx-12-hba0-array0-a vsan 4
  * fcid 0x830100 [pwwn 10:00:00:00:c9:87:be:1c] [esx-12-hba0]
  * fcid 0x830200 [pwwn 50:0a:09:82:89:2a:df:b1] [array0-a]
```

Step 3: Test Fibre Channel reachability using the **fcping** command and trace the routes to the host using the fctrace command.

Cisco created these commands to provide storage networking trouble-shooting tools that are familiar to individuals who use ping and traceroute. Examples are below:

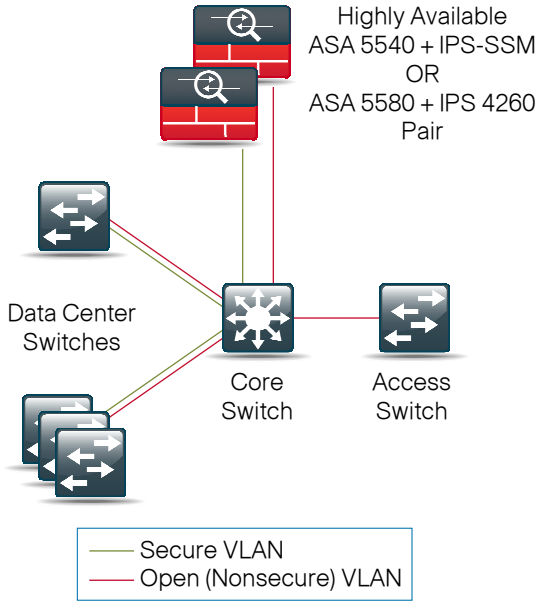
```
fcping dev esx-12-hba0 vsan 4
28 bytes from 10:00:00:00:c9:87:be:1c time = 758 usec
28 bytes from 10:00:00:00:c9:87:be:1c time = 675 usec
28 bytes from 10:00:00:00:c9:87:be:1c time = 674 usec
28 bytes from 10:00:00:00:c9:87:be:1c time = 666 usec
28 bytes from 10:00:00:00:c9:87:be:1c time = 680 usec

5 frames sent, 5 frames received, 0 timeouts
Round-trip min/avg/max = 666/690/758 usec

fctrace device-alias esx-12-hba0 vsan 4
Performing path discovery.
Route present for: 10:00:00:00:c9:87:be:1c
20:00:00:0d:ec:cd:21:c0(0xfffc83)
```

Security Data Center Design

Agency Overview

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

Figure 20. Secure Data Center Overview

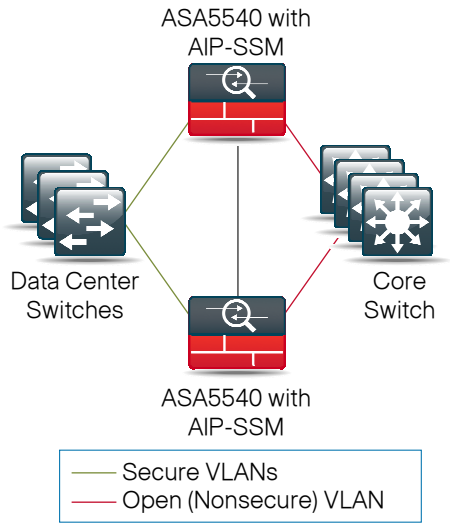


To protect the valuable electronic assets located in the data center, network security assures the facility is protected from automated or intentional snooping and tampering, and prevents compromise of hosts by resource-consuming worms, viruses, or botnets. Data center security must integrate with the agency's disaster-recovery strategy to enable the expected level of data-resource availability. Security policy must not interfere with access to data at the disaster recovery (DR) site during unavailability of the HQ site, or hinder data replication to the DR site.

Technical Overview

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 error carried out within the agency's network. To minimize the impact of unwanted network intrusions, firewalls and intrusion prevention systems (IPSs) should be deployed between clients and centralized data resources.

Figure 21. Cisco ASA 5540 and AIP-SSM



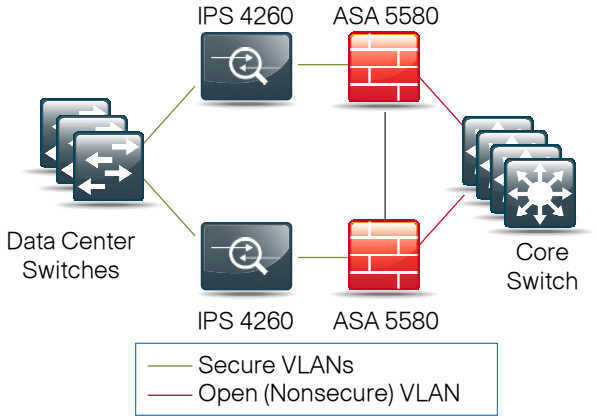
This design employs a pair of Cisco Adaptive Security Appliance (ASA) 5500s for data center firewall security. There are two different security configurations, differentiated by the scale and performance requirements that they must address.

The lower-scale, lower-performance configuration applies a pair of Cisco ASA 5540 appliances, each including an integrated IPS module; the Cisco Adaptive Inspection Prevention Security Service Module (AIP-SSM), which provides up to 650 Mbps of firewall throughput (Figure 21).

The larger-scale, higher-performance configuration consists of a pair of

Cisco ASA 5580-20s, each connected directly to a Cisco IPS 4260 appli-ance. This configuration offers up to 5 Gbps of firewall throughput. The IPS 4260s in this design support 1-2 Gbps of throughput. If higher IPS through-put is needed, additional IPS 4260s could be applied to Gigabit inter¬faces on the ASA 5580 or the IPS could be upgraded to the IPS 4270s that offer 2-4 Gbps of throughput (Figure 22).

Figure 22. Cisco ASA 5580 and IPS 4260



In both cases, the pair of ASAs is configured for active and standby high availability to ensure that access to the server room's centralized data is minimally impacted by outages caused by software maintenance or hard-ware failure.

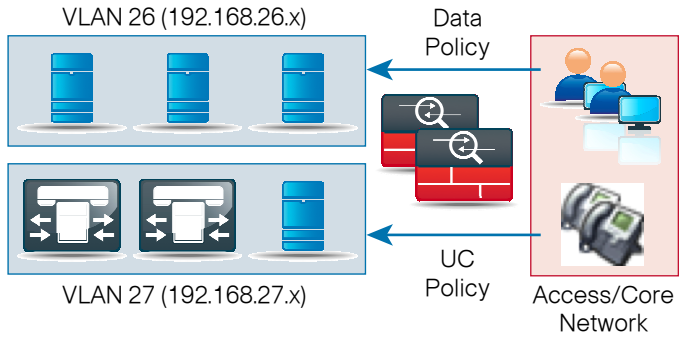
The Cisco ASAs are configured in routing mode for greatest capabilities; as a result, the secure network must be in a separate subnet from the client subnets. The transparent-mode capability on the ASA could be employed to simplify IP subnet allocation, however, this would result in diminished security capability.

The data center IPSs monitor for and mitigate potential malicious activity not filtered by the security policy defined on the ASAs. The IPS sensors are deployed in promiscuous intrusion detection system (IDS) mode so that they only monitor and log abnormal traffic. As a more advanced option, they can be deployed in line to fully engage their intrusion prevention capabilities, wherein they mitigate traffic that violates the configured policy.

Security Topology Design

The network defines two secure VLANs in the data center. The number of secure VLANs is arbitrary, and was built as an example of how to create multiple secured networks to host services that require separation. High-value applications such as Enterprise Resource Planning (ERP), Customer Relationship Management (CRM), and finance may need to be separated from other applications, so you may wish to segregate those applications into their own VLAN (Figure 23).

Figure 23. Multiple Secure Networks



As another example, services that are indirectly exposed to the Internet (via a proxy in the Demilitarized Zone (DMZ)) should be separated from other services, if possible, to prevent Internet-borne compromise of some serv-ers 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.

Process

Configuring Security Features

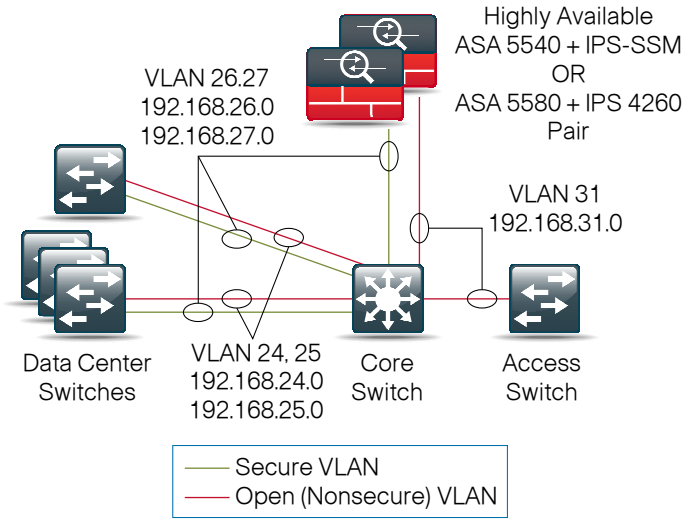
1. Configure VLANs
2. Configure the ASA Pair
3. Configure the ASA and IPS for Active-Standby High Availability

Complete the following procedures to configure the security features.

Procedure 1 Configure VLANs

VLAN trunks connect the ASA and IPS appliances to the core and server switches. One Gigabit Ethernet port per ASA is configured with a subinterface for each secured subnet. This interface is then assigned an IP address, which will be the default gateway for the subnet. The core switch VLAN interface does not have an IP address assigned as it does for most of the other VLANs (Figure 24).

Figure 24. Secure Data Center Connections



Step 1: Enter the following text at the command line to configure the VLAN:

```
interface GigabitEthernet0/0.26
  vlan 26
  nameif DCVLAN26
  security-level 100
  ip address 192.168.26.1 255.255.255.0 standby 192.168.26.2
!
interface GigabitEthernet0/0.27
  vlan 27
  nameif DCVLAN27
  security-level 100
  ip address 192.168.27.1 255.255.255.0 standby 192.168.27.2
```

Step 2: Each VLAN carries only one secure subnet. Configure the switch ports that connect to the security appliances in the same secure VLANs as servers and other appliances in the data center.

Tech Tip

The ASA 5580 is configured with several more interfaces, and does not use a trunk to connect to the data center VLANs. Be sure to review the ASA 5580 configuration in the *Cisco SBA for Midsize Agencies—Borderless Networks Foundation Configuration Files Guide* to note differences in interface numbers, and lack of VLAN trunking on the Gigabit Ethernet ports.

Step 3: Add the VLANs to the core switch ports that connect to the security appliances:

```
interface GigabitEthernet3/0/10
  description ASA5540DC
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 1,26,27
  switchport mode trunk
  srr-queue bandwidth share 10 10 60 20
  queue-set 2
  priority-queue out
  mls qos trust cos
  auto qos voip trust
  spanning-tree link-type point-to-point
```

Step 4: Configure the same VLANs on trunk ports and port channels connected to blade server switches, servers, or standalone appliances.

```
interface Port-channel15
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 1,24-27
  switchport mode trunk
```

Tech Tip

Standalone appliances or servers will typically connect to access ports, while virtualized hosts will usually need to connect to trunk ports to allow access to multiple VLANs.

Procedure 2 Configure the ASA Pair

Because the ASAs are the gateway to the secure VLANs in the server room, the ASA pair must be configured to participate in the network's EIGRP updates to advertise the connected secure subnet into the LAN. This way, the servers connected to the secure VLAN will be reachable.

Step 1: Enter the following text at the command line to configure the ASA pair:

```
router eigrp 1
  no auto-summary
  network 192.168.26.0 255.255.255.0
  network 192.168.27.0 255.255.255.0
  network 192.168.31.0 255.255.255.0
  passive-interface DCVLAN26
  passive-interface DCVLAN27
```

Procedure 3 Configure Active-Standby High Availability

The ASA and IPS appliances are configured for Active-Standby High Availability. When 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.

Step 1: Configure one interface on each ASA as the state-synchronization interface that the ASAs use to share configuration updates, determine which device is active in the high-availability (HA) pair, and exchange state information for active firewall sessions.

```
interface GigabitEthernet0/2
  description LAN/STATE Failover Interface
!
failover
failover lan unit primary
failover lan interface failover GigabitEthernet0/2
failover polltime unit msec 200 holdtime msec 800
failover polltime interface msec 500 holdtime 5
failover key [key]
failover replication http
failover link failover GigabitEthernet0/2
failover interface ip failover 192.168.36.1 255.255.255.252
standby 192.168.36.2
```

The **failover key** value must match on the two devices that are configured in the active-standby HA pair. This key is used for two purposes: to authenticate the two devices to each other when the tunnel is established, and to secure state synchronization messages between the devices that enable the ASA pair to maintain service for existing connections when the standby ASA becomes primary. The two lines of the configuration that begin with **failover polltime** reduce the failover timers from the defaults to achieve subsecond failover. Improved failover times reduce application and user impact during outages. Reducing the failover timer intervals below these values is not recommended.

Process

Defining a Firewall Policy

1. Configure a Whitelist Security Policy
2. Troubleshoot the Whitelist Policy Development Process
3. Configure a Blacklist Security Policy

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

To effectively deploy security between the various functional segments of an agency'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 an agency's application traffic and performance requirements while optimizing security.

Network security policies can be broken down into two basic categories: "whitelist" policies and "blacklist" policies.

A whitelist policy offers a more implicit security posture, blocking all traffic except that which must be allowed (at a sufficiently granular level) to enable applications.

While simpler to maintain and less likely to interfere with network applications, a blacklist policy offers somewhat less security. The only traffic that is blocked is that which specifically poses the greatest risk to centralized data resources.

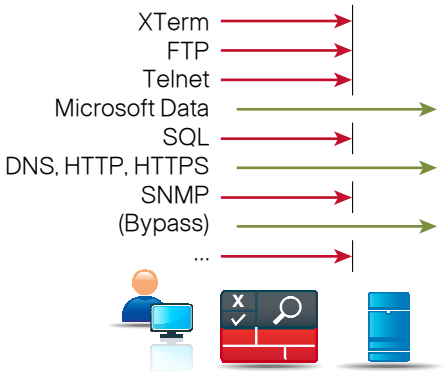
A whitelist policy is the best-practice option if you have the opportunity to examine the network's expectations and adjust the policy to avoid interfering with network activity.

Whether you choose a whitelist or blacklist policy basis, IDS or IPS deployment should be considered to control 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. In the best circumstances, IPS may be able to 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 that a network is subject to (for example, PCI 2.0).

While a detailed examination of regulatory compliance considerations exceeds the scope of this document, you should include regulation in your network security design. Noncompliance may result in regulatory penalties.

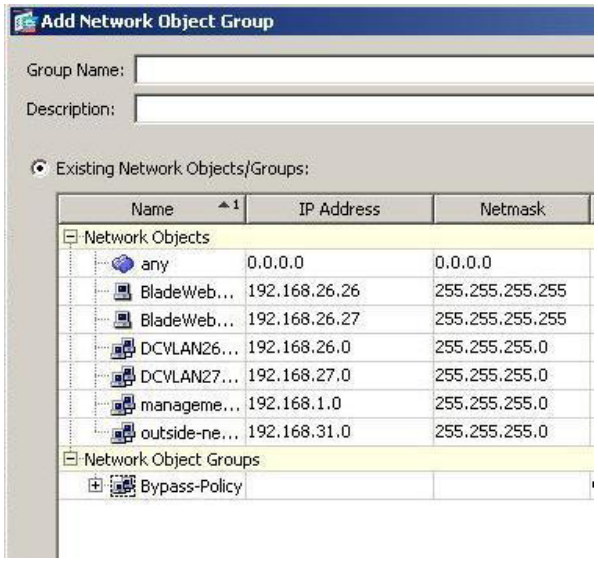
A whitelist security policy is generally better positioned than a blacklist security policy to meet regulatory requirements because only traffic that must be allowed for agency operations is allowed. Other traffic is blocked and does not need to be monitored to assure that unwanted activity is not occurring. This reduces the volume of data that will be forwarded to the IDS or IPS, and minimizes the number of log entries that must be reviewed in the event of an intrusion or data loss.

Figure 25. Whitelist Security Policy



This section will introduce examples of various types of access policies allowed between the user network and server room resources. The various policies are constructed using the building-block concepts of ASA object groups, which identify the applications that are accessed (service group) and the hosts that carry these applications (network group), and tie access to the individual hosts to the service definition. By defining hosts individually as network objects, hosts can be added to and removed from the various policy groups to enable and disable access to the various hosts' services. A last-case bypass rule will be defined to allow wide-open access to hosts that are assigned to the bypass object group.

Figure 26. Add Network Object Group Window



Tech Tip

The bypass rule group is available for troubleshooting, or to provide temporary access to services on the host that must be opened for maintenance or service migration.

Procedure 1 Configure a Whitelist Security Policy

Security policy configuration is fairly arbitrary to suit the policy and management requirements of an agency. Thus, examples here should be used as a basis for your network's security requirements.

Step 1: To effectively define a whitelist security policy, answer these questions:

- What applications will be used on the network?
- Can their 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 DR site?

A blacklist policy that blocks high-risk traffic offers a lower-impact, but less-secure option (as compared to a whitelist policy) in cases where you are unable to pursue a detailed study of the network's application activity or if the network does not allow you to support application troubleshooting.

Step 2: A basic data-service policy can be configured to allow common services such as HTTP, HTTPS, and DNS, and some other services typically seen in Microsoft-based networks. Enter the following configuration to control access so only specific hosts may be accessed:

```
name 192.168.26.0 Secure-Subnets
!
object-group network Application-Servers
 description HTTP, HTTPS, DNS, and MSExchange
 network-object host BladeWeb1Secure
 network-object host BladeWeb2Secure
!
object-group service MS-App-Services
 service-object tcp eq domain
 service-object tcp eq www
 service-object tcp eq https
 service-object tcp eq netbios-ssn
 service-object udp eq domain
 service-object udp eq nameserver
 service-object udp eq netbios-dgm
 service-object udp eq netbios-ns
!
access-list outside_access_in extended permit object-group MS-
App-Services any object-group Application-Servers
!
access-group outside_access_in in interface outside
```

Step 3: IT management staff may need specific access to certain resources; in this example, we allow access to SSH and SNMP. To control this, we allow access to a specific host address range (in this example, 192.168.31.224-255) that is managed with DHCP.

```
name 192.168.26.0 Secure-Subnets
name 192.168.31.224 Mgmt-host-range description Address pool
for IT users
!
object-group service Mgmt-traffic
 service-object tcp eq ssh
 service-object udp eq snmp
!
access-list outside_access_in extended permit object-group
Mgmt-traffic Mgmt-host-range 255.255.255.224 Secure-Subnets
255.255.254.0
!
access-group outside_access_in in interface outside
```

Step 4: A more flexible design for management-network access applies cut-through proxy access control through the ASA to the management network. Cut-through proxy provides the capability to restrict access to hosts via a firewall policy that only permits users that present valid authentication credentials. This policy prevents unwanted users from gaining access to specific hosts or services.

As mentioned earlier, the 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.

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

```
name 192.168.26.26 BladeWeb1Secure
name 192.168.26.27 BladeWeb2Secure
!
object-group network Bypass-Policy
 description Open Policy for Server Access
 network-object host BladeWeb1Secure
 network-object host BladeWeb2Secure
access-list outside_access_in extended permit ip any object-
group Bypass-Policy
access-group outside_access_in in interface outside
```

Procedure 2 Troubleshoot Whitelist Development

Whitelist policy development can be challenging. The following steps will help you refine and improve your initial attempt.

Step 1: If you find that identifying all of the access that must be allowed to the secure VLANs is very difficult, you might want to log all traffic that is handled by the deny action at the end of the rule set. This will allow you to see all of the traffic that you have not explicitly dealt with that needs an explicit firewall term.

Step 2: Another troubleshooting or development option is to assign the whole subnet to the bypass rule and enable logging so that anything that is not handled by an explicit rule will be permitted and applications will function properly. You will be able to track their activity from the logs and define specific rules to handle the applications' requirements.

Procedure 3 Configure a Blacklist Security Policy

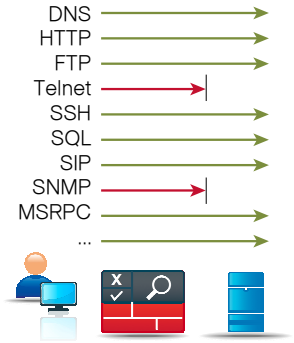
If your agency does not have the desire or resources to maintain a granular, restrictive policy to control access between centralized data and the user community, a simpler, easy-to-deploy policy that limits only the highest-risk traffic may be more attractive.

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.

By leaving the majority of the network access open, the server room's resources are exposed to compromise.

When using a less-restrictive policy for data access between the user network and the server room, IDS or IPS should be strongly considered to minimize the likelihood of data security compromise, or to at least offer a forensic trail in the event data tampering or loss is discovered. Applying IPS properly will reduce the likelihood of unwanted network activity.

Figure 27. Blacklist Security Policy

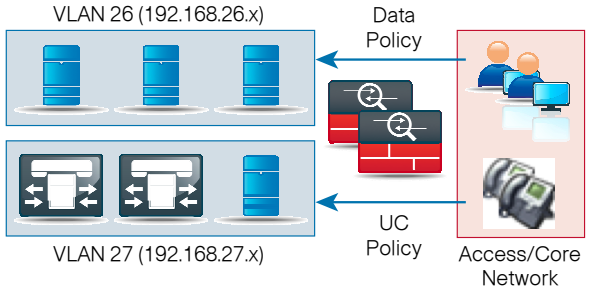


If you decide to apply a blacklist policy, you may still wish to configure a specific policy to protect voice-over-IP (VoIP) server resources, as recommended by the Cisco Voice Technology Group.

If you choose to implement a separate Unified Communications (UC) policy for traffic, you may wish to partition UC resources on their own separate VLAN.

For example: You could deploy your desktop data resources on VLAN 26, and put UC resources in VLAN 27 as shown below.

Figure 28. UC Resource Separation



The following policy description includes a discussion of an optional policy for VLAN 27 that provides this type of compartmentalization.

The policy presented here allows all requests from the core to access the server room services, except for a few specific services. It blocks Telnet connection requests and SNMP queries, which are connection services that tend to be used for management traffic, and are typically not needed by network users. Although you might use Telnet for terminal emulation services, SSH is a better choice as user information, such as passwords, and other application data is carried across the network in an encrypted form to be concealed from unwanted onlookers.

Step 1: Network administrative users may need to issue SNMP queries from desktop computers to monitor network activity. The first portion of the policy explicitly allows SNMP queries for a specific address range that will be allocated for IT staff. Enter the following commands:

```
name 192.168.26.0 Secure-Subnets
name 192.168.31.224 Mgmt-host-range description Address pool
for IT users
access-list outside_access_in remark Access from mgmt-host
pool to both secure subnets via ssh and snmp.
access-list outside_access_in extended permit udp Mgmt-host-
range 255.255.255.224 Secure-Subnets 255.255.254.0 eq snmp
```

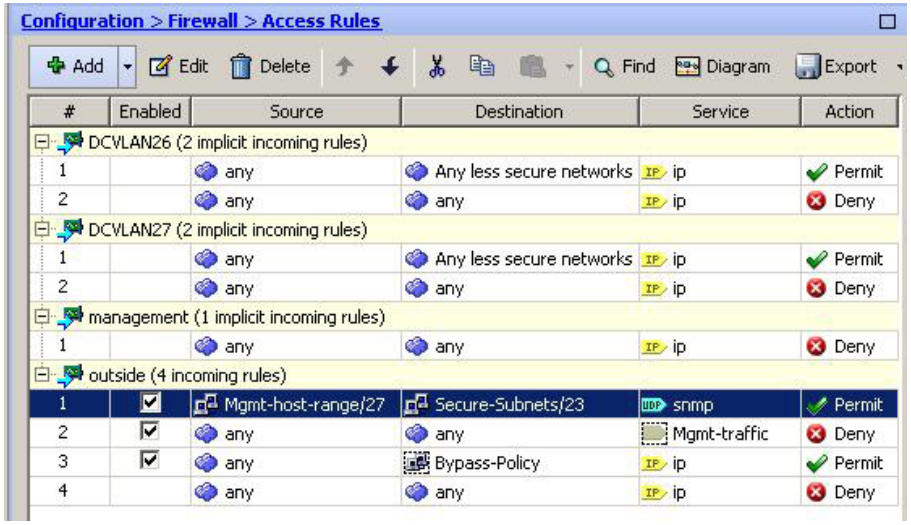
Step 2: Block Telnet and SNMP with the following command:

```
object-group service Mgmt-traffic
  service-object tcp eq ssh
  service-object udp eq snmp
access-list outside_access_in 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.

```
access-list outside_access_in extended permit ip any object-
group Bypass-Policy
log disable
```

Figure 29. Policy configuration in ASDM



Process

Deploying an Intrusion Protection System (IPS)

1. Complete Initial Configuration
2. Complete Basic Configuration
3. Define and Tune the IPS Policy
4. Configure IPS Signature Updates
5. Configure IDS or IPS Event Monitoring
6. Troubleshoot the IPS

From a security standpoint, intrusion prevention systems are complementary to firewalls. This is due to the fact that firewalls are generally access-control devices and are built to block access to an application. In this way, a firewall can be used to remove access to a large number of application ports, reducing the threat to the servers. IPS watches network and application traffic that is permitted to go through the firewall looking for attacks. If it detects an attack, the traffic is blocked, preventing the attack and sending an alert to inform the agency about the activity. IDS is similar to IPS except that it just provides alerts and does not block attacks.

Promiscuous versus Inline

There are two primary deployment options when using IPS devices, promiscuous (IDS) or inline (IPS). There are specific reasons for each deployment model based on risk tolerance and fault tolerance. In an IPS deployment, the device sits in the actual network packet flow and inspects the real packets. With IDS, the device inspects only copies of packets which prevents it from being able to stop a malicious packet when it sees one.

The advantage IPS mode offers is that the sensor, when it detects malicious behavior, can simply drop it. This allows the IPS device a much greater capacity to actually prevent attacks. An IDS box has to try and utilize another inline enforcement device to drop it. This means that for things like single-packet attacks (slammer over User Datagram Protocol [UDP]) an IDS could not prevent the attack from occurring. However, an IDS can be of great value when identifying and cleaning up infected hosts. The disadvantage for IPS mode is that, because it is an inline device, it needs to be able to keep up with the traffic load on the network, including handling bursts.

Reasons for using IDS:

- No impact to the network (latency, availability)
- Easier to deploy than IPS (no network changes)

Reasons for using IPS:

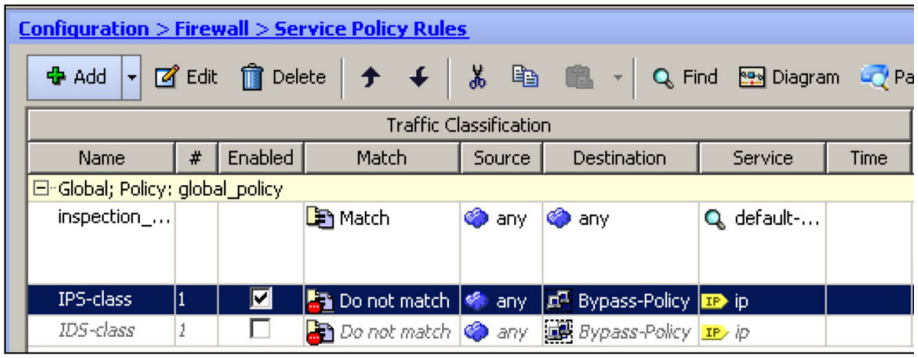
- Higher security than IDS (ability to drop bad packets)
- Reduced false positives and false negatives

For the headquarters design using ASA 5540 and ASA-SSM, two global policies were built:

- One for IPS that is enabled and sends all traffic to the SSM module in inline IPS mode, except for traffic designated as bypass traffic.
- The other is an IDS policy that is currently disabled and sends all traffic to the SSM module in promiscuous IDS mode, except for traffic designated as bypass traffic.

An agency may choose an IPS or IDS deployment, depending on regulatory and application requirements. Cisco recommends that you start with an IDS or promiscuous design for initial deployment and then move to IPS once the traffic profile at the deployment is known and the agency is comfortable that no production traffic will be affected. The primary reason for using IPS is that the sensor blocks malicious activity instead of just alerting (Figure 30).

Figure 30. Service Policy Rules



IPS Deployment Options

As described in the previous section, the two methods for deploying Cisco IPS are inline (IPS) where the sensor is in the actual packet flow or promiscuous mode (IDS) where the sensor sees copies of the packets.

Beyond that, other deployment options for inline IPS mode are defined by how the device is put into the traffic flow. The appliance version of the IPS has two inline options (Figure 31):

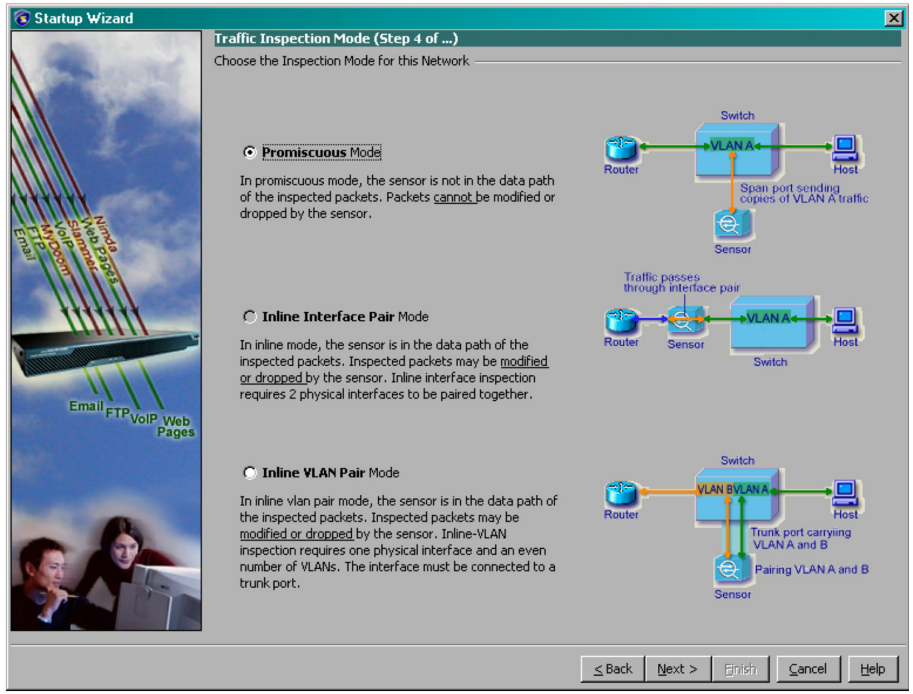
- VLAN pairing where traffic comes in and out of the IPS on the same physical interface. This requires a trunk port on the attached device because the sensor will move packets in the specified VLAN pair from VLAN X to VLAN Y and conversely.
- Interface pairing mode where traffic comes to the sensor on one physical interface and leaves on another. This type of deployment acts most like a physical wire.

While very similar in features and functionality, Cisco IPS appliances and modules for the ASA have some important differences.

- The Cisco ASA cannot be placed out-of-band while watching a monitor port passing the packets directly to the SSM module for analysis. It must sit inline in the traffic flow.
- The AIP-SSM module works on the traffic either in IPS or IDS mode depending on the configuration.

This configuration difference on the ASA allows you to easily move the AIP-SSM module from inline (IPS) to promiscuous mode (IDS) by changing the configuration on the ASA. Because the appliance is not part of a hosted chassis that controls packet flow, the configuration requires a few more steps to move from inline to promiscuous. These steps generally involve some cabling changes and switch configurations to set up the actual monitor port. Because of the physical differences, the appliance can more easily do multiple things at the same time, such as IDS inspection in front of the firewall and IPS inspection behind the firewall, or IDS in one network and IPS in an entirely different network.

Figure 31. Traffic Inspection Mode Map



Reader Tip

A discussion about how traffic moves through the ASA/AIP-SSM combination can be found here:

Procedure 1 Complete Initial Configuration

The first step in configuring an IPS sensor is to use the console to access the sensor or use the session command from the ASA to set up basic networking information such as IP address, gateway, access lists to allow remote access, etc. Once these critical pieces of data are entered, the rest of the con¬figuration is easily accomplished using a GUI tool like IPS Manager Express, IPS Device Manager, or ASA Device Manager.

Step 1: Gain access to the 4260 console by following the directions in this link: http://www.cisco.com/en/US/docs/security/ips/7.0/configuration/guide/cli/cli_logging_in.html#wp1032737

Alternatively, access the 4260 console from the ASA CLI by entering the following command:

```
DC_ASA_5540a# session 1
```

Step 2: After you gain access, login to the IPS device is required. The default username and password is cisco/cisco, and the password must be changed after the first login.

Step 3: After login, enter the setup command as follows:

```
sensor# setup

--- 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

Setup Configuration last modified: Mon Oct 12 23:22:27 2009

Enter host name [sensor]: DC_SSM_b
Enter IP interface [192.168.1.62/24,192.168.1.250]:
192.168.1.62/24,192.168.1.250
Modify current access list? [no]: yes
Current access list entries:
  No entries
Permit: 0.0.0.0/0
Permit:
Use DNS server for Global Correlation? [no]:
Use HTTP proxy server for Global Correlation? [no]:
Modify system clock settings? [no]:
Participation in the SensorBase Network allows Cisco to
collect aggregated statistics about traffic sent to your IPS.
SensorBase Network Participation level? [off]:

The following configuration was entered.

service host
network-settings
host-ip 192.168.1.62/24,192.168.1.250
host-name DC_SSM_b
telnet-option disabled
access-list 0.0.0.0/0
ftp-timeout 300
no login-banner-text
dns-primary-server disabled
dns-secondary-server disabled
dns-tertiary-server disabled
http-proxy no-proxy
exit
time-zone-settings
offset 0
standard-time-zone-name UTC
exit
summertime-option disabled
ntp-option disabled
exit
service global-correlation
network-participation off
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>.
```

Procedure 2 Complete Basic Configuration

Once the setup is complete, you can continue configuration using IPS Manager Express (IME) or ASDM.

The basic steps to configuring a sensor after running setup are:

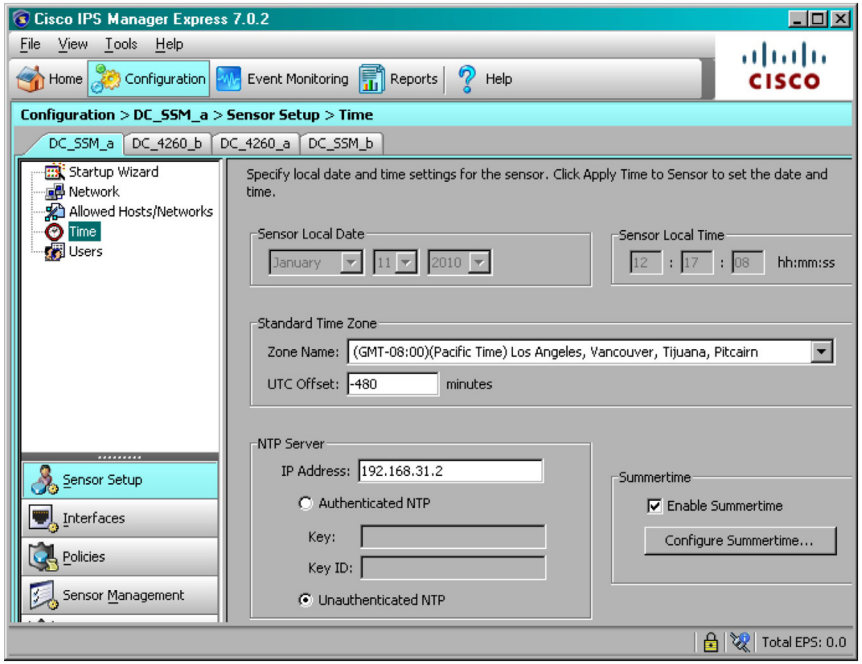
- Configure time settings
- Enable interfaces
- Build interface pairs or VLAN pairs
- Assign interfaces to virtual sensors

Step 1: To configure the time settings, access **Sensor Setup** >**Time** (for both appliances and AIP SSMs). From there, configure the timezone, summertime, and NTP server for the device (Figure 32).

Tech Tip

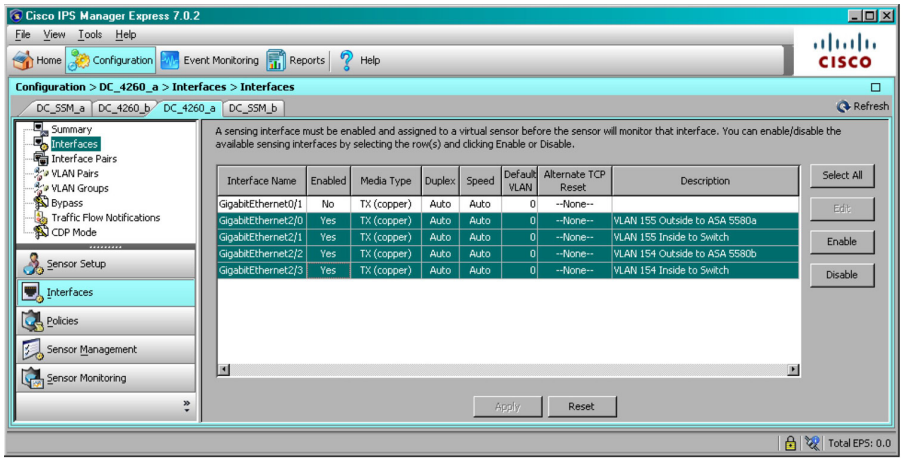
Modules get their base time from their hosting chassis on bootup, but use NTP to keep that time correctly synced. Generally a reboot is needed after changing timezone or summertime settings (Figure 32).

Figure 32. Time Window



Step 2: Enable the interfaces by accessing **Interfaces** > **Interfaces** and enabling the interface needs for IPS inspection use. This step is for appliances only and is not applicable on the AIP SSM since it uses a backplane interface that only connects the base ASA chassis (Figure 33).

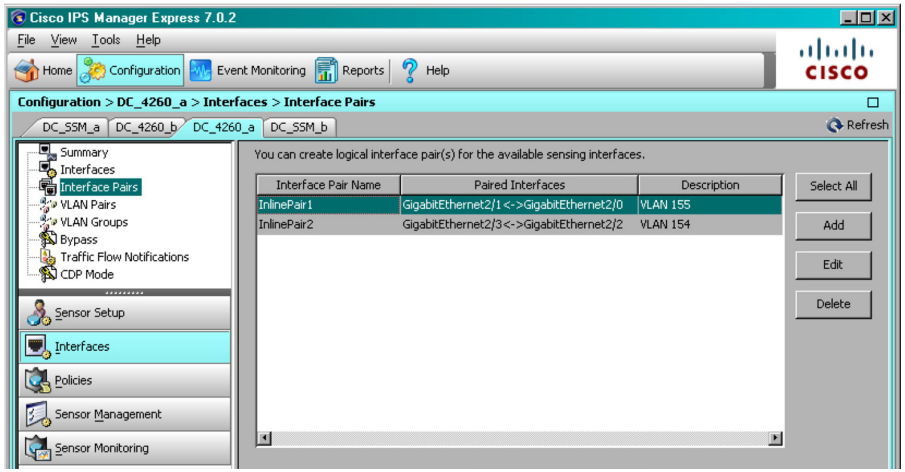
Figure 33. Interfaces Window



Step 3: To build interface pairs, access **Interfaces** > **Interface Pairs** or **VLAN Pairs** (for appliances only). (Figure 34)

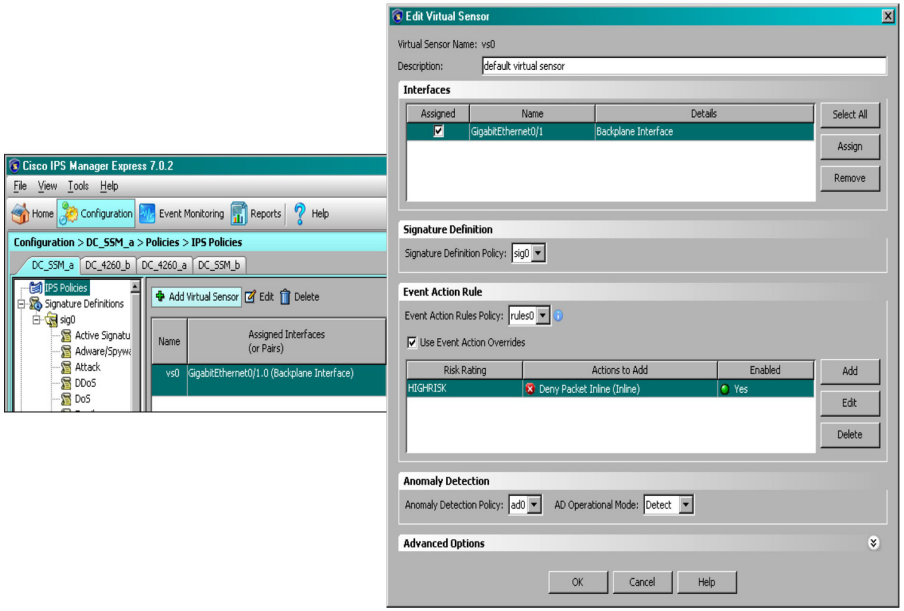
Depending on the deployment model required for the sensor, you need to create interface pairs to pair physical interfaces, or pair up VLANs on the same physical interface to allow traffic to flow through the sensor. In the DR site on the 4260, interface pairing was used and two pairs were created, which allowed one interface pair to be used for ASA interface DCVLAN154 and one pair for interface DCVLAN155.

Figure 34. Interface Pairs Window



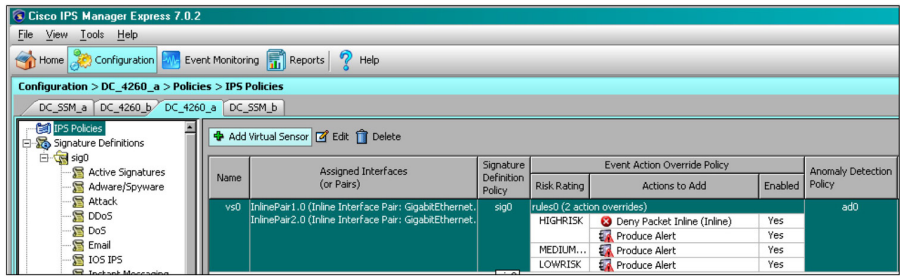
Step 4: To assign interfaces to virtual sensors, access **Policies->IPS Policies** (this applies to all devices). For each module, edit the existing virtual sensor policy to assign the backplane interface (the only interface) to the virtual sensor, click **OK** and **Apply**. (Figure 35)

Figure 35. IPS Policies Window



Step 5: For each appliance, assign the interfaces you built in Step 3 to the virtual sensor for inspection (Figure 36).

Figure 36. Policies > IPS Policies



Procedure 3 Define and Tune the IPS Policy

By default, Cisco IPS has an Event Action Override configured to deny any attack that has a risk rating of 90 or higher. This allows the sensor to block a fairly substantial percentage of the most serious attacks with signatures that are out-of-the-box accurate. Make policy changes on the sensor while it is possible to do this on a case-by-case basis. It is far easier to do this using the Policy table or the Event Action Rules.

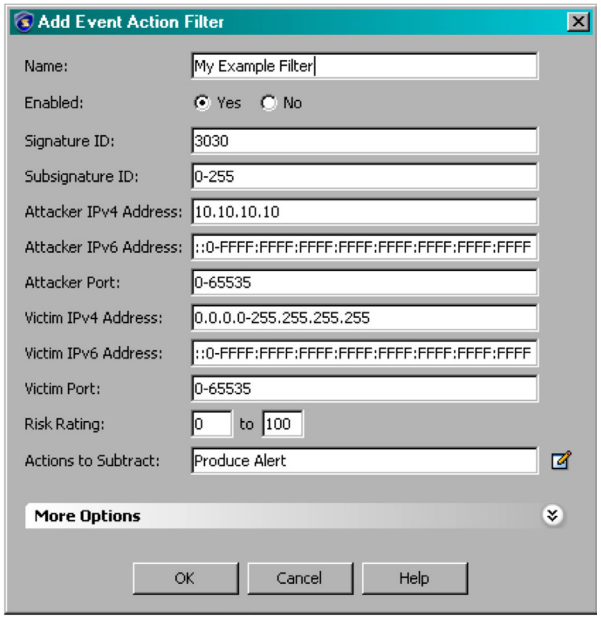
By simply changing the Event Action Rules from 90–100:

- At 100, you have changed the policy on the sensor so that only the most accurate and highest-severity signatures will take default deny packet actions on the sensor.
- At 85 or even 80–100, you have increased the range of events the sensor blocks by default. This makes the sensor's behavior more aggressive, blocking more attacks, but also possibly blocking a small amount of legitimate traffic if the sensor has not been tuned to the environment it operates in.

Tuning is a big topic and is covered in depth in other documents. Understand that tuning is a process rather than a one-time event. In general, you will need to look at events being triggered and determine if they are interesting or accurate. If not, then there are a number of steps you can take to lessen their impact.

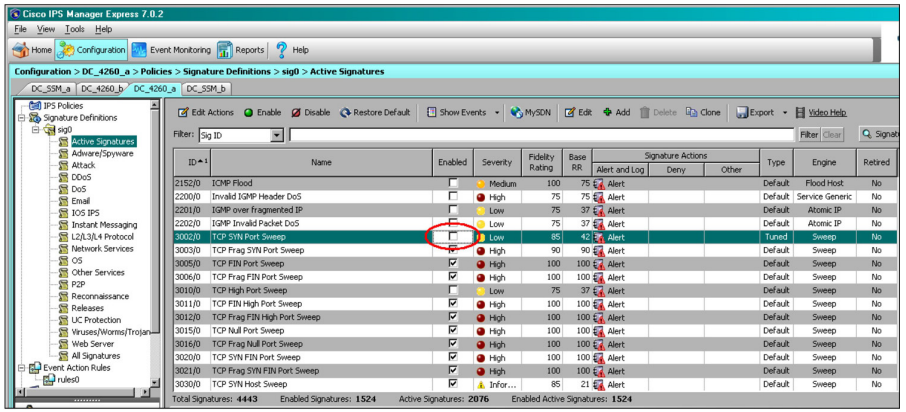
Step 1: Use Event Action Filters to remove an action on an event (or even the act of producing the alert in the first place). (Figure 37)

Figure 37. Add Event Action Filter



Step 2: Disable or retire a signature or remove an action from the signature-specific settings. This prevents the signature from triggering (retiring also prevents it from taking up resources, but it takes longer to bring it back online if needed later). (Figure 38)

Figure 38. Active Signatures

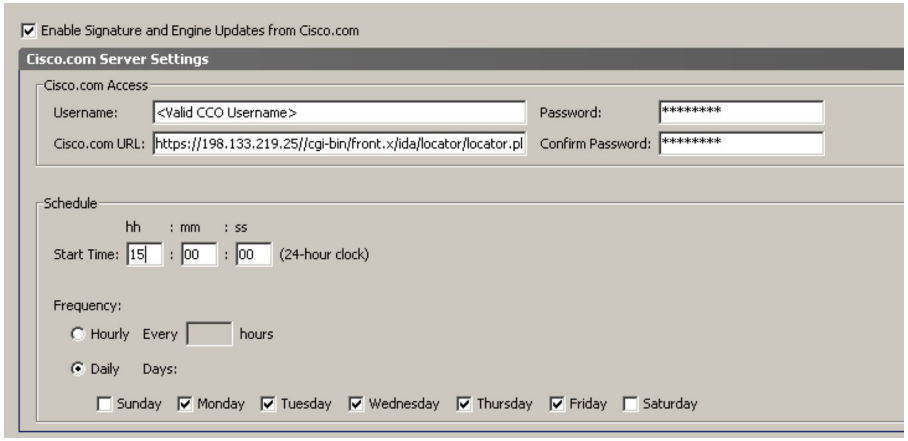


Procedure 4 Configure IPS Signature Updates

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 have each sensor update its signatures directly from Cisco.com.

Step 1: To configure an IPS signature update in ASDM/IME, access **Configuration** > **IPS** > **Sensor Management** > **Auto Cisco.com Update**. (Figure 39)

Figure 39. Auto Update Settings



Tech Tip

Note that using the auto update feature from Cisco.com will only update the sensor's Engine files and Signature files. Major and minor code versions and service packs are not updated with this mechanism.

IPS software is available here (note this requires a valid Cisco.com login): http://tools.cisco.com/support/downloads/pub/Redirect.x?mdfid=268439591.

To receive automatic notifications of code version releases and other IPS news, sign up for Cisco Threat Defense Bulletins here: http://tools.cisco.com/gdrp/coiga/showsurvey.do?surveyCode=380&keyCode=123668_4.

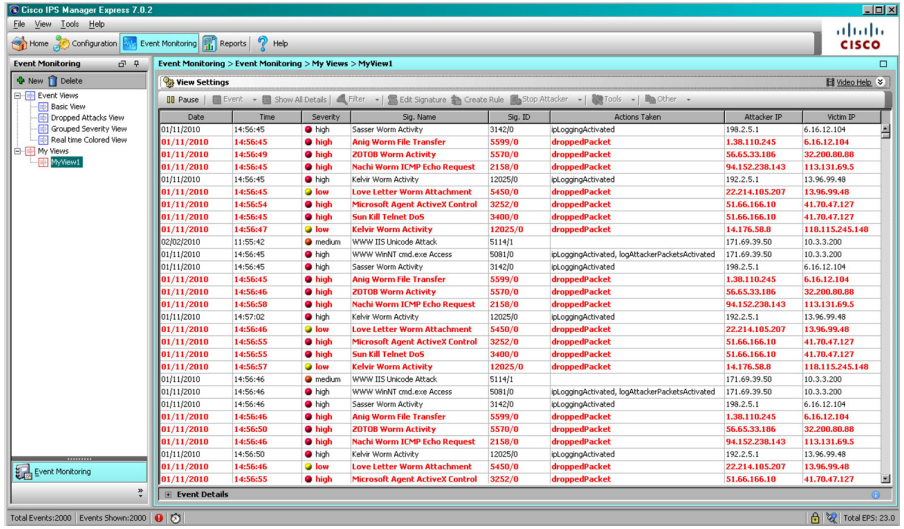
Procedure 5 Configure IDS or IPS Event Monitoring

Because both IDS and IPS devices produce alerts when they detect activity, it is important to set up a monitoring solution to retrieve, store, and display these events. IPS Manager Express (IME) is one such solution for Cisco IPS. It is available on the IPS software download page on Cisco.com.

IME is a complete management and monitoring solution for Cisco IPS solutions that allows a user to set up, configure, monitor, and tune an IPS/IDS deployment. It is available at no extra cost on Cisco.com in the same place as Cisco IPS software updates and upgrades.

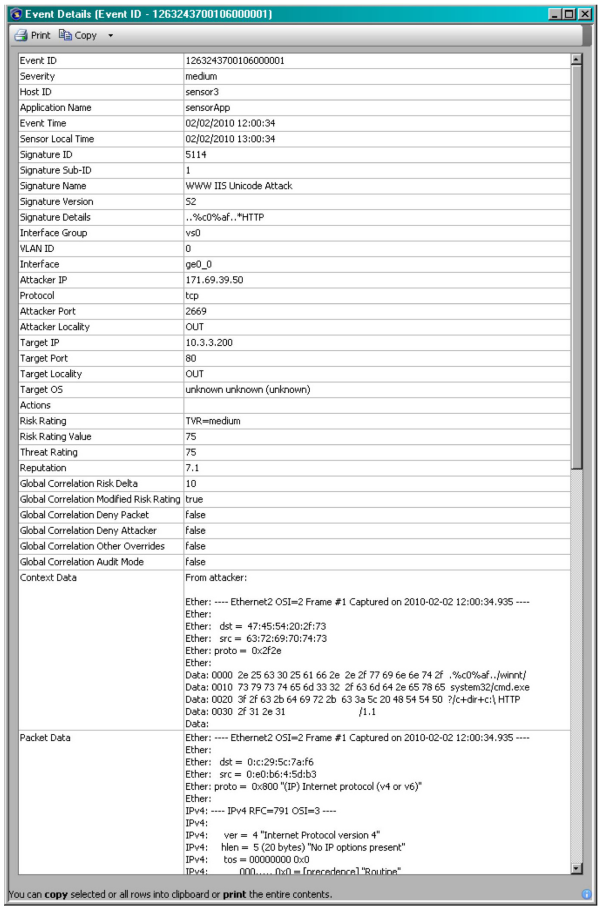
IME is a standalone, installed package that includes a service to automatically pull events from up to 10 sensors (as of IME 7.0.2). When the application is running, you can also use IME to configure up to 10 sensors individually. Events in IME can be viewed in either a real-time format or a time-based filtering capability (Figure 40).

Figure 40. Auto Window



Step 1: Right-click a specific event to get more data (Figure 41).

Figure 41. Event Details Window



Procedure 6 Troubleshoot the IPS

If you suspect network errors are the result of the IPS device blocking legitimate traffic, you can confirm and eliminate the problem.

Step 1: The first step in identifying whether the IPS is blocking legitimate traffic is to take the sensor out of the processing path.

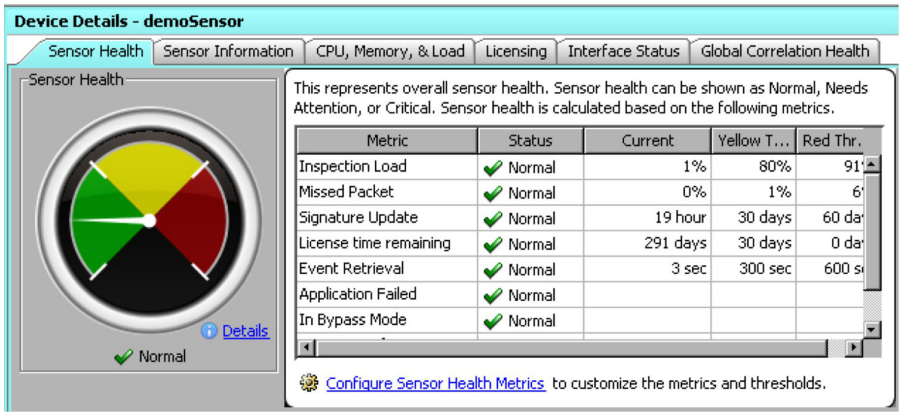
To do this, go into ASDM and either add the devices being impacted to the Bypass policy group, which will remove all inspection including firewall inspection for those IP addresses, or disable the policy that sends traffic to the SSM module, which removes IPS inspection for all packets. This allows the traffic to flow through the ASA without getting inspected by the SSM module.

In the appliances, taking the sensor out of the processing path can be easily accomplished by putting the sensor into "Bypass On" mode, which passes traffic around the inspection engine which prevents any IPS inspection from occurring.

If either of these actions solves the problem, then more detailed trouble-shooting is in order at a time when it is possible without impacting network traffic. If this does not solve the problem, it is unlikely to be an IPS-related issue and you can focus troubleshooting efforts elsewhere.

Step 2: Follow-on steps might include checking IME to see if the sensor is healthy and responsive. If not, a TAC case might be needed to determine the problem (Figure 42).

Figure 42. Troubleshooting using IME



Step 3: If the sensor is working fine, check the event logs to see if the sensor is firing events with deny actions related to the IP addresses or services being impacted. If the sensor is firing events that are blocking traffic, the sensor is either seeing real attacks and blocking them, or it is firing on false positives.

Step 4: Filter out false positives using the Event Action Filters in the **Sensor Configuration** > **Policies** bottom right screen. Adding a filter to remove the deny action for the event being fired incorrectly should solve the problem.

Notes

Resilient WAN Design

Agency Overview

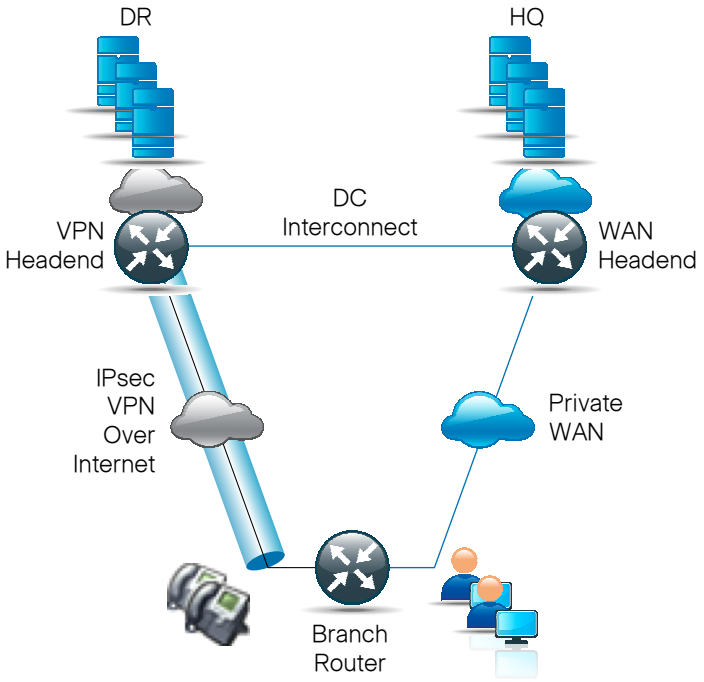
Many agencies require network connectivity for remote sites to access data at the HQ. This need for network connectivity can occur naturally as an agency establishes a physical presence in new markets or grows and begins to occupy space not adjacent to an original location. The network must be able to establish connectivity regardless of the available local connectivity options, or provide secure transport over low-cost network options such as broadband Internet connections. Typically, connectivity must accommodate data and voice service, and depending on the agency, may require specialized capabilities such as support for videoconferencing or physical security infrastructure. Specific types of traffic will likely require preferential treatment to assure that applications function properly when the network is busy, or some applications may require special services to reduce the impact from the lower bandwidth of the WAN as compared to LAN resources. Furthermore, depending on the nature of the agency, there may also be a need for a high level of availability for the remote sites WAN connectivity, either to data resources at the HQ site, or to secondary data resources at a disaster recovery site. If a disaster recovery site is part of the network design, connectivity must be available to provide data transport to synchronize data from the HQ's server room with the resilient data store at the disaster recovery site, and to provide an alternate route when remote sites must rely on resilient connectivity to thedisaster recovery site to gain access to the HQ's data.

Technology Overview

With today's need for a continuous and reliable network connection for various application services, remote sites that rely on a single connection to the HQ will likely experience an undesirable downtime and loss of productivity and revenue. Therefore, a disaster recovery site and a secondary WAN connection at the remote site are necessary to assure access to HQ data is maintained. A disaster recovery site provides resiliency and fault-tolerance capabilities during a primary network outage or downtime. This section provides more detail on how to achieve it.

In the past, a leased-line or frame-relay link was typically expected to offer primary connectivity, and secondary connectivity could be provided by lower-cost WAN connectivity such as a fractional leased line, an ISDN line, or even a dial connection. Current applications such as web-based tools, database queries over a WAN, and virtual desktop applications require more bandwidth, and the proliferation of Ethernet-connected broadband Internet has caused a shift toward using an Internet Virtual Private Network (VPN) as a viable backup connectivity option.

Figure 43. Resilient WAN Overview



Adding a second link from the remote site router to the disaster recovery site's server farm increases availability of the WAN design and will improve business continuity by providing access to user, application, and network services in the event of a WAN failure to the headquarters site.

The HQ is connected via a separate WAN link to the disaster recovery site. This link should be provisioned separately from the remote sites' WAN connectivity to reduce the chances that a problem that disrupts connectivity from remote sites to the HQ affects connectivity between the HQ server room and the disaster recovery resources.

The remote site router's secondary link could be provisioned as a separate dedicated WAN connection, or it could use a VPN through a public network such as the Internet. In either case, high availability is offered by running dynamic routing over the connection to converge routing over the secondary link to the disaster recovery site during loss of connectivity on the primary link.

The primary WAN link, which can be a leased T1/E1 connection, provides connectivity to the primary data center for applications and services. The disaster recovery site server farm has been configured to provide business continuity when the applications or services at the primary data center are down.

Process

Configuring the Resilient WAN

1. Configure the WAN Interface
2. Enable Dynamic Routing
3. Configure VPN on the Resilient WAN Link
4. Configure Remote Site IPSec
5. Configure Embedded Event Management (EEM) Scripts

This deployment guide covers a generic example for a fractional T1 Internet link using the voice/WAN interface card (VWIC) T1/E1 card. Optionally, a serial high-speed WAN interface card (HWIC) can be used. Other connections like an Ethernet handoff from a broadband modem, leased line, or a MPLS connection can be used.

The WAN headend involves two sites, the primary and the disaster recovery site. The two headend Cisco 3845 routers are interconnected with each other. Various technologies like Ethernet or leased connections can be used. Enhanced Interior Gateway Routing Protocol (EIGRP) routing protocol is configured to exchange routing and network updates between the two sites. A single instance of EIGRP is used to reduce the complexity and provide faster convergence.

Procedure 1 Configure the WAN Interface

Step 1: On the VWICs, you are required to specify the mode as T1 or E1. Enter the following, which is a global configuration command, where 0 0 specifies the HWIC is in card slot 0 and WIC slot 0:

```
card type t1 0 0
```

Step 2: Clocking for the router is configured to use Port 0 on the T1/E1 high-performance WAN interface card (HWIC). First, enable the card to provide clocking. Then, select the clock with a priority of 1 (highest) and configure port 1 with a priority of 2 using the following global configuration commands:

```
network-clock-participate wic 0
network-clock-select 1 T1 0/0/0
network-clock-select 2 T1 0/0/1
```

Step 3: In the situation of a primary link failure, the clock is derived from the second port 0/0/1. The third line in the preceding configuration will help achieve this. The following highlighted commands select port 1 on the VWIC. The second command may vary based on the service speed, however, in our deployment, the channel-group command allocates all 4 timeslots to a serial interface 0/0/1:0, which is created after issu¬ing this command.

```
controller T1 0/0/1
  cablelength short 110
  channel-group 0 timeslots 1-4
```

Step 4: The resulting serial interface from the channel-group command allows us to configure the address required for the WAN. In our case the network subnet was 10.0.2.0/30.

```
interface Serial0/0/0:0
  description Backup Link (Internet)
  ip address 10.0.2.2 255.255.255.252
  ip wccp 62 redirect in
  ip pim sparse-mode
```

Procedure 2 Enable Dynamic Routing

To enable dynamic routing, EIGRP is configured with the same autonomous system number as the other router and switches.

Step 1: Using the network command, enable EIGRP on all interfaces within the network range specified, which is all within this router.

```
router eigrp 1
  passive-interface default
  no passive-interface Serial0/0/0:0
  no passive-interface Tunnel0
  network 10.0.1.0 0.0.0.255
  network 192.168.0.0 0.0.255.255
  no auto-summary
```

The Cisco 2911/2811 Integrated Services Router (ISR) remote site router will become EIGRP neighbors with both the headquarters router over the primary WAN interface and the disaster recovery router over the secondary link. All data will traverse the link to the headquarters site during normal operation because the secondary link is lower bandwidth and has a higher-link cost in EIGRP.

Step 2: If the secondary link's bandwidth is the same as the primary link, EIGRP can be configured to make the secondary link the less desirable of the two. Use delay parameter to tweak the metric on the required interface to make it less desirable. Use the following interface command under the Tunnel interface:

```
delay <value> (tens of microseconds)
```

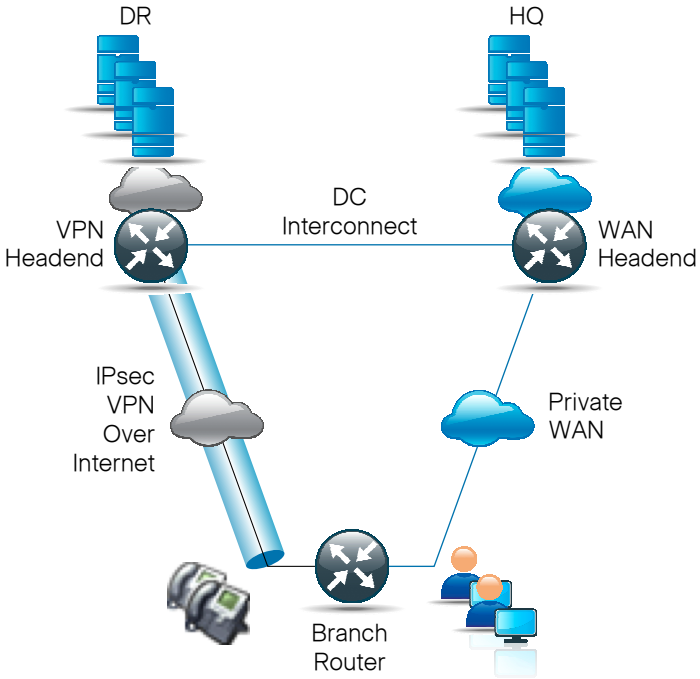
Step 3: The default delay for a T1 link is 20 ms for routing protocol metric calculation. For example: Increasing the link delay by 50 percent will make the T1 link less desirable and the remote site will only use the link as a backup. Enter the **delay 3000** command to increase the delay to 30 ms.

Step 4: Use the **passive-interface default** command to disable routing updates on all interfaces on a router. Then you can enable routing on only the interfaces where it is needed with the no **passive-interface [interface]** command.

Procedure 3 Configure VPN on the Resilient WAN Link

No location in the world is completely free from the threat of natural or man-made disasters of varying degrees, from fiber cuts and power outages, to full-scale regional meteorological or geological events. A agency that expects a high level of continuity must provide for resilient access to its data, particularly in circumstances when the headquarters site is endangered. The SBA Data Center design provides a secondary WAN connection to the disaster recovery site to accommodate data access resiliency. The configuration offers a VPN connection over the Internet to back up the primary WAN connection, which can provide an alternate route to data resources at the HQ or to backup data at the disaster recovery site.

Figure 44. VPN Connectivity



The following example shows how to connect remote site IPsec peers to the headend disaster recovery router. The design applies Cisco IOS® IPsec virtual tunnel interface (VTI) to provide encrypted transport of data and voice information with minimal configuration burden and maximum functionality. VTI offers two modes of operation: static VTI, which can initiate tunnels to other static VTI sites, or multiple static VTI sites, which can initiate tunnels to a template-based dynamic VTI (DVTI) aggregation point that offers simple configuration. This is the recommended solution because:

- DVTI does not require you to know the remote sites' public address, which simplifies configuration for remote sites that may be assigned dynamic address or translated by Network Address Translation (NAT).
- DVTI only requires you to configure one tunnel for the headend, offering the least complex configuration and troubleshooting.
- VTI offers a virtual interface for applications of QoS policies, NAT, Firewall, IPS, ACLs, and tunnel monitoring, as compared to a traditional **crypto-map** VPN configuration.
- VTI configuration provides superior dynamic routing flexibility to enable the requirements of the SBA design.

Remote sites initiate their connection to the DVTI responder on the headend router, which creates a VTI for every remote site's connection. DVTI applies a template-based configuration for remote sites' connectivity so that multiple tunnels may be created with one DVTI configuration; additional configuration is not needed to support multiple remote sites.

Step 1: Use Internet Security-Association Key Management Protocol (ISAKMP) configuration to define a cryptographic shared-secret key and negotiation policy shared between remote sites and the headend.

```
crypto keyring sba-keys
  pre-shared-key address 0.0.0.0 0.0.0.0 key sba
crypto isakmp policy 1
  encr aes
  authentication pre-share
  group 2
crypto isakmp profile sba-isakmp
  keyring sba-keys
    match identity address 0.0.0.0
    virtual-template 1
```

Step 2: IPsec policy defines the cryptographic cipher that the router will apply to data transiting the tunnel. Cisco IOS Software supports a wide range of cryptographic transforms, from older Digital Encryption Standard (DES) and 3DES to various strengths of Advanced Encryption Standard (AES). Apply the following example, which applies 128-bit AES, which is the current recommendation that offers the best combination of performance and cryptographic security.

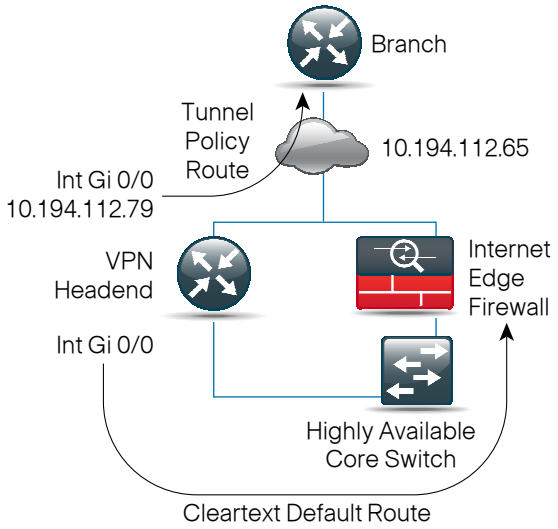
Note that the sba-xform label is used to apply the esp-aes IPsec policy to the IPsec profile.

```
crypto ipsec transform-set sba-xform esp-aes
crypto ipsec profile sba-ipsec
  set transform-set sba-xform
```

Step 3: Apply the following tunnel interface configuration to define the IP address on the tunnel interface, as well as local and remote tunnel endpoints, and associate IPsec protection with the virtual interface:

```
interface Virtual-Template1 type tunnel
  ip unnumbered Port-channel1.159
  tunnel source FastEthernet0/2/0
  tunnel mode ipsec ipv4
  tunnel protection ipsec profile sba-ipsec
```

Figure 45. VPN Hub Placement



Tech Tip

For ease of troubleshooting, use unique, intuitive labels for the configuration of the keyring, ISAKMP profile, and IPsec profile rather than general or random labels.

Tech Tip

When applying the virtual-template configuration, be sure that you apply the type tunnel option. Without the option, Interface Virtual-Template will not apply to the cryptographic configuration.

Step 4: The VPN hub is connected to the network core behind the Internet Edge Firewall. The Internet Edge ASA must forward all incoming VPN traffic to the router's private IP address, and accommodate the VPN traffic in the ASA's outside-to-inside access policy. Apply the following configuration on the Active Internet Edge ASA, which will enable connectivity to the VPN headend by translating the outside address of 10.194.112.101 to the VPN headend's private address, 192.168.159.2. This configuration will allow VPN traffic to traverse the ASA and connect to the headend disaster recovery router.

```
name 192.168.159.2 vpn-hub
!
object-group service isakmp-esp
  service-object esp
  service-object udp eq 4500
  service-object udp eq isakmp
!
access-list outside_access_in extended permit object-group
isakmp-esp any host 10.194.112.101
!
static (inside,outside) 10.194.112.101 vpn-hub netmask
255.255.255.255
!
access-group outside_access_in in interface outside
```

Procedure 4 Configure Remote Site IPSec

The remote site IPsec tunnel is activated when the router sends traffic on the tunnel interface, which most likely has EIGRP running on it, and it attempts to establish a neighbor relationship with a peer at the other end of the tunnel. After the IPsec tunnel is up, the remote site and headend routers become EIGRP neighbors and exchange routing information over the tunnel. These routes should only take precedence when the primary leased-line connectivity is unavailable, and the higher-cost routes over the tunnel take precedence.

Step 1: Apply the following IPsec VTI configuration on the remote site router to connect to the disaster recovery site:

```
crypto isakmp policy 1
  encr aes
  authentication pre-share
  group 2
crypto isakmp key sba address 0.0.0.0 0.0.0.0
!
!
crypto ipsec transform-set sba-xform esp-aes
!
crypto ipsec profile sba-ipsec
  set transform-set sba-xform
!
interface Tunnel0
  ip unnumbered FastEthernet0/0.72
  tunnel source Serial0/0/1:0
  tunnel destination 10.0.1.250
  tunnel mode ipsec ipv4
  tunnel protection ipsec profile sba-ipsec
```

This configuration will establish and maintain a permanent tunnel over the backup WAN connection when backup WAN connectivity is available.

Procedure 5 Configure EEM Scripts

If the tunnel should only be established when the primary link fails, interface tracking can be used to bring the tunnel up and down with an Embedded Event Manager (EEM) script. The EEM script is executed when the interface's routing status changes.

EEM is a Cisco IOS feature that provides the capability for the router to execute scripts that are a portion of the router's configuration. This integrated capability allows the router to react and adjust to changes in network connectivity and behavior. EEM scripts are part of the router's CLI configuration, and are entered, as any other configuration, from the router's configuration prompt.

Tech Tip

As in the previous DVTI headend configuration, unique, intuitive configuration labels simplify troubleshooting.

Step 1: Enable tracking, which monitors the primary WAN interface's ability to route IP traffic.

```
track 123 interface Serial0/0/0:0 ip routing
```

Step 2: Configure the first EEM script, which enables the IPsec VPN connection when the primary WAN loses its ability to route.

```
event manager applet start-tunnel
  event track 123 state down
  action 1 cli command "enable"
  action 2 cli command "configure terminal"
  action 3 cli command "interface tunnel0"
  action 4 cli command "no shut"
  action 5 cli command "end"
```

Step 3: Configure the second EEM script, which disables the IPsec VPN connection when the primary WAN's ability to carry traffic is restored.

```
event manager applet stop-tunnel
  event track 123 state up
  action 1 cli command "enable"
  action 2 cli command "configure terminal"
  action 3 cli command "interface tunnel0"
  action 4 cli command "shut"
  action 5 cli command "end"
```

This configuration offers the benefit of reducing connectivity fees over the secondary connection and should only be used if the second link is subject to bandwidth or time-based usage charges. Failover to the IPsec connection takes longer with this method as the router must bring up the IPsec tunnel and routing must converge before the connection can pass user data.

Resilient WAN Optimization

Agency Overview

This section covers the use of Wide-Area Application Services (WAAS) in a high-availability data center scenario where one data center is active and the second data center is in standby or disaster recovery mode. WAAS provides application acceleration and optimization between remote locations and a central location or data center. As a solution, the Cisco WAAS is a combination of hardware and software. WAAS can support a primary and secondary or standby data center configuration. Additionally, WAAS provides a specific product optimized for replication between two data centers, but that scenario will not be covered in this design.

Reader Tip

In this document, we refer to the solution using a generic term "Application Acceleration" and the hardware as "Application Acceleration device." The Cisco brand name for the software is WAAS and the brand name for the hardware is Wide-Area Virtualization Engine (WAVE).

Technology Overview

WAAS in the Primary Data Center

The configuration of WAAS in the primary data center is covered in the *Cisco SBA for Midsize Agencies—Borderless Networks Foundation Deployment Guide*. To create a high-availability design, the only addition necessary is a secondary headend WAAS Application Acceleration device placed in the standby data center. The configuration of the secondary device is the same as the primary. Should a failure occur between the remote location(s) and the primary data center, data will only be passed to the standby site. All routing is handled by the IP routing protocols used in the design so there are no specific configuration changes needed to support WAAS in an HA design. If the primary location becomes unavailable, the WAAS Central Manager may not be able to provide reporting on the WAAS network. Should an outage occur and the primary data center is unavailable, the WAAS network will continue to provide optimization without the Central Manager.

WAAS in the Standby Data Center

The WAAS Application Acceleration device in the standby data center is configured in the same way as the WAAS Application Acceleration device in the primary data center, but remains idle until the secondary data center becomes active.

The exception to this is the IP addressing used when the device is first set up. The addressing and other specifics related to the initial configuration depend on the addressing used in the standby data center. Follow the deployment instructions outlined in the *Cisco SBA for Midsize Agencies—Borderless Networks Foundation Deployment Guide* to initially configure and register the data center headend device with the WAAS Central Manager.

WAAS in the Remote Site

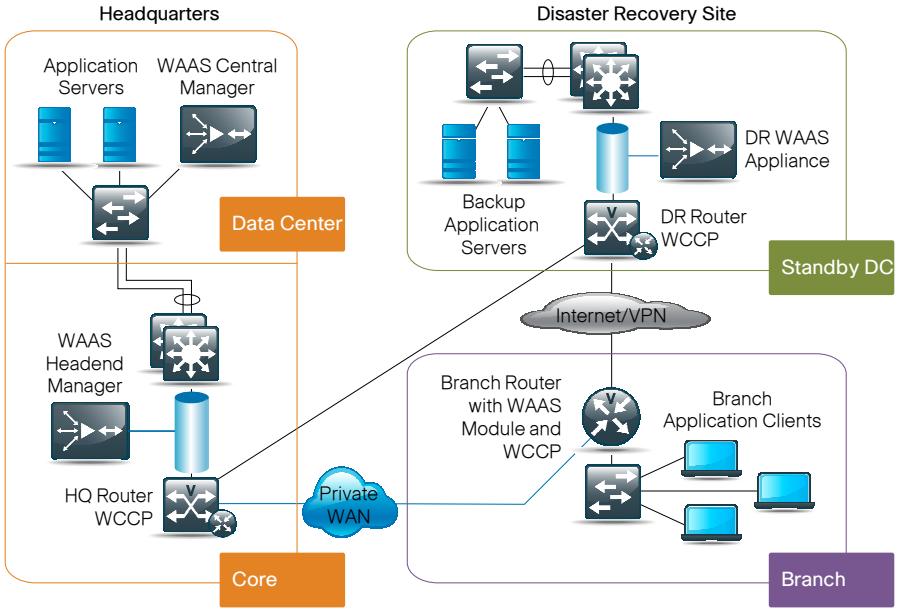
WAAS relies on standard IP routing protocols for HA configuration, and as such, there are no specific WAAS configuration requirements at the remote sites. All HA or failover routing is handled in the configuration of the remote site router. Once a failure between a remote site and the primary data center is detected, the Cisco Internet Services Router (ISR) at the remote site automatically redirects traffic to the standby data center. Any existing application sessions that are being optimized between the remote site and the primary data center will be dropped and need to be reestablished with the standby data center. How this behavior affects the user experience depends on the type of application in the standby data center and the method of optimization employed by WAAS.

Provisioning and replication of applications and data between the primary and standby data center is beyond the scope of this guide, but these issues need to be considered in the overall data center design. Once the WAAS connection between the remote site and the standby data center is established, application optimization starts automatically. At first, an application is optimized using compression, which, on average, provides a 30 percent improvement in performance. Once data is populated between the remote site WAAS Application Acceleration device and the data center Application Acceleration device, users experience additional performance enhancements and bandwidth savings.

Tech Tip

A secondary WAAS Central Manager can be placed in the standby data center for a resilient design for WAAS configuration and reporting. Please refer to the *Cisco WAAS Configuration Guide* for details.

Figure 46. WAN Optimization Overview



Process

Configuring the Cisco WAAS Central Manager

1. Prepare the WAAS
2. Complete the Initial Setup

Procedure 1 Prepare the WAAS

Step 1: In the data center, unpack and connect the second WAAS device you want to configure as the data center WAVE in the WAAS network. Set the port that connects to the WAVE to full duplex. For hardware installation instructions, refer to the hardware installation guide for the WAVE.

Tech Tip

Cisco strongly recommends that you not use half-duplex connections on the WAVE or on routers, switches, or other devices. Use of half duplex impedes the system's ability to improve performance and should not be used. Check each Cisco WAVE interface and the port configuration on the adjacent device (router, switch, firewall, WAVE) to verify that full duplex is configured.

Step 2: Power up the designated data center WAVE and open a console connection.

Step 3: When a WAAS device starts for the first time, you are prompted to run the setup utility that you use to set up the basic configuration for the device. When prompted, press **Enter** and then enter the administrator password, which is **default**.

The configuration prompt will wait several seconds before proceeding with the WAVE setup sequence.

If you want to quit the setup utility, you can press **Esc** at any time.

Tech Tip

If you do not press **Enter** in time to enter the basic configuration, log into the WAAS device through the terminal console and enter the **setup** command to manually invoke the setup utility. When you log in, the username is **admin** and the password is **default**.

Procedure 2 Complete the Initial Setup

Step 1: The first step of the setup utility displays a default configuration.

To continue with these default settings, enter y. To enter quick configuration mode to change the default settings, enter n.

```
Step 1: The following defaults can be configured:
Device mode: Application-accelerator
Interception Method: WCCP
Management Interface: GigabitEthernet 1/0
Autosense: yes
DHCP: yes
Timezone: UTC 0 0
To keep above defaults and continue configuration, press 'y'.
To change above defaults and continue configuration, press 'n'
[y]:
```

Tech Tip

If you use the default settings, the setup utility will skip some of the following steps.

Step 2: Enter the required information as you are prompted to do so by the setup utility.

For example: Choose **application-accelerator** as the device mode that you want to configure on the WAAS device. You can accept the default choice (shown in brackets) at a prompt by pressing Enter.

```
Step 2:
Configure WAAS Settings
-----------------------
Select device mode:
1.application-accelerator
2.central-manager
Enter your choice [1]: 1
```

Step 3: Specify the IP address or hostname of the WAAS Central Manager that the Core-WAE1 should register with.

```
Step 3: Enter Central Manager address: xxx.xxx.xxx.xxx
```

Tech Tip

The IP address that you enter in Step 3 is that of the Central Manager in the primary data center.

Step 4: Choose the interception method. The default method is normally the correct one to choose because it is automatically set to Web Cache Communication Protocol (WCCP) if no Cisco WAVE Inline Network Adapter is installed.

```
Step 4: Select interception method (inline|wccp|other) [wccp]:
wccp
```

Step 5: Choose the interface to configure as the management interface for communicating with the WAAS Central Manager. With the Cisco WAVE Inline Network Adapter, you can choose to share one of the inline interfaces for management traffic or you can use one of the built-in Gigabit Ethernet interfaces (out-of-band management).

```
Step 5:
Configure network settings
--------------------------
Select interface to configure as management interface:
  NO INTERFACE NAME STATUS IP ADDRESS NETMASK
  1: GigabitEthernet 1/0 UP unassigned unassigned
  2: GigabitEthernet 2/0 DOWN unassigned unassigned
Enter choice [1]: 1
```

Continue to answer the questions displayed in the setup utility.

When you are prompted for the IP address of the interface, enter the IP address for the management interface that you chose in this step.

Step 6: When you are prompted to enter the WCCP router list, enter the IP addresses of 1-4 routers separated by spaces. The easiest configuration is to accept the default, which is the router you configured as the default gateway. To accept the default, press **Enter**.

```
Step 17: Enter the space separated list of routers(maximum 4)
for WCCPv2 [10.10.10.1]:
```

Step 7: When you are prompted to choose a license, choose the ones you have purchased for use on your WAE. Activating the appropriate licenses is required for various acceleration features to operate. Not all licenses are supported on all WAE models.

```
Step 18:
The product supports the following licenses:
1. Transport
2. Enterprise
3. Enterprise & Video
4. Enterprise & Virtual blade
5. Enterprise, Video & Virtual blade
Enter the license(s) you purchased [2]:
```

Step 8: The setup utility will display a set of example router configurations for your convenience.

Press **Enter** to continue.

Step 9: When finished, you will see a summary of the information that you entered. When prompted to accept the configuration, enter y. When prompted to apply the configuration, enter y. Once you apply the changes, the device is visible on the network and can be pinged.

If you choose not to accept the configuration, you have the option to go through the setup questions again and reenter the values. Your previous values are used as the defaults.

Step 10: Save the configuration on Core-WAE1.

```
Core-WAE1# copy running-config startup-config
```

Process

Configuring WCCP on the DR Site Router

1. Configure WCCP
2. Configure WAAS on the Headquarters Router

Procedure 1 Configure WCCP

Step 1: Enable the WCCP protocol on the headquarters router.

```
ip wccp version 2
ip wccp 61
ip wccp 62
```

Tech Tip

IP WCCP version 2 will not show in the configuration file.

Procedure 2 Configure WAAS on the HQ Router

Step 1: On the internal or LAN interface (server-farm facing) of the HQ router (3925/3845), enter the following commands. The commands are applied to the port channel, which in turn applies them to the ports connected to the network core.

```
interface Port-channel1.31
encapsulation dot1Q 31
ip address 192.168.31.2 255.255.255.0
ip wccp 62 redirect in
```

Step 2: On the external router interface (WAN facing) of the HQ router (3925/3845) enter the following commands:

```
interface Serial0/0/0:0
ip address 10.0.1.1 255.255.255.252
ip wccp 61 redirect in
```

Notes

Resilient Server Design

Agency Overview

The network is playing an increasingly important role in the success of an agency. Key applications such as enterprise resource planning (ERP), e-commerce, email, and portals must be available around the clock to provide uninterrupted 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. According to respondents of the Yankee Group 2005 Application Management Survey, application performance issues result in an average productivity decrease of 14 percent. This is evidence that application performance, as well as availability, directly affects employee productivity and the bottom line of an agency. As more users work more hours utilizing key agency applications, it becomes even more important to address application availability and performance issues to ensure achievement of operational 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 agency 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 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 server banks 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.

The Application Control Engine (ACE) is the latest SLB offering from Cisco. Its main role is to provide Layer 4 through 7 switching, but the 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 Web and 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.** 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.** 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.** ACE improves application performance and reduces response time by minimizing latency and data transfers for any HTTP-based application, for any internal or external end user.
- **Server Offload.** ACE offloads TCP and SSL processing which allows servers to serve more users and handle more requests without increasing the number of servers.

ACE hardware is always deployed in pairs for highest availability: one primary and one secondary. If the primary ACE fails, the secondary 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.

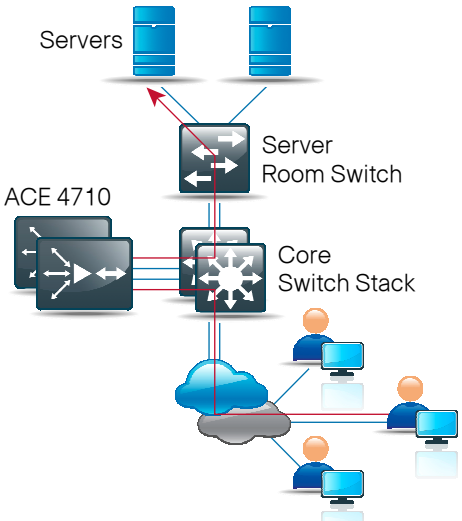
Additionally, ACE may be used to push requests for cacheable content such as image files to a set of caches that can serve them more cost-effectively than the application servers.

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.

ACE reduces the amount of data sent from the Web application server to the browser by utilizing hardware compression and patented Delta Encoding. Delta Encoding determines exactly what has changed from page to page, to the level of detail of a single byte, and sends only the content that has changed.

ACE further improves the end-user application experience by reducing latency and the number of round trips required for application access. ACE eliminates unnecessary browser cache validation requests and provides automatic embedded object version management at the server, resulting in significantly improved application response times for application users.

Figure 47. Resilient Server Overview



There are several ways to integrate ACE into the data center network. Logically, the ACE is deployed in front of the Web application cluster. Requests to the application cluster are directed to a virtual IP address (VIP) configured on the ACE. The 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 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.

Process

Configuring ACE

1. Add the ACE to the Network
2. Configure a Load-Balancing Policy

In this example, we will first configure the ACE appliance with the required parameters to be recognized on the network. Then we will define the policies for directing the traffic. While the first part of the configuration is typically performed at the CLI when booting ACE, both parts can be configured via the ACE GUI.

To save room in this guide, we have chosen to use the CLI commands for both network and application policy configuration. When setting up the ACE for the first time, the default password for the admin account must be changed.

Procedure 1 Add the ACE to the Network

Step 1: Enter the following at the command line:

```
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":
  Confirm the new password for user "admin":
  admin user password successfully changed.
  Enter the new password for user "www":
  Confirm the new password for user "www":
  www user password successfully changed.
Cisco Application Control Software (ACSW)
TAC support: http://www.cisco.com/tac
Copyright © 1985-2009 by Cisco Systems, Inc. All rights
reserved.
The copyrights to certain works contained herein are owned
by other third parties and are used and distributed under
license.
Some parts of this software are covered under the GNU Public
License. A copy of the license is available at http://www.gnu.
org/licenses/ gpl.html.
  ACE>
This script will perform the configuration necessary for a
user to manage the ACE Appliance using the ACE Device Manager.
The management port is a designated Ethernet port that has
access to the same network as your management tools including
the ACE Device Manager.
You will be prompted for the Port Number, IP Address, Netmask,
and Default Route (optional).
Enter 'ctrl-c' at any time to quit the script
ACE>Would you like to enter the basic configuration dialog
(yes/no) [y]: n
switch/Admin#
```

Step 2: Before proceeding with any additional configuration, set up the basic network security policies to allow for management access into the ACE.

```
access-list ALL line 8 extended permit ip any any
class-map match-all http-vip
  2 match virtual-address 192.168.24.100 tcp eq www
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: Ethernet VLAN trunks to the network's switching resources connect the ACE appliances. Configure two Gigabit Ethernet ports on each ACE to trunk to the core switch as follows:

```
interface gigabitEthernet 1/1
  channel-group 1
  no shutdown
interface gigabitEthernet 1/2
  channel-group 1
  no shutdown
interface port-channel 1
  switchport trunk allowed vlan 24
  no shutdown
```

As such, the switch ports that connect to the security appliances must be configured so that they are members of the same secure VLANs and forward secure traffic to switches that offer connectivity to servers and other appliances in the server room.

The ACE appliances are configured for Active-Standby High Availability. When ACE 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 server room.

Step 4: A fault-tolerant (FT) VLAN is a dedicated VLAN used by a redundant ACE pair to communicate heartbeat and state information. All redundancy-related traffic is sent over this FT VLAN (including TRP protocol packets, heartbeats, configuration sync packets, and state replication packets).

```
ft interface vlan 12
  ip address 10.10.12.11 255.255.255.0
  peer ip address 10.10.12.12 255.255.255.0
  no shutdown
ft peer 1
  heartbeat interval 300
  heartbeat count 10
  ft-interface vlan 12
ft group 1
  peer 1
  priority 120
  peer priority 110
  associate-context Admin
  inservice
```

Step 5: For the ACE to begin passing traffic, create a VLAN interface and assign an IP address to it. Since we are employing one-armed mode, a NAT pool needs to be created as well.

```
interface vlan 24
  ip address 192.168.24.2 255.255.255.0
  peer ip address 192.168.24.3 255.255.255.0
  access-group input ALL
  nat-pool 1 192.168.24.99 192.168.24.99
  netmask 255.255.255.0 pat
  service-policy input remote_mgmt_allow_policy
  no shutdown
ip route 0.0.0.0 0.0.0.0 192.168.24.1
```

At this point, the ACE should be reachable on the network. Now we can begin configuring a load-balancing policy.

Procedure 2 Configure a Load-Balancing Policy

Step 1: To start, define the application servers that require load balancing.

```
rserver host webserver1
  ip address 192.168.24.12
  inservice
rserver host webserver2
  ip address 192.168.24.13
  inservice
```

Step 2: Next, create a simple HTTP probe to test the health of the Web servers.

```
probe http http-probe
  port 80
  interval 15
  passdetect interval 60
  request method head
  expect status 200 200
  open 1
```

Step 3: Place the Web servers and the probe into a server farm.

```
serverfarm host webfarm
  probe http-probe
  rserver webserver1 80
    inservice
  rserver webserver2 80
    inservice
```

Step 4: Now configure the load-balancing policy and assign it to the VLAN interface.

```
class-map match-all http-vip
  2 match virtual-address 192.168.24.100 tcp eq www
policy-map type loadbalance first-match http-vip-l7slb
  class class-default
    serverfarm webfarm
policy-map multi-match int24
  class http-vip
loadbalance vip inservice
loadbalance policy http-vip-l7slb
loadbalance vip icmp-reply active
nat dynamic 1 vlan 24
interface vlan 24
  service-policy input int24
```

At this point, the application should be accessible via the VIP we created (192.168.24.100) and the requests distributed between the two Web servers.

Summary

IT organizations face significant challenges associated with the delivery of applications and critical agency data with adequate service levels to a globally distributed workforce. Application-delivery technologies help IT organizations improve availability, performance, and security of all applications. The Cisco Application Control Engine provides core-server load-balancing services, advanced application acceleration, and security services to maximize application availability, performance, and security. It is coupled with unique virtualization capabilities, application-specific intelligence, and granular role-based administration to consolidate application infrastructure, reduce deployment costs, and minimize operational burdens.

Resilient Wireless Design

Agency Overview

To address today's agency challenges, users expect access to data anytime and anywhere. Whether inside the confines of an agency's physical location, at a hotspot, in the home, or out on the street, different wireless technologies have made it possible to connect without being connected. Within the walls of a specific agency location, the predominant wireless technology is 802.11, commonly referred to as Wi-Fi.

While Wi-Fi is provided in a variety of speeds, or bandwidth, all provide a fairly common set of services, including:

- Secure access to agency resources, voice, video, data, printers, etc.
- Ability to be mobile within the office
- Guest access from the agency network to the Internet

Wi-Fi is now a part of everyday agency life. Many users rely upon this network service for mobile access to data, collaboration, and voice services. Providing a seamless and uninterrupted user experience, even during a major failure, is possible with a Cisco Wireless LAN Controller (WLC) within the Disaster Recovery data center. This secondary controller provides continued secure access for employee and guest services, minimizing disruption to the agency.

The Cisco WLCs work in conjunction with each other and the access points (APs) to provide continuous service without user or administrative intervention during an outage at the HQ site or remote locations, thereby lowering operational overheads and simplifying disaster recovery procedures.

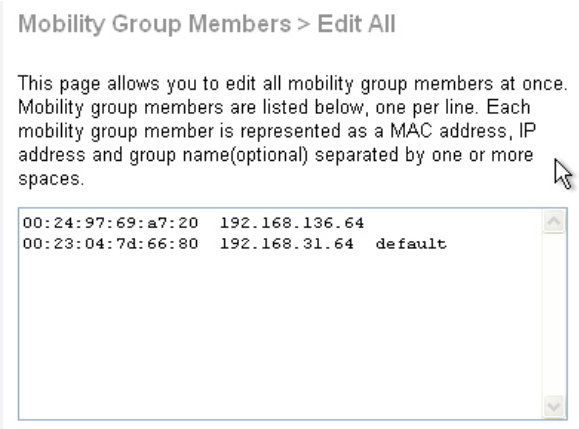
Technology Overview

Within the *Cisco SBA for Midsize Agencies—Borderless Networks Foundation Deployment Guide*, we configured each remote site access point (AP) in H-REAP mode. This means the AP can work either connected to the WLC in the data center or in autonomous mode. This process was the first step to allow for high availability at the remote sites. To keep this resiliency within the headquarters and to allow our remote site access points to continue to associate new clients, you must add an additional controller. By deploying wireless this way, you alleviate the requirement for a controller at each remote site while still having the benefit of common management, security policy, and user experience regardless of where the user is logging into the network.

The first step in this process is to configure a new controller in the data center for N+1 failover. The "N" indicates the controller (or controllers) that service the desired number of APs that we have in our network and the "+1" is the single controller that can take that capacity should any active controller fail. This failover controller needs to have the same SSIDs, security policy, and features as the primary controller. The only difference between the active controller and the failover is the VLANs to which the WLANs will be connected.

There are a few technologies that we are deploying that are important to understand. Each of these technologies and features bring together a complete solution that is robust, flexible, and easily managed.

Figure 48. Mobility Group Member Configuration Screen



Wireless Local-Area Network

Cisco uses wireless local-area networks (WLANs) to separate services, security postures, and broadcast domains in much the same way a wired virtual local-area network (VLAN) would be utilized. Often, the use of the Service Set Identifier (SSID) and WLAN will be interchanged in this and other Cisco documents.

Hybrid Remote Edge Access Point

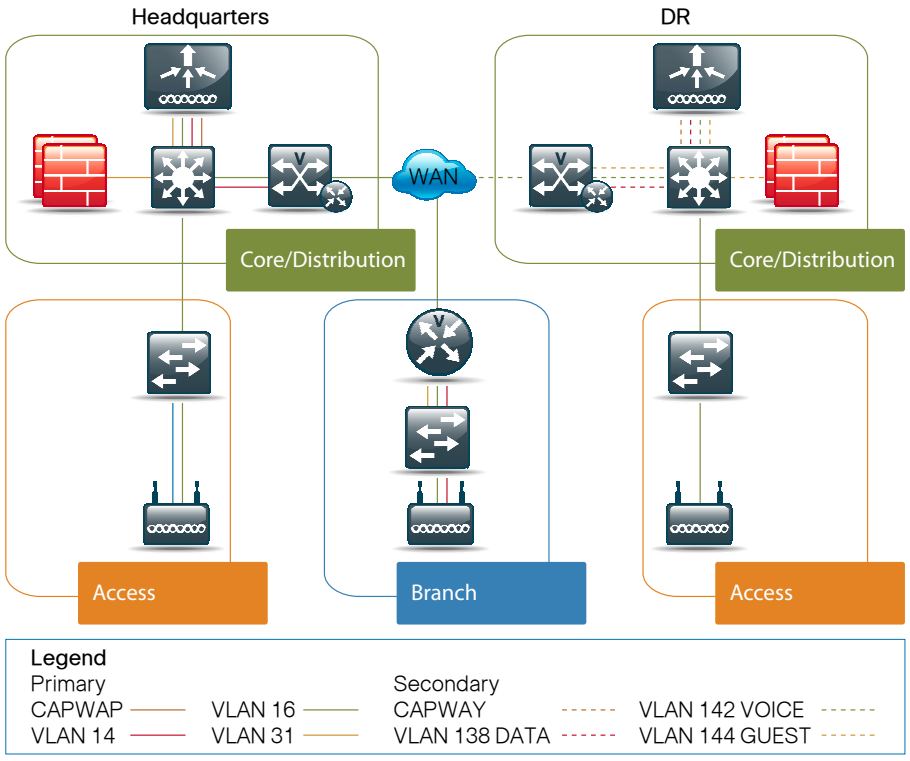
Hybrid Remote Edge Access Point (H-REAP) is a method of deploying an access point to allow connections to stay up even when connection to the WLC is lost. While the WLC is down, new clients cannot connect and existing

clients cannot renew encryption keys or "rekey." During normal operation, the central WLC maintains control of the configuration, authentication, and software of the APs, which gives the IT manager complete control of management and policy while maintaining a high degree of user flexibility.

Mobility Groups

Mobility groups and mobility members are the controllers that share client and other information. Anytime there is more than one controller in a wireless domain, they must know about each other. If the primary controller were to lose connectivity or fail, the secondary controller will pick up where the primary left off by assuming control of all connected access points in the network.

Figure 49. Resilient Wireless Overview



The following dependencies apply to this design. All controllers must:

- Be running the same software version.
- Have the same SSIDs/WLANs.
- Have the same mobility group configuration.

Tech Tip

IEEE 802.11 is a set of standards that carry out wireless local-area network (WLAN) computer communication in the 2.4, 3.6, and 5 GHz frequency bands. Today, the most common version of the standard in use is 802.11b and 802.11g, with a maximum raw data rate of 11 Mbit/s and 54 Mbit/s, respectively. The newest standard is 802.11n with the expected maximum raw data rate of 50-144 Mbit/s, which will significantly enhance the wireless throughput for applications such as real-time video.

Process

Configuring Resilient Wireless

1. Configure the Switch in the Advanced Server Room
2. Configure the Wireless Module
3. Complete Optional Tuning

Procedure 1 Configure Advanced Server Room Switch

Step 1: Configure the switch in the Advanced Server Room that will be connected to the secondary controller as earlier, but with the VLANs 136, 138, 140, 142, and 144 as shown:

```
interface Port-channel11
  description WLAN Controller
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 136,138,142,144
  switchport mode trunk
```

Use Gigabit Ethernet 6/0/13 and 7/0/13 as your physical connected interfaces.

Step 2: Configure your secondary controller by repeating the configuration steps from earlier with the following information:

```
Management interface: 192.168.136.64
AP Manager Interface: 192.168.136.65
Voice (SBAVoice) WLAN interface: 192.168.142.5/24
Default Gateway: 192.168.142.1
DHCP Server: 192.168.152.10

Data (SBAaccess) WLAN interface: 192.168.138.5/24
Default Gateway: 192.168.138.1
DHCP Server: 192.168.152.10

Guest (Guest) WLAN interface: 192.168.144.5/24
Default Gateway: 192.168.144.254
DHCP Server: 192.168.136.64

DHCP Pool for your guest network
192.168.144.10 thru 192.168.144.100
Default Gateway: 192.168.144.254
DNS Server: (provided by your service provider)
```

Step 3: Configure your mobility group on each controller.

Controller>Mobility Management>Mobility Groups

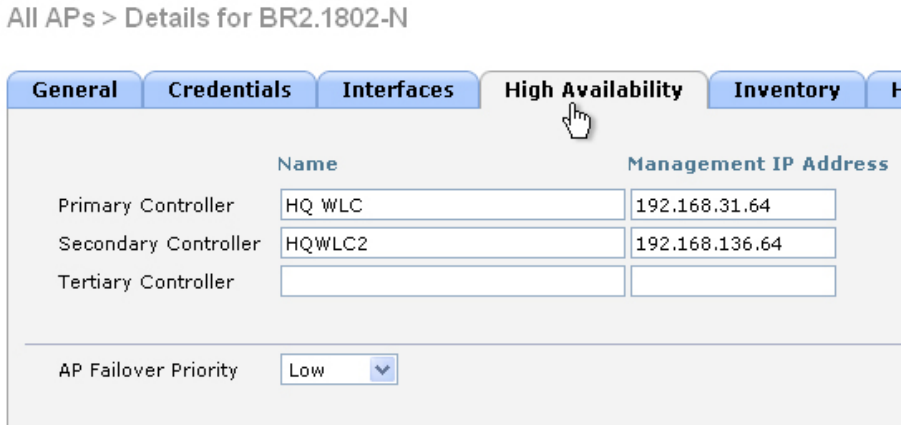
Procedure 2 Configure the Wireless Module

Step 1: Enter the controller MAC address, IP address, and **default** as your mobility group as configured earlier on each controller and click **Apply**.

Step 2: Configure High Availability on each access point in your network.

Wireless>AP-Name>High Availability (tab)

Figure 50. AP Wireless LAN Controller HA Configuration



There is no need to set a failover priority as each WLC has enough capacity for all APs in the network. If this were not the case, it is possible to specify which APs have priority during failover.

Procedure 3 Complete Optional Tuning

You may tune your network to optimize your failover to improve AP failover time.

Step 1: Apply the output below, which shows the default timeout of the AP should the WLC become unreachable within 120 seconds.

```
(Cisco Controller) >show advanced timers

Authentication Response Timeout (seconds).....10
Rogue Entry Timeout (seconds).................1200
AP Heart Beat Timeout (seconds)...............30
AP Discovery Timeout (seconds)................10
AP Local mode Fast Heartbeat (seconds)........disable
AP Hreap mode Fast Heartbeat (seconds)........disable
AP Primary Discovery Timeout (seconds)........120
```

Step 2: Move the discovery timeout to 60 seconds and set the backup controller globally.

```
(Cisco Controller) >config advanced timers ap-primary-
discovery-timeout 60
Warning! Setting AP primary discovery timer does not apply to
Mesh APs.Apply(y/n)?y

(Cisco Controller) >show advanced timers

Authentication Response Timeout (seconds).....10
Rogue Entry Timeout (seconds).................1200
AP Heart Beat Timeout (seconds)...............30
AP Discovery Timeout (seconds)................10
AP Local mode Fast Heartbeat (seconds)........disable
AP HREAP mode Fast Heartbeat (seconds)........disable
AP Primary Discovery Timeout (seconds)........60
(Cisco Controller) >config advanced backup-controller
primary HQWLC2 192.168.136.64
(Cisco Controller) >show advanced backup-controller

AP primary Backup Controller .....HQWLC2 192.168.136.64
AP secondary Backup Controller ...0.0.0.0
```

Notes

Resilient Unified Communications Design

Agency Overview

In the event of a failure that makes user services provided by the HQ data center unavailable, some, if not all, user services may need to be provided from a backup location. Which user service this is required for will vary based on what is considered critical to the operation of the agency.

This section will focus on the telephony service provided by the SBA foundation and how to extend seamless service from either the headquarters data center or the disaster recovery data center. The foundation architecture provides two levels of resiliency for the telephony service by utilizing a backup Cisco Unified Communications Manager appliance and integrated Survivable Remote Site Telephony (SRST) within the ISR at the remote site. In the event of server connectivity or WAN failure, the telephony system automatically fails over to another part of the system without user or administrator intervention. Should the HQ data center fail, the telephony services will automatically fail over to the appliance in the disaster recovery data center.

The foundation Unified Communications Module in the *Cisco SBA for Midsize Agencies—Borderless Networks Foundation Deployment Guide* utilizes Active Directory and may also rely on DNS for connectivity to this service. These services, therefore, also need to be available while operating at the disaster recovery Data Center when the HQ site is offline.

Access to the Public Switched Telephone Network (PSTN) and media resources for the HQ site users can be provided by the disaster recovery site. The ISR located there can be deployed with the same integrated services deployed in the HQ ISR to provide conference bridges and the PSTN gateway function. Although the additional gateway is provided, there is normally a requirement to move the Direct Inward Dialing (DID) numbers from the gateway at the HQ site to a gateway at the disaster recovery site. This operation requires coordination with the service provider and will not be covered in this deployment guide.

Technical Overview

The Cisco Unified Communication Managers are deployed in a cluster at the HQ site to provide resiliency. This is a two-node cluster and will be extended to a three-node cluster, with the third node across the WAN at the disaster recovery site. The Cisco Unity® Connection is a single node that supports clustering with a latency of 10 ms and must be on the same LAN as the other node. Cisco Unity Connection is not deployed as a highly available voice messaging system as part of this data center disaster recovery deployment.

By following the node installation steps in the Rapid Deployment Method document that is part of the *Cisco SBA for Midsize Agencies—Borderless Networks Foundation Deployment Guide*, the third Cisco Communications Manager can be deployed using the steps for "Second Node." Once completed, along with the additional steps in this module, all telephony devices will use CUCM2 as their primary node, then CUCM1 should CUCM2 be unavailable. In the event that both CUCM1 and CUCM2 are unavailable, as would be the case during a major failure at the HQ site, they will use CUCM3 that is located at the disaster recovery site.

One of the advantages of the disaster recovery telephony node being a member of the same cluster as the HQ nodes is that they share the same configuration information contained in the primary or first node database. This information is downloaded to the new node during the installation process and synchronized when any changes are made. As failures occur or resolve, the various devices will fail over automatically and also fall back to the higher-priority nodes with no user or administrative intervention required.

Although additional resiliency has been added at the user service layer, we still rely on network services and the network to be highly available and provide the same level of functionality. Without the underlying layers, the ability of the user services to function correctly may be severely impacted.

Network Foundation Layer

The network layer is the foundation for every other layer. For this deployment, there are specific requirements that need to be met for supported operation, including the following:

- The link between the HQ data center or server farm and the disaster recovery site must ensure the latency between the Unified Communications servers is below 80 ms roundtrip and has sufficient bandwidth to allow QoS to be configured with enough queues and bandwidth to support the traffic between the nodes in the cluster.
- A minimum of 1.5 Mbps must be allocated to the CS3 or signaling queue. The actual bandwidth could be higher depending on call volume.

The secondary or backup links from the remote sites to the disaster recovery site also need sufficient bandwidth to support the same quantity of signaling, voice, and video traffic as the primary links.

Ideally, the secondary links should be equal in size to the primary links as this allows the Call Admission Control to be simplified. If there are differences in the primary path and the secondary paths' bandwidth for voice and video calls, the use of a different technology may be required. The Resource Reservation Protocol (RSVP) is more suited to this scenario and is covered in the Unified Communications Solution Reference Network Design (SRND). Although outside the scope of this deployment guide, RSVP may be used to solve this design problem.

Network Services

There are a few network services that the Unified Communications system relies on for its own operation and to provide a quality experience for the users.

QoS was configured as part of the foundation for the primary links and should be configured on the backup paths as well. This may, of course, be a problem if the backup path is over a non-QoS-enabled service, such as the Internet. In that case, QoS should be configured on the egress interface of each site so that signaling and voice traffic is prioritized ahead of the data packets. Although there will be no guarantee during congestion, configuring QoS will overcome some of the latency and jitter that would be introduced without it.

As many applications and services rely on DNS and Active Directory, both of these services must also be available at the disaster recovery site and need to be configured in the Cisco Unified Communications Manager so any host name resolution or user authentication and synchronization will continue while the HQ site is unavailable.

The following section will walk you through the additional configuration required in the Cisco Unified Communications Manager and also the additional configuration required in the ISRs that have the integrated media resources and PSTN gateway services.

Process

Configuring the Unified Communications Manager

1. Verify and Optionally Configure the Secondary DNS
2. Add a Backup Active Directory
3. Add CUCM3
4. Configure a Disaster Recovery Site Subnet
5. Provide Annunciator and Music-on-Hold from the DR Site
6. Configure Site-Specific Media Resource Group List
7. Configure Additional Resources

Using the Rapid Deployment Method (RDM) and following the first section that guides you through the installation of the software and activation of the services, we can quickly add our extra node that is located at the disaster recovery site.

To complete the node installation phase, however, you need the IP address, subnet mask, and gateway for CUCM3. CUCM3's hostname must be added to the primary DNS server and allowed to replicate to the DNS server located at the disaster recovery site. The Cisco Unified Communications Manager license needs to be updated to add an additional node, making a total of three.

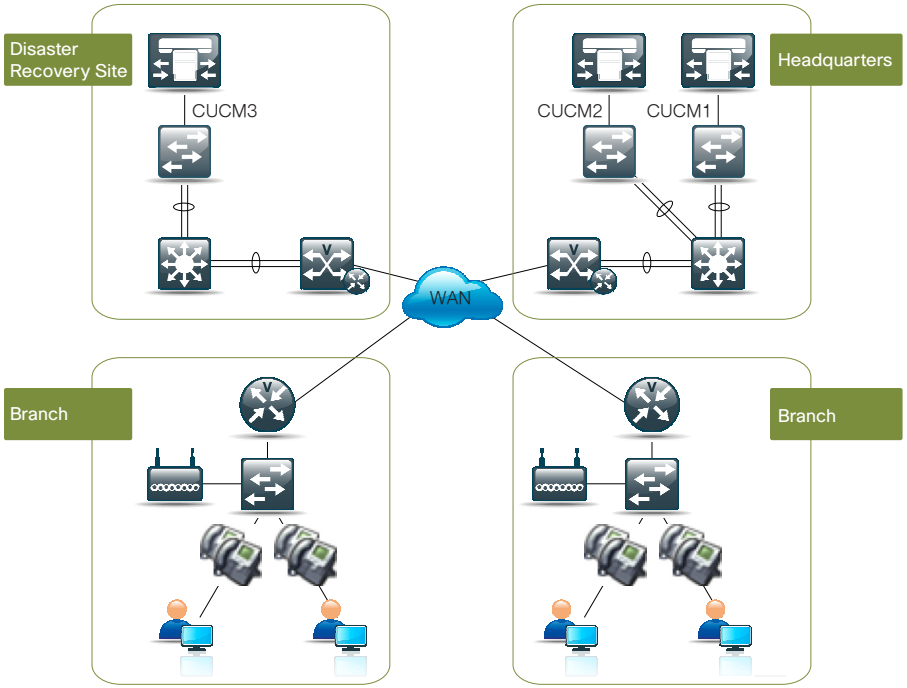
The following information was used for the deployment example:

```
Cisco Unified Communications Manager Hostname cucm3.cisco.local
IP Address                192.168.152.20
Netmask                   255.255.255.0
IP Gateway                192.168.152.1
Primary AD Hostname       ad.cisco.local
Primary DNS Address       192.168.28.10
Secondary AD hostname     dr-ad.cisco.local
Secondary DNS Address     192.168.152.10
```

Use the Platform Installation section in RDM to install and activate the additional node.

CUCM1 and CUCM2 should both use the HQ site DNS as the primary DNS server and, optionally, can have the disaster recovery site DNS server as the secondary. CUCM2 should have the disaster recovery site DNS as the primary and, optionally, have the HQ site DNS as the secondary.

Figure 51. Resilient Unified Communications Overview



Procedure 1 Optionally Configure the Secondary DNS

Step 1: Verify the DNS setting by logging into the console of each node and using the following show command to verify the settings:

```
show network eth0
```

Step 2: Use the following commands to add or modify the DNS configuration:

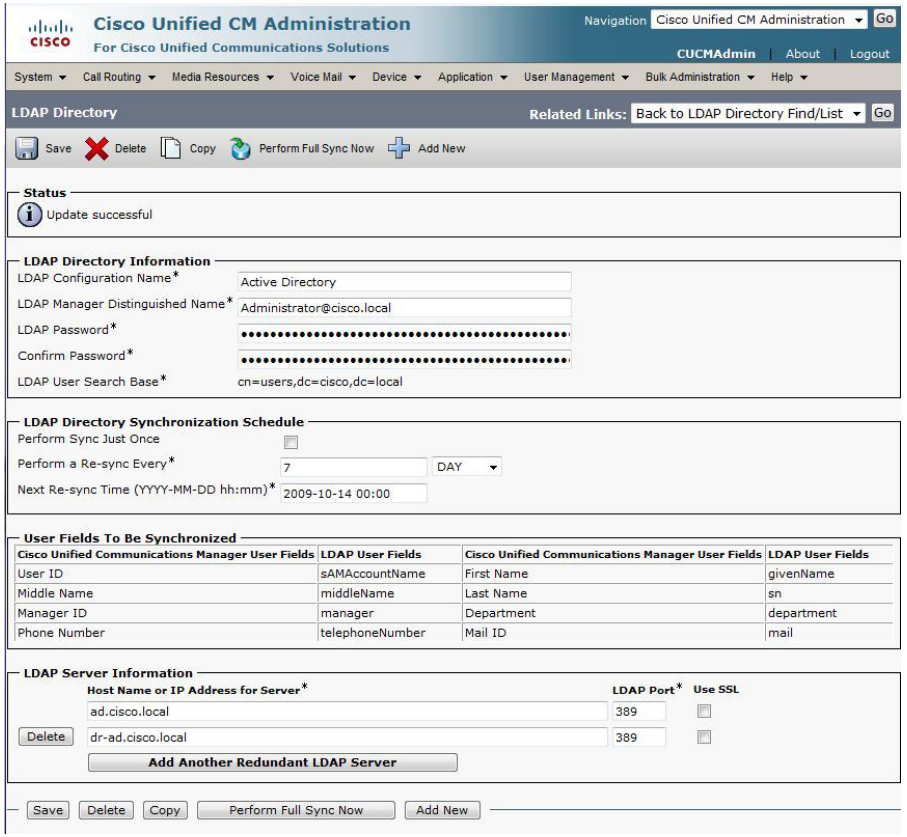
```
set network dns primary
set network dns secondary
```

Procedure 2 Add a backup Active Directory

Step 1: Select **System** > **LDAP** > **Directory** from the Cisco Unified CM Administration interface.

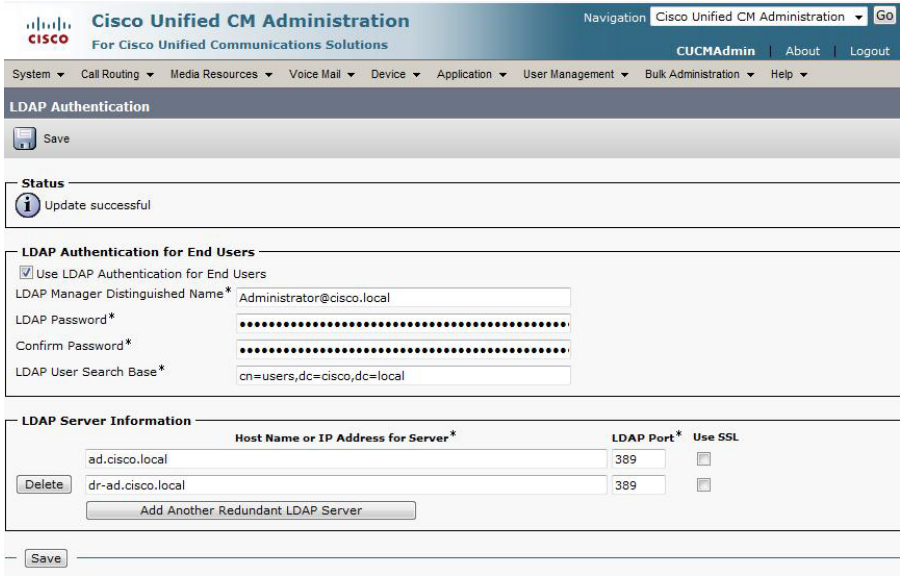
Step 2: Select the LDAP directory that is already configured and then click **Add Another Redundant LDAP Server**. Enter the backup Active Directory Hostname and then click **Save**.

Figure 52. LDAP Directory



Step 3: Select **System** > **LDAP** > **Authentication** and click **Add Another Redundant LDAP Server**, enter the backup Active Directory hostname, and then click **Save**.

Figure 53. LDAP Authentication



Procedure 3 Add CUCM3

Add CUCM3 as the third option for registering devices.

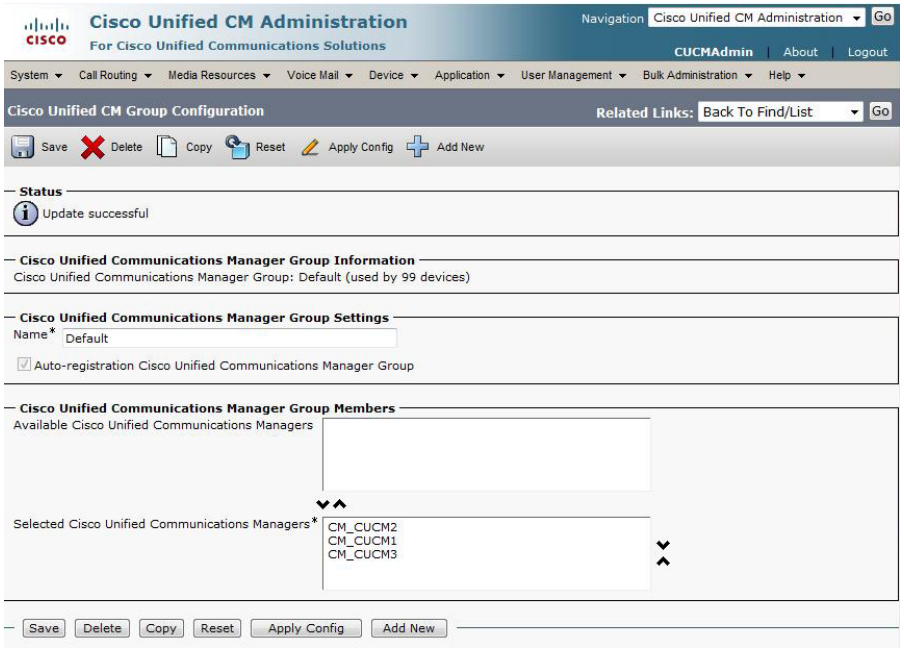
Step 1: Select **System** > **Cisco Unified CM Group** and click **Find**.

Step 2: Select the **Default** group.

Step 3: From the Available Cisco Unified Communications Managers box, select **CUCM3** and move it to the last entry in the Selected Cisco Unified Communications Managers box.

Step 4: Click **Save**.

Figure 54. Cisco Unified CM Group Configuration.



Procedure 4 Configure a Disaster Recovery Site Subnet

Complete the following steps to ensure correct device profiles are associated with devices located at the disaster recovery site.

Step 1: Select **System** > **Device Mobility** > **Device Mobility Info**.

Step 2: Select **Add New** and enter the:

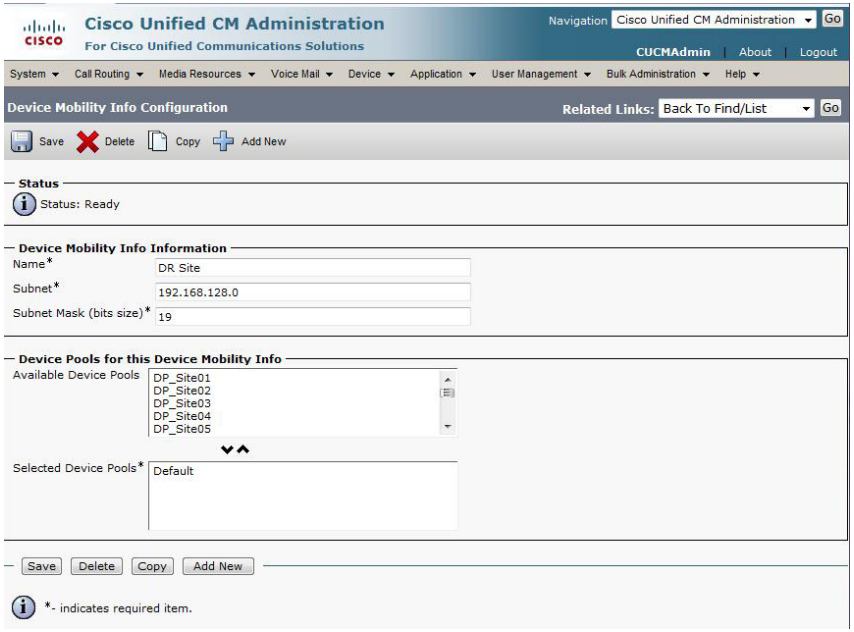
- Name (name of the disaster recovery site)
- Subnet (the network address for the site)
- Subnet Mask (number of bits to cover all subnets)

To cover all subnets with one Device Mobility Information entry, define the Subnet and Subnet Mask to include all subnets at the disaster recovery site by using classless inter-domain routing (CIDR).

Step 3: Select the **Default device pool** from the Available Device Pools selection box and move it to the Selected Device Pools box.

Step 4: Click **Save**.

Figure 55. Device Mobility Info Configuration



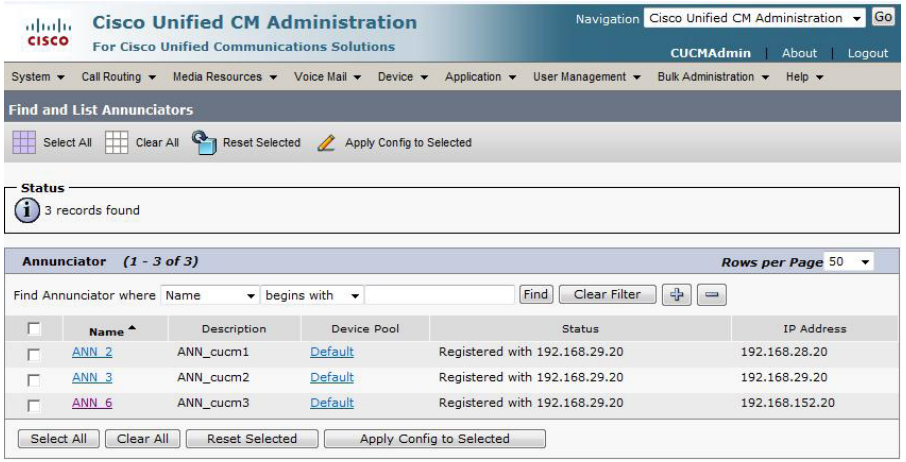
Procedure 5 Provide Annunciator & MoH from DR Site

Configure the media resources provided by CUCM3 to provide Annunciator and Music-on-Hold from the disaster recovery site.

Step 1: Select **Media Resources** > **Annunciator** then click **Find**.

Step 2: In the resulting list, note the name of the Annunciator associated with CUCM3's IP address, for example, ANN_6.

Figure 56. Find and List Annunciators



Step 3: Select **Media Resources** > **Media Resource Group**.

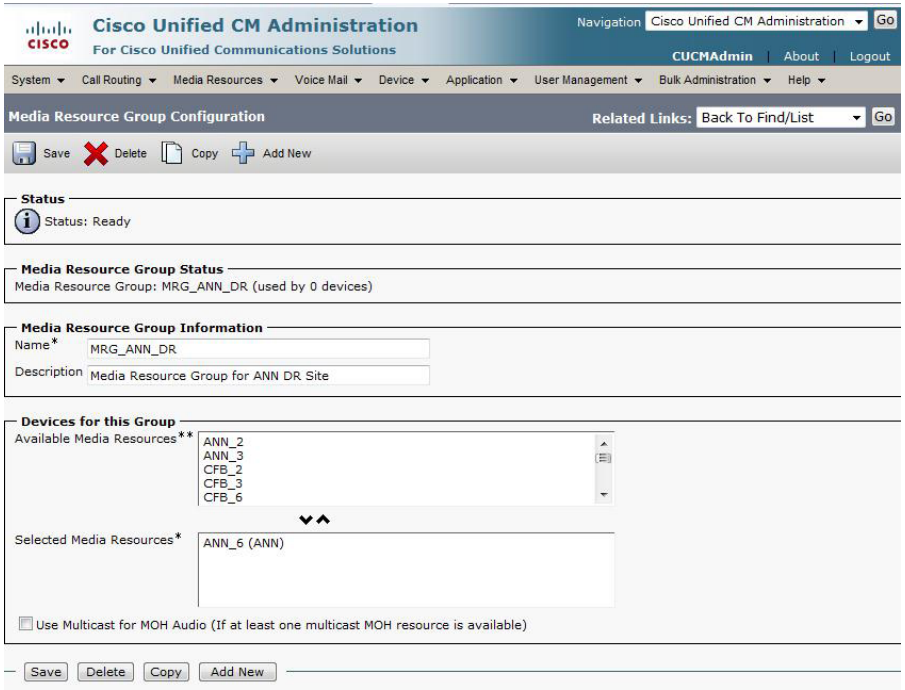
Step 4: Click **Add New** and enter the:

- Name (for example: MRG_ANN_DR)
- Description

Step 5: Select the correct Annunciator from the Available Media Resources box and move it to the Selected Media Resources box.

Step 6: Click **Save**.

Figure 57. Media Resource Group Configuration



Step 7: Select **Media Resources** > **Music-on-Hold Server** and click **Find**.

Step 8: In the resulting list, note the name of the Music-on-Hold Server associated with CUCM3's IP address, for example: MOH_6

Procedure 6 Configure Media Resource Group List

The previously added Media Resource Groups need to be added to each site-specific Media Resource Group List. Use the following steps to add this for Site01, which is the remote site. Then, repeat the steps for all sites that will utilize the disaster recovery site.

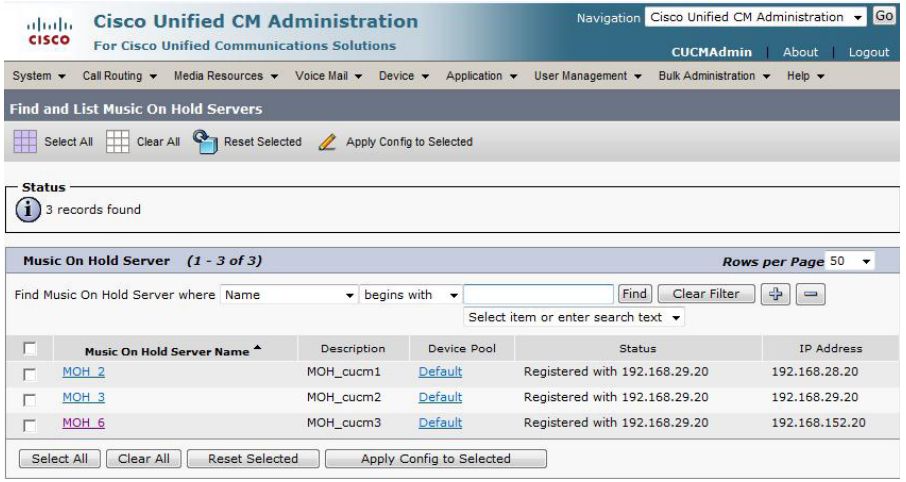
Step 1: Select **Media Resources** > **Media Resource Group List** then click **Find**.

Step 2: Select the site-specific MRGL (MRGL_Site01).

Step 3: Select the MRGs created earlier from the Available Media Resource Groups box and move them to the Selected Media Resource Groups box, ensuring they are the last two in the list.

Step 4: Click **Save**.

Figure 58. Find and List Music-on-Hold Servers



Step 5: Select **Media Resources** > **Media Resource Group**.

Step 6: Click **Add New** and enter the following:

- Name (for example: MRG_MOH_DR)
- Description

Step 7: Select the correct Music-on-Hold Server from the Available Media Resources box and move it to the Selected Media Resources box.

Step 8: Click **Save**.

Figure 59. Media Resource Group List Configuration

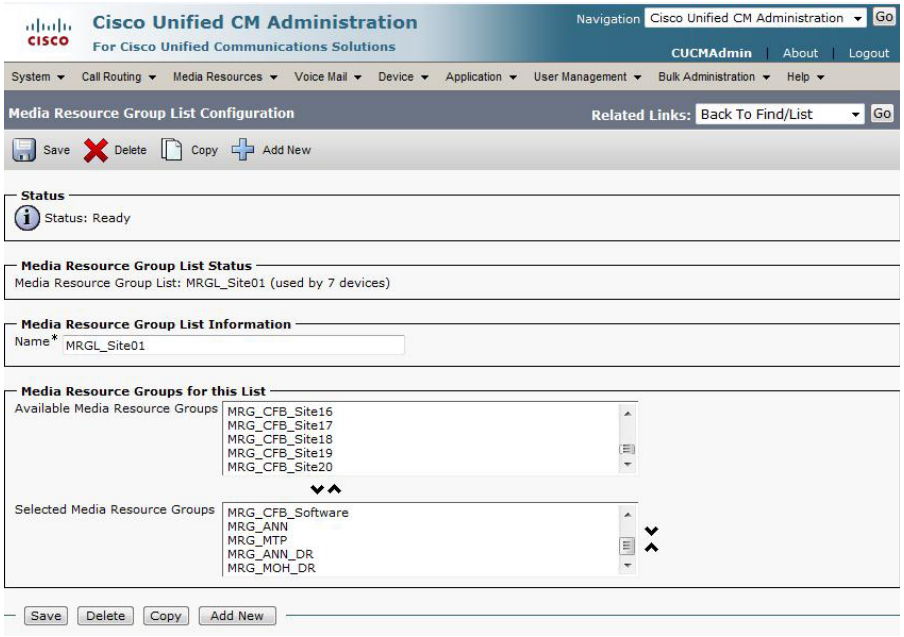
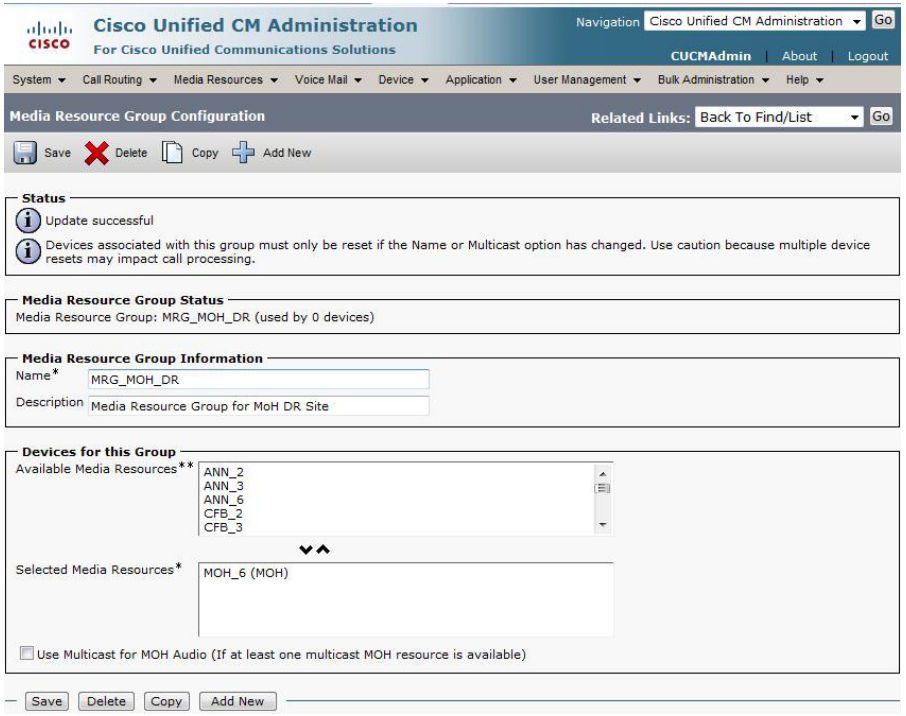


Figure 60. Media Resource Group Configuration



This completes the configuration required in the Cisco Unified Communications Manager.

Procedure 7 Configure Additional Resources

Within each ISR at the HQ and the remote sites, there are a PSTN gateway and media resources, such as conference bridges, that need to be aware of the additional Cisco Unified Communications Manager node.

Step 1: Add another dialpeer to the SIP gateway that has a lower preference than the ones that target CUCM1 and CUCM2:

```
dial-peer voice 102 voip
  description SIP TRUNK to CUCM3
  preference 3
destination-pattern 1408555....
  voice-class codec 1
  session protocol sipv2
  session target ipv4:192.168.152.20
  incoming called-number .
```

Step 2: Add the following command to the Skinny Client Control Protocol (SCCP) configuration to define CUCM3's IP address:

```
sccp ccm 192.168.152.20 identifier 3 priority 3 version 7.0
```

Step 3: Next, the SCCP group needs to have the newly defined CCM associated. Modify sccp ccm group 1 and add the additional associate command with the priority to ensure it is used as last.

```
sccp ccm group 1
associate ccm3 3 priority 3
```

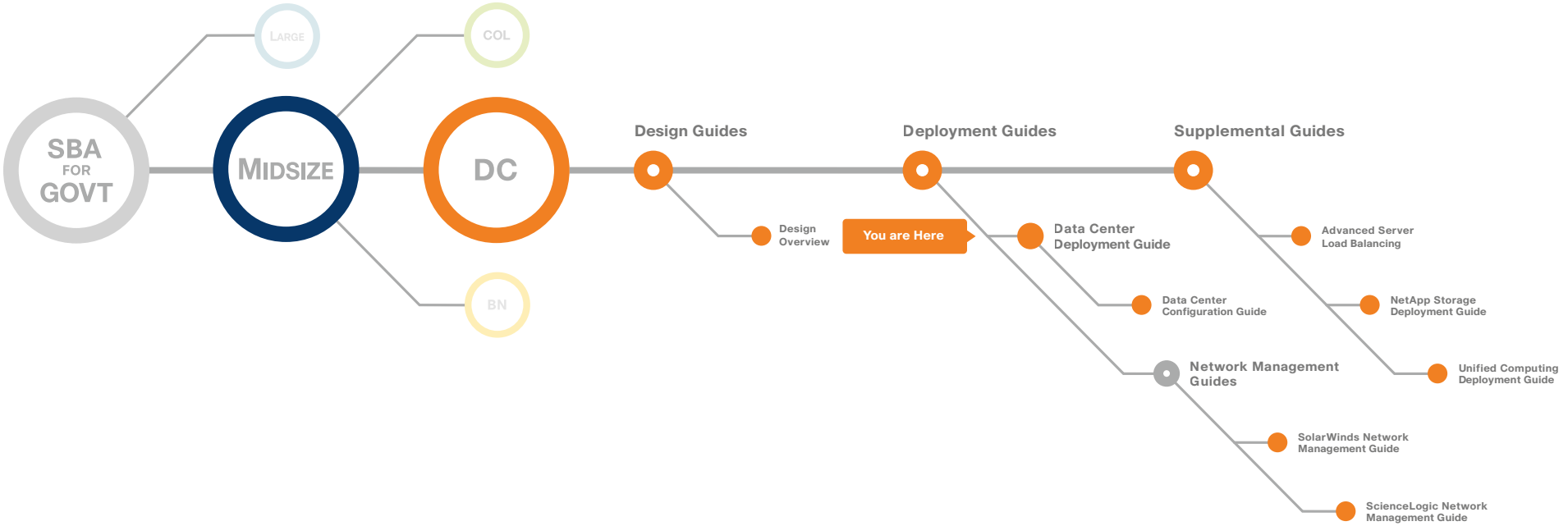
Step 4: Repeat these modifications for all ISRs at sites that utilize the disaster recovery site.

Notes

Appendix A:
Data Center for Midsize Agencies Product List

Functional Area	Product	Part Numbers	Software Version
Virtualized Storage	MDS 9124	DS-C9134-K9	3.3(2)
	MDS 9134	DS-C9124-K9	4.1(1c)
	4-Gig SFP	DS-SFP-FC4G-SW	
Data Center Switching	Catalyst 3750G	WS-C3750G-24TS-S1U	12.2-40.SE
	Nexus 5010	N5K-C5010P-BF	4.1.(3)
	Nexus 2148T	N2K-C2148T-1GE	4.1(3)
Application Services	Application Control Engine (ACE) 4710 Appliance	ACE-4710-0.5F-K9	A3.2.2
Application Services Wide-Area Application Services (WAAS)	HQ CM WAAS Apliance	WAVE-274-K9	All use 4.1.3b
	HQ AA WAAS Appliance	WAVE-574-K9	
	Remote Site WAAS Network Module	NME-WAE-502-K9	
Wireless	Wireless LAN Controller 5508	AIR-CT5508-100-K9	AIR-CT5500- K9-6-0-188-0.aes
Wireless Access Points	1140 Fixed with Internal Antennas	AIR-LAP1142N (Country-specific)	Controller-Based Software
	1250 Ruggedized, External Ant.	AIR-LAP1252AG (Country-specific)	
Security	HQ Site		
	2x ASA5540 w/ ASA-SSM-40	ASA5540-AIP40-K8	ASA software: 8.2.2
	DR Site		IPS software: 7.0.2E3
	2x ASA5580-20	ASA5580-20-8GE-K8	
	2x IPS-4260-K9	PS-4260-K9	

Appendix B:
SBA for Midsize Agencies Document System



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

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

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

C07-641157-00 12/10