Newer Cisco SBA Guides Available

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

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

Foundation Deployment Guide

SMART BUSINESS ARCHITECTURE

February 2012 Series

Preface

Who Should Read This Guide

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

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

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

Release Series

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

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

month year Series

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

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

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

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

How to Read Commands

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

Commands to enter at a CLI appear as follows:

```
configure terminal
```

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

```
ntp server 10.10.48.17
```

Commands with variables that you must define appear as follows:

```
class-map [highest class name]
```

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

```
Router# enable
```

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

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

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

```
interface Vlan64
  ip address 10.5.204.5 255.255.255.0
```

Comments and Questions

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

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

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

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

Table of Contents

What's In This SBA Guide 1
About This Guide 1

Introduction 2
Design Goals 4
Business Overview 4
Technical Overview 5

Global Configuration Module 10
Technical Overview 10
Applying Global Configuration 10
IP Subnet and VLAN Assignment 13

LAN Module 15
Technical Overview 15
LAN Core 16
Deployment Details 19
Configuring the LAN Core 19
LAN Access 29
Configuring the Access Layer 31
Server Room 37
Configuring the Server Room LAN 38

Security Module 43
Technical Overview 43
Deployment Details 46
Configuring firewall for Internet access for internal network 47
Configuring Internet Edge Cisco ASA for DMZ Services 54
Configuring Internet Edge Cisco ASA for Guest WLAN Service 59
Configuring Cisco ASA for the Server Room 64
Deploying Cisco Intrusion Prevention System 72
Configuring AnyConnect Client Remote-Access VPN 83

Wide-Area Network Module 91
Technical Overview 91
Deployment Details 92
Configuring the Headquarters WAN Router 93
Configuring the Remote-Site WAN Routers 98
Configuring the Remote-Site LAN Access Switch 102

Wireless Module 106
Technical Overview 106
Deployment Details 107
Configuring Wireless LAN Connectivity to the Core 107
Initializing the Wireless Controllers 109
Configuring WLCs for Voice and Data Access 114
Connecting APs to the Headquarters LAN 118
Configuring Remote-Site Wireless Access 119
Configuring Guest Access 124
Application Optimization Module 130
Technical Overview 130
Deployment Details 132
Configuring the Cisco WAAS Central Manager 132
Configuring the WAAS Headend Appliances 135
Configuring the Cisco WAAS Remote-Site Appliances 138
Configuring WCCP on the WAN Routers 141
Server Load Balancing Module 144
Technical Overview 144
Deployment Details 146
Configuring Cisco ACE 146
Appendix A: Midsize Organizations Deployment Product List 149
Appendix B: RADIUS Authentication with Windows Server 2008 153
Installing Active Directory Certificate Services and Network Policy Services 153
Appendix C: Changes 168

What's In This SBA Guide

About SBA

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

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

For more information, see the *How to Get Started with Cisco SBA* document:

http://www.cisco.com/en/US/docs/solutions/Enterprise/Borderless_Networks/Smart_Business_Architecture/SBA_Getting_Started.pdf

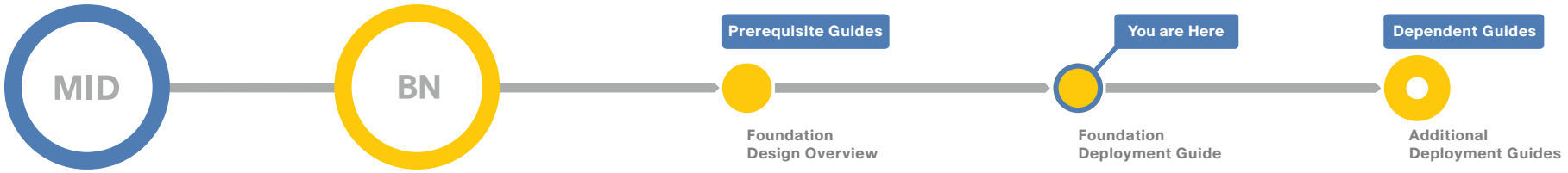
About This Guide

This *foundation deployment guide* is organized in sections, which each include the following parts:

- **Business Overview**—The challenge your organization faces. Business decision makers can use this part to understand the relevance of the solution to their organizations' operations.
- **Technology Overview**—How Cisco solves the challenge. Technical decision makers can use this part to understand how the solution works.
- **Deployment Details**—Step-by-step instructions for implementing the solution. Systems engineers can use this part to get the solution up and running quickly and reliably.

To learn what changed in this guide between the previous series and the current series, see Appendix C: Changes.

This guide presumes that you have read the prerequisite foundation design overview, as shown on the Route to Success below.



Route to Success

To ensure your success when implementing the designs in this guide, you should read any guides that this guide depends upon—shown to the left of this guide on the route above. Any guides that depend upon this guide are shown to the right of this guide.

For customer access to all SBA guides: http://www.cisco.com/go/sba
For partner access: http://www.cisco.com/go/sbachannel

Introduction

The Cisco® Smart Business Architecture (SBA) is a comprehensive design for networks with up to 2500 users. This out-of-the-box design is simple, fast, affordable, scalable, and flexible. There are three options based on your scaling needs: up to 600 users, up to 1000 users, and up to 2500 users.

The Cisco SBA for Midsize Organizations incorporates LAN, WAN, wireless, security, WAN optimization, and unified communication technologies tested together as a solution. This solution-level approach simplifies the system integration normally associated with multiple technologies, allowing you to select the modules that solve your organization's problems rather than worrying about the technical details.

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

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

The *Cisco SBA for Midsize Organizations—Borderless Networks Foundation Deployment Guide* includes the following modules:

- The first module, the Global Configuration Module, covers configuration of the elements that are universal among many, if not all, of the devices in the solution. As an example, Secure Shell (SSH) Protocol setup can be used throughout the design for secure remote management of devices.
- The LAN Module includes guidance for all segments of the organization LAN. The LAN Core section focuses on that portion of the LAN that serves as the central aggregation for all user access switching at the headquarters, and serves as the interconnect point for the WAN and server room. The LAN Access section explains how to configure the LAN switches at headquarters and remote sites for desktop computer, phone, and other device connectivity. The Server Room section explains the configuration of server ports on the switches, VLAN usage and trunking, resiliency, and connectivity to the LAN core.
- The Quality of Service (QoS) Module is integrated throughout the document and provides you with guidance on protecting your traffic as it crosses the network. The LAN and WAN modules walk you through the steps for deploying this critical service.
- The Security Module focuses on the deployment of firewalls and advanced security services to protect the information assets of your organization. The Cisco Intrusion Prevention System (IPS) section explains how to install Cisco IPS, which monitors your network for intrusions or attacks. The Remote Access VPN section explains how to provide secure remote access to your network for teleworkers and mobile users.
- The WAN Module includes the WAN aggregation at the headquarters, as well as the connectivity to remote locations. The WAN module also describes connectivity to the LAN infrastructure from those remote locations.
- The Wireless Module describes the wireless infrastructure for the headquarters and remote sites, its use for employees accessing the intranet and Internet, as well as secure guest-user access to the Internet.
- The Application Optimization Module shows you how to optimize the bandwidth between the headquarters and remote offices. By ensuring economical use of your IT resources, you can delay WAN upgrades or make room for new applications.
- The Server Load Balancing Module shows how to scale and provide additional resiliency for servers and applications.
- The Appendix provides the complete list of products used in the lab testing of this design, as well as the software revisions used on the products in the system.

The *Foundation Deployment Guide* is voice-ready because it includes the QoS settings, VLANs and IP subnets needed for voice endpoints. It also includes the Dynamic Host Configuration Protocol (DHCP) scopes for the voice VLANs.

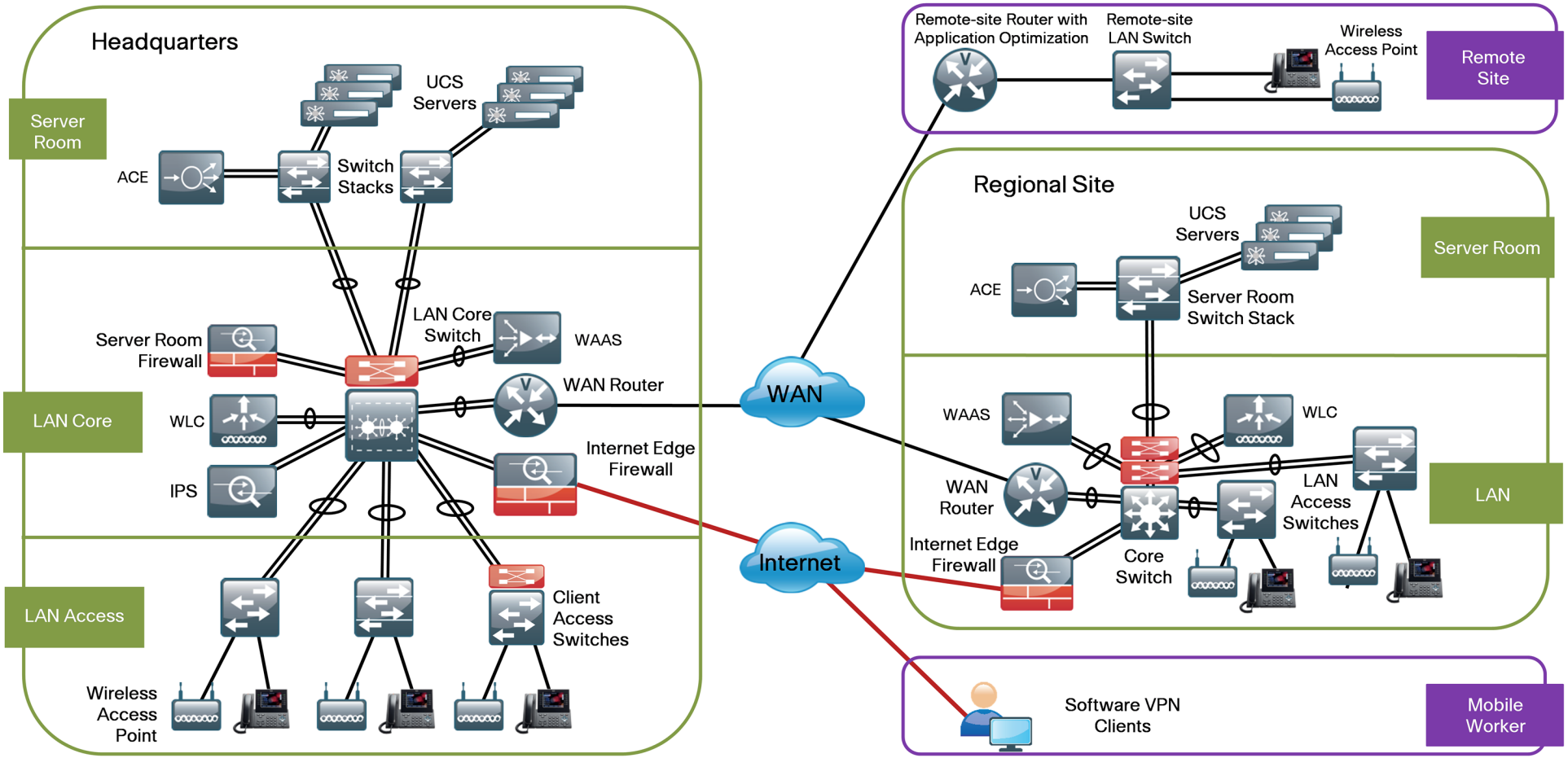
Reader Tip

For information about configuring the DHCP option that assigns the call control agent for voice endpoints, see the *Cisco SBA for Midsize Organizations—Collaboration Unified Communications Manager Deployment Guide*.

To enhance the architecture, there are also a number of supplemental guides that address specific functions, technologies, or features that may be important to solving your business problems.

Figure 1 illustrates the complete Cisco SBA for Midsize Organizations foundation design with all modules deployed.

Figure 1 - Network architecture baseline

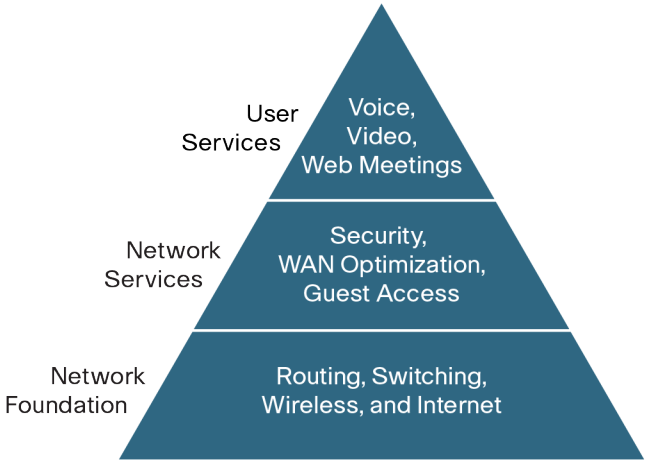


Design Goals

From the beginning, one of the primary concepts of this design has been the "modular concept." The deployment process is divided into modules according to the following principles:

- Ease of use—Develop a design that could be deployed with the minimal amount of configuration and day-two management.
- Cost-effectiveness—Meet the budget guidelines for a company of this size.
- Flexibility and scalability—Products must be able to grow or be repurposed within the architecture.

When possible, reuse the same products throughout the various modules to minimize the number of products required for spares.



Business Overview

The *Cisco SBA for Midsize Organizations—Borderless Networks Foundation Deployment Guide* is designed to address five primary needs of midsize organizations:

- To provide reliable access to organization resources
- To minimize time required to select and absorb technology investments
- To enable workforce mobility
- To provide guest and partner access
- To reduce operational costs

Provide Reliable Access to Organization Resources

Data networks are critical to organizations' ability to operate and compete. Online workforce-enablement tools only offer benefit if the data network provides reliable access to information resources. Collaboration tools and content distribution rely on high-speed, low-latency network infrastructure to provide an effective user experience. However, as networks become more complex, the level of risk increases for network-availability loss or poor performance due to inadequate design, configuration errors, maintenance and upgrade outages, or hardware and software faults. The design and methods used in this deployment guide were created to minimize these risks.

Minimize Time Required to Select and Absorb Technology Investments

New technology can impose significant costs, including the time required to select the proper equipment, the investment in the equipment, and the time and workforce investment that is required to deploy the new technology and establish operational readiness. Matching the correct equipment to solve business problems with the right mix of scalability, growth, and cost can be difficult given the number of choices in the market. When you introduce new technology, it takes time for you to understand how the technology operates and to ascertain how to effectively integrate the new technology into the existing infrastructure. Over time, you can refine the methods and procedures that you use to deploy a new technology to be more efficient and accurate.

This deployment guide eases your organization's cost of technology selection and implementation by providing recommended equipment appropriate for the midsize organization along with methods and procedures that have been developed and tested by Cisco. By applying the guidance within this document, you can reduce the time required to assimilate the technology into your organization's network and you can deploy the technology quickly and accurately, so that your organization can achieve a head start realizing the return on your investment.

Enable Workforce Mobility

The ability for a user to maintain productivity without being tethered to their desk for computer and telephone connectivity is driving increased efficiency into the operation of most organizations. By providing network access in a conference room without the need to run wires to every meeting-attendee, organizations can reduce infrastructure costs and enable a more productive environment. Organizations looking to control overhead costs by improving office space efficiency can use wireless mobility

features. For example, by sharing workspace between multiple users, reaching hard-to-wire locations for office space, or enabling ad hoc meetings in lunch rooms, organizations can maximize their workspace efficiency. Common network access at headquarters and remote locations means users can be productive regardless of their work location for the day.

This design provides mobility services that increase employee productivity by allowing users to move throughout the physical plant while maintaining access to their applications, and it controls costs by maximizing the use of office space.

Provide Guest and Partner Access

Organizations' facilities are frequently used by a wide range of guests, including customers, partners, and vendors. While they are on site, many of these guests desire network connectivity to gain access to permitted organizational resources, as well as VPN connectivity to their employer's network and the Internet so they can be as productive as possible. However, by offering guests the same level of network access as the organization's users an organization can be exposed to a significant risk. Additionally, variations in frequency and number of guests can cause difficulty predicting when and where the connectivity will be required. The design provides wireless service that offers authenticated guest access to the Internet without allowing access to the organization's internal resources.

Reduce Operational Costs

Organizations constantly pursue opportunities to reduce network operational costs, while maintaining the network's effectiveness for end users. Operational costs include not only the cost of the physical operation (power, cooling, etc.), but also the labor cost required to staff an IT department that monitors and maintains the network. Additionally, network outages and performance issues impose costs that are more difficult to quantify, in the form of loss of productivity and interruption of business continuity.

The network provided by this deployment guide offers network resilience in its ability to tolerate failure or outage of portions of the network, along with a sufficiently robust-yet-simple design that staff should be able to operate, troubleshoot, and return to service in the event of a network outage.

Technical Overview

The modules in this guide describe a design that enables communications across the organization. This section provides architectural guidance specific to the network components or services you need to deploy.

LAN Module

The LAN Core, as the hub of communications between all modules in the network, is one of the most important modules in the design. Although there are multiple Cisco products that can provide the functionality needed in the core—primarily fault tolerance and high-speed switching—this architecture provides flexibility so that the infrastructure can grow with the company.

The design offers three options:

- The first option supports up to 600 users with a resilient core-stack design using the Cisco Catalyst® 3750 switch.
- The second option targets the 1,000-user mark with a resilient Cisco Catalyst 4507RE chassis equipped with dual supervisor modules.
- The third option scales to 2500 users, with a pair of Cisco Catalyst 6500 switches configured in a resilient Virtual Switching System (VSS).

All three options provide the required fault tolerance and bandwidth capacity, as well as port density in terms of the number of physical ports needed to connect devices from the other modules. The actual product selected will be driven by the business needs and size of the organization:

- Up to 600 users—The Cisco Catalyst 3750 product line is a stackable Gigabit Ethernet switch that provides resilience and scalability via Cisco StackWise technology. In the basic design, we use a pair of stacked 12- or 24-port (depending on the required number of uplinks to other devices) Cisco Catalyst 3750 switches that use Small Form-Factor Pluggable transceivers to offer a port-by-port option of either twisted-pair or fiber-optic Gigabit Ethernet cables. The Cisco Catalyst 3750 core switch provides both Layer 2 and Layer 3 switching capabilities and is configured to route traffic between other modules in the LAN. As the organization grows to require more switch ports in the core, the Cisco Catalyst 3750 switch supports in-service stack-member addition to increase port capacity without the need to schedule an outage.

- Up to 1000 users—A design to support more users requires additional switching capacity and more ports to connect to the additional client LAN-access switches. For this design, we selected a resilient Cisco Catalyst 4507R+E switch equipped with dual supervisor modules, dual power supplies, and dual Ethernet blades to offer the fault tolerance needed in the core. Its flexible chassis design allows for different line-card options to match the number and speed of uplink ports required. Additional line cards can be added to the Cisco Catalyst 4507RE switch as bandwidth and port requirements increase.
- Scaling to 2500 users and beyond—As organizations continue growing, demand increases for larger numbers of high-speed ports and switching capacity. This need is addressed by a pair of Cisco Catalyst 6500 Series switches with VS-720 supervisor blades, configured in a highly-available VSS 1440. The Cisco Catalyst 6500 platform offers maximum flexibility for line-card configuration, high levels of port density for 10 gigabit connectivity, and very high forwarding rates for Layer 2 and Layer 3 switching to support larger organizations with lots of connected users at the headquarters site. This platform provides a basis for migration to the Cisco SBA for Enterprise Organizations—Borderless Network design.

Client LAN Access Module

The client LAN access switches address the primary responsibility of connecting end-users' devices to the network. The client LAN access design provides Layer 2 switching functionality for all connected endpoints, either directly through wired-Ethernet connections, or indirectly via connected wireless access points (APs). Switches must supply adequate bandwidth to every endpoint device, both on the access port and in the connection to the core.

Another important function of the LAN access switch role is supplying Power over Ethernet (PoE). PoE/PoE+ delivers power to IP telephones, wireless access points (APs), security cameras, and other low-power devices. PoE/PoE+-enabled endpoint devices receive network connectivity and power through a single twisted-pair Ethernet cable, which resolves the need to install power connections in locations such as ceilings for cameras and wireless APs. Including PoE in the design removes the added cost of re-engineering the network in the future as PoE devices are deployed.

The SBA for Midsize Organizations—Borderless Networks design accommodates LAN access-switching requirements through four product lines that offer 10/100/1000 access ports, Gigabit Ethernet and 10 Gigabit Ethernet uplinks, and PoE+. The following product choices are available:

- The Cisco Catalyst 2960-S Series is an economical fixed-configuration switch with stacking capability and multiple uplink options.
- The Cisco Catalyst 3560-X Series is a fixed-configuration, non-stackable switch with modular uplinks that provides flexibility and features for many access-level switching environments with low port-density requirements.
- The Cisco Catalyst 3750-X Series is a fixed-port stackable switch with modular uplinks that is capable of expansion.
- The Cisco Catalyst 4500 E-Series offers a flexible, chassis-based modular switch, with a wide range of line-card configuration options for large, high-density deployments.

Server Room/Advanced Server Room Module

Server room switches provide network connectivity for servers and appliances that offer network and user services to a variety of devices in the network. The server room design has two product lines to choose from: the Cisco Catalyst 3750-X and the Cisco Catalyst 3560-X switches. The Cisco Catalyst 3750-X offers flexible port density, online expandability, and fault tolerance through Cisco StackWise Plus capability. The Cisco Catalyst 3560-X switch offers a lower cost option for applications where switch resiliency is not a priority.

Both the server room method of network connectivity and the client LAN access method connect devices to the network; the difference between the two methods that changes the switch model is the requirement in the LAN access method for PoE. While PoE-capable device are not typical in the server room, using PoE-capable switches offers a benefit worth considering: the minor initial cost savings of a non-PoE switch may not be worth the benefits of using the same switch across multiple modules. Although configurations differ between LAN access switches and server room switches, the ability to use a single switch type between multiple modules can lower operational costs by allowing for simpler sparing and management, as well as provide a better chance of reuse as the organization grows.

QoS Module

In a network where multiple applications share a single transport, you need to provide varying levels of service to guarantee satisfactory application performance. Real-time traffic, like voice, is very delay-and-drop sensitive. Therefore you must handle it with priority so that the data stream is not interrupted. QoS provides the organization with the ability to define different traffic types for both data and multimedia applications and to create more deterministic handling for real-time traffic and levels of priority for critical business applications.

In the LAN, the need for QoS is less evident due to the available high bandwidth, Gigabit and 10-Gigabit Ethernet, but even high-speed LANs have congestion points where packets can be delayed or dropped in buffers to manage traffic flow. In the WAN, the need for QoS is much more evident as the difference in available bandwidth as you leave the LAN to cross the WAN can be very large and creates congestion points as you cross from high to low bandwidth. It is important to note that QoS cannot create bandwidth; rather, it takes bandwidth from one class to give to another class with higher priority.

QoS is an important part of the foundation design as it allows organizations to combine separate voice and data networks onto a single IP-based transport. To ensure that the design is easy to use, Cisco keeps QoS as simple as possible to maintain correct operation of the real-time traffic on the network and to allow the organization to customize it if desired to classify specific business-critical application handling. QoS is integrated throughout the design and the steps to configure QoS are in modules that require device-specific configuration.

The QoS design provides the guidance necessary to:

- Establish a limited number of classes to map applications.
- Handle different classes of service with bandwidth and priority policies.
- Map the policies to LAN and WAN interfaces to achieve intended results.

This approach establishes a solid baseline that is scalable to handle the expanding needs of the organization.

Security Module

Within the design, there are many requirements and opportunities to include or improve security. The deployment guide will cover software and hardware VPN for the mobile teleworker and small-office or home-office (SOHO) worker. There is additional security at the switch-port level where devices connect to the switch; this type of security will be covered in detail in the LAN and WAN modules.

At the headquarters, there is another layer of security to protect the business information assets. These devices provide direct and indirect protection against potential threats. The first product in the headquarters security perimeter is the Cisco ASA 5500 Series Adaptive Security Appliance (ASA). The Cisco ASA 5500 is a hardened, multifunction device providing firewall capability, VPN, and Secure Sockets Layer (SSL) VPN access for remote/mobile users. The Cisco ASA 5500 also has a slot for a services module, and this design uses the IPS module.

Intrusion Detection System and IPS

The IPS module adds the ability to inspect application layer data for attacks and to block malicious traffic based on the content of the packet or the reputation of the sender.

The indirect security is established by the use of intrusion detection. This is a passive method for monitoring threats. Once a threat is detected, mitigation steps can be taken. The Cisco IPS 4200 Series allows the company to continuously monitor the network traffic for potential threats. When a threat is detected, the system sends an alert to the appropriate monitoring resource, and engineering or operational staff take action to resolve the issue.

Remote-Access VPN

VPNs are the foundation for remote access.

Remote mobile workers use hotspots in coffee shops, hotels, airports, and other locations to access the Internet. Once the mobile worker is connected to the Internet, they can use a software VPN client to gain secure access to company resources. Cisco offers SSL software VPN clients for this purpose.

Application Optimization Module

Remote sites must connect back to the main office to access applications. This connectivity affects the bottom line of a business; therefore, it is critical to maximize its usage for cost-effectiveness. Application optimization allows greater amounts of voice and data to traverse WAN links without incurring the cost of buying additional bandwidth. The ability to add application optimization with minimal cost and effort is an essential requirement. You will realize less operational impact, improved resilience, and lower costs when you implement an application optimization solution that integrates effectively with the WAN infrastructure.

The recommendation is Cisco Wide Area Application Services (WAAS) software. WAAS runs on a variety of devices that are selected based on the specific performance requirements of applications, WAN links, and number of users.

The WAAS solution has three components: an application optimization device at each remote site, an application optimization endpoint at the headquarters that acts as an aggregation point for the remote sites, and a Central Manager that is the control point for the entire WAAS solution. The SBA design uses the Cisco Services Ready Engine (SRE) in the router at the remote sites, the Cisco Wide Area Virtualization Engine (WAVE) appliances WAVE-594 or WAVE-694 for the application acceleration endpoint at the headquarters, and a Cisco WAVE-294 or a Virtual WAAS (vWAAS) appliance as the Central Manager at the headquarters.

WAN Module

The WAN aggregation is the point of connection between the headquarters and remote sites. The WAN interconnects all locations and aggregates traffic for the Internet at the headquarters. While the SBA foundation design includes Internet access, the Internet is not used for connectivity between locations. The WAN module offers guidance for two size ranges:

- WAN-25 accommodates headquarters WAN aggregation for around 25 remote sites.
- WAN-75 supports larger WANs with up to 75 sites aggregated at one location, and it may include regional sites that use the WAN-25 design for regional WAN aggregation.

The headquarters routers' ability to support additional services influenced device selection; beyond the primary function of routing traffic between locations, the device needs to support voice, media, and gateway services, application optimization, and security functions through the expansion capabilities provided by software features or add-on hardware modules.

Given all these requirements, the Cisco 3925 Integrated Services Router Generation 2 (ISR G2) is the recommended option for the WAN-25 headquarters router or regional aggregation sites; the Cisco 3945 ISR G2 is recommended for the WAN-75 design.

The Cisco 3945 and 3925 ISR G2s are flexible, modular platforms that enable high-speed routing and other services—such as voice—for connectivity needs between the headquarters and remote sites.

The remote sites are designed to support ~25 users with computers, IP phones, and wireless connectivity. User access to email and other applications, IP telephone, and Internet access are provided through the WAN. At remote sites, the LAN access switch delivers PoE for IP phones and wireless APs so individual power connections per device are not required.

In addition, QoS and application optimization offer cost savings and improved performance through efficient use of the WAN bandwidth.

The Cisco ISR G2 models 2911, 2921, and 2951 are the recommended platforms for connecting remote sites back to the headquarters. All three platforms provide integrated services with voice gateway capability for local connectivity to the public switched telephone network (PSTN), application optimization, and data, voice, and video service over the WAN.

For LAN access at the remote sites, the SBA design uses Cisco Catalyst 2960-S, Catalyst 3560-X, or Catalyst 3750-X. Each enables simple network access and PoE. In keeping with the principle of ease of use, each product applies the same basic configuration as the Cisco Catalyst 3750-X, 3560-X, and 2960-S switches that are used in the headquarters LAN, which keeps deployment and operational cost to a minimum.

For wireless connectivity at the remote site, the SBA design uses the Cisco 1140, 1260, and 3500 Series APs that are managed by the wireless controller at the headquarters.

Wireless Module

The foundation design includes both wired and wireless access to improve the effectiveness of the user by allowing them to stay connected regardless of location. The design uses 802.11 Wi-Fi technology for transporting voice, data, and even video. The 802.11a/b/g/n support in the wireless design provides easy migration from legacy Wi-Fi networks to the highest speed and performance infrastructure available.

Traditional wireless network designs used the autonomous or standalone access point (AP) model where each AP is individually configured and managed. This methodology made it difficult to monitor and expand the network size and functionality. At the heart of the SBA design for wireless is a centralized Wireless LAN Controller (WLC) appliance that can be scaled to support the number of APs and locations necessary to support the organization.

In the wireless design, Cisco recommends using the 5508 Series Wireless LAN Controller that provides support for up to 500 APs each. To keep the design simple yet resilient, secure, and scalable we use one pair of WLCs for guest traffic, data, and voice traffic for the organization users. The same APs that offer employee access to internal network access via authentication also offer guest and partner access. Each AP tunnels the wireless guest access data back to the WLC and, via a secured VLAN, the wireless guest data is handed to the firewall, which prevents those users from accessing

internal assets. You can add more WLCs to provide additional scalability and resiliency if needed.

The APs used in the wireless LAN (WLAN) are the Cisco 1140, 1260, and 3500 Series Lightweight APs with 802.11a/b/g/n support. Power is provided for AP operation using PoE from the LAN switches, which allows installation without the need for electrical outlets for every location. Both the headquarters and remote-site locations use the same Cisco AP models for a standard and efficient design. If a remote site loses connection to the headquarters WLC, the APs at that site will continue to operate in standalone mode and switch traffic locally.

Every location provides the same wireless Service Set Identifiers (SSID) for data, voice, and guest access, which simplifies mobility. Though the SSIDs are universal across the network, the design switches WLAN traffic for remote-site voice and data local to that site for efficient transport. The design uses RADIUS authentication to provide access to internal networks. The guest WLAN uses an OPEN web authentication, which allows expiring account-access controls.

Server Load Balancing Module

Application performance and availability directly affect employee productivity and the bottom line of an organization. As organizations do business on a global level, it becomes even more important to address application availability and performance issues to ensure achievement of business processes and objectives.

Server load balancers (SLBs) spread the load across servers to improve their response to client requests, improve application response and availability, and increase the productivity of organizations that rely on network-based applications to conduct business.

The Cisco Application Control Engine (ACE) is the latest SLB offering from Cisco for Layer 4 through Layer 7 switching, TCP processing offload, Secure Socket Layer (SSL) offload, compression, and various other acceleration technologies. We recommend the Cisco ACE 4710 appliance for use with the SBA design.

Notes

Global Configuration Module

Business Overview

The ability to standardize a setting or variable across a large number of instances reduces complexity and aids in comprehension. As networks become more complex, organizations are striving to simplify operations to reduce risk and lower cost. IT team members are required to wear many hats in smaller organizations; they may deal with the LAN infrastructure in the morning, the Internet Edge in the afternoon, and a WAN issue in the evening. The ability to use a common admin role to access network devices, and to gather statistics from a large number of devices with timestamps to aid with correlation of events, is crucial to reducing the challenge of deploying and monitoring a network.

The *Foundation Deployment Guide* Global Configuration module benefits your organization by providing a standardized approach to secure network device access, network protocol settings, and the baseline for network management application access. The end result is a network foundation that is easier to deploy and manage, which will help lower your operational costs.

Technical Overview

A small IT staff can find it daunting to manage a network of switches and routers for LAN and WAN, network appliances and modules that provide security and other network services, and network-based user services like IP telephony. The ability to standardize on common settings, features, and services reduces time to repair and makes it easier to train new staff about network operations.

This module provides recommendations for the settings for Cisco IOS routers and switches within the SBA for network designs up to 2500 users. To provide consistent and secure network device access, we recommend Secure Shell (SSH) Protocol for use across the network. For when you need browser-based access, we support both HTTP and HTTPS access. Adding host names to the network's DNS and using fully qualified IP domain names is helpful for accessing devices (as opposed to memorizing every device's IP address, which can change over time as well); some network devices *require* IP domain name services for operation. Finally, to reduce the ability for someone viewing a configuration printout to see confidential passwords, Cisco uses password-encryption services.

When you are troubleshooting an event or anomaly in a network, it is important to be able to correlate events across a large number of devices. We recommend Network Time Protocol (NTP) for the foundation of the network because it provides a consistent and synchronized timestamp for network event and debug logs. The ability to view the same point in time across network device logs can be helpful when troubleshooting a problem.

This module explains how to complete each of the procedures that make up the global configuration.

Tech Tip

The actual settings and values depend on your current network configuration. Please review all settings and configuration changes for a given module before submitting them so you are familiar with the intent and potential impact on your network.

Process

Applying Global Configuration

1. Set device host name
2. Create local login and password
3. Configure DNS for host lookup
4. Enable NTP and set local time zone
5. Enable management access
6. Enable SNMP for management

The following global system administration procedures will simplify and help secure the management of your network.

Reader Tip

Although many devices include a default configuration and an interactive setup dialog, all routers and switches in the SBA design are configured from a blank configuration, as reached by running the **write erase** command, followed by the **reload** command.

Procedure 1 Set device host name

Step 1: To make identification easier, set the device host name. This will typically match the name that the device has in DNS, without the domain name.

```
hostname [hostname]
```

Procedure 2 Create local login and password

The enable password secures access to the device configuration mode. By enabling password encryption, you prevent the use of plain text passwords within the configuration files.

When enabling password encryption, be sure to adhere to your corporate security standards.

Step 1: Set an enable password and password encryption.

```
enable secret [password]
service password-encryption
```

Step 2: Configure credentials with supervisor privilege for local login.

```
username [username] privilege 15 password [password]
```

Procedure 3 Configure DNS for host lookup

At the command line of a Cisco IOS device, it is helpful to be able to type a domain name instead of the IP address.

Step 1: Configure the name server command with the IP address of the DNS server for the network.

```
ip name-server 10.10.48.10
```

Procedure 4 Enable NTP and set local time zone

The Network Time Protocol (NTP) is designed to synchronize time across all devices in a network.

Synchronize network devices to a local NTP server in the network.

Step 1: Enable NTP.

```
ntp server 10.10.48.17
ntp update-calendar
```

Tech Tip

Some platforms may not offer the **ntp update-calendar** command. This command periodically updates the device's onboard hardware clock. If the command is not available, the step may be skipped without serious impact.

Step 2: Set the local time zone for the device location.

```
clock timezone PST -8
clock summer-time PDT recurring
```

Procedure 5 Enable management access

By enabling HTTPS access, you can provide for the use of the secure web-based GUI and management interface. Cisco recommends using Secure Shell (SSH) protocol for remote console management of network devices. SSH establishes a secure link that prevents sensitive data from being transferred across the network as human-readable cleartext.

Step 1: Configure an IP domain name. The domain name must be defined prior to configuring SSH.

```
ip domain-name [domain name]
```

Step 2: Enable HTTP(S) access and disable HTTP access. When you configure **ip http secure-server, you** automatically generate RSA keys that will also be used for SSH.

```
no ip http server
ip http secure-server
```

Tech Tip

Secure versions of terminal and web access methods exist and should be used when possible (for example, SSH to replace Telnet, and HTTPS to replace HTTP). If you only want to allow secured access to the switch web interface, issue the command "no ip http server".

Step 3: Set SSH to version 2, for improved security over version 1.

```
ip ssh version 2
```

Step 4: Secure authentication can use local accounts configured on the device or accounts on an authentication server in the network. Enable remote SSH login.

```
line vty 0 15
  login local
  transport input ssh
```

Step 5: (Optional) You can use an access list to limit the networks that can access the device. In this example, only devices on the 10.10.48.0/24 network will be able to access the device via SSH.

```
line vty 0 15
  access-class 55 in
access-list 55 permit 10.10.48.0 0.0.0.255
```

Tech Tip

All IP addresses, VLAN numbers, and other specific values used in this Deployment Guide are for example purposes only.

Procedure 6 Enable SNMP for management

Option 1. Basic Access

Step 1: Define a read-only and a read-write Simple Network Management Protocol (SNMP) community for network management. In this example, the read-only community is "cisco" and the read write community is "cisco123".

```
snmp-server community cisco RO
snmp-server community cisco123 RW
```

Option 2. More Secure Access

Step 1: Use an access list on the SNMP server to limit the networks that can access the device. In this example, only devices on the 10.10.48.0/24 network would be able to access the device via SSH.

```
snmp-server community cisco RO 55
snmp-server community cisco123 RW 55
access-list 55 permit 10.10.48.0 0.0.0.255
```

Tech Tip

Within this design there are a variety of devices, from switches and routers to various appliances and modules. Most of the products rely on a command-line interface (CLI) for initial boot and startup configuration. Once the product is up and running from the initial boot configuration, many products also provide a GUI. The extent to which you can configure each device from a GUI after the initial boot setup varies by product.

IP Subnet and VLAN Assignment

As you review configuration guidance, you may notice differences in the second octet. The second octet's address is assigned based on which design the configuration was developed in:

- 6 and 7 are part of the Midsize-500 design
- 8 and 9 are part of the Midsize-1000 design
- 10 and 11 are part of the Midsize-2500 design

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

Table 1 - Headquarters' VLANs

VLAN number	Purpose	IP subnet: Midsize-2500	IP subnet: Midsize-1000	IP subnet: Midsize-600
100	HQ Wired Data A	10.10.0.0/24	10.8.0.0/24	10.6.0.0/24
102	HQ Wired Voice A	10.10.2.0/24	10.8.2.0/24	10.6.2.0/24
104	HQ Wired Data B	10.10.4.0/24	10.8.4.0/24	10.6.4.0/24
106	HQ Wired Voice B	10.10.6.0/24	10.8.6.0/24	10.6.6.0/24
115	HQ Management	10.10.15.0/25	10.8.15.0/25	10.6.15.0/25
116	HQ Wireless Data	10.10.16.0/22	10.8.16.0/22	10.6.16.0/22
120	HQ Wireless Voice	10.10.20.0/22	10.8.20.0/22	10.6.20.0/22
127	Internet Edge	10.10.27.0/25	10.8.27.0/25	10.6.27.0/25
N/A	Remote-Access VPN	10.10.28.0/23	10.8.28.0/23	10.6.28.0/23
132	WAN Routing	10.10.32.0/24	10.8.32.0/24	10.6.32.0/24
148	Server Room	10.10.48.0/24	10.8.48.0/24	10.6.48.0/24
149	Server Room	10.10.49.0/24	10.8.49.0/24	10.6.49.0/24
150	Server Room; LAN and WAN Infrastructure	10.10.50.0/24	10.8.50.0/24	10.6.50.0/24
153	Secure Server Room Outside	10.10.53.0/24	10.8.53.0/24	10.6.53.0/24
154	Secure Server Room Inside	10.10.54.0/24	10.8.54.0/24	10.6.54.0/24
155	Secure Server Room Inside	10.10.55.0/24	10.8.55.0/24	10.6.55.0/24
N/A	Remote Sites	10.11.0.0/16	10.9.0.0/16	10.7.0.0/16

Internet DMZs and guest wireless LAN are allocated in a different address range, so that they are outside the summarized network that holds the internal LAN, reducing the likelihood that a firewall misconfiguration would inadvertently allow traffic that should be denied.

For the remote sites, the same VLAN numbers are applied at all of the sites, although IP subnet numbers are unique. This provides operational simplicity by offering template-based configuration for switch and router interface configuration. VLAN numbers are in the range between VLAN 64 and 70; remote sites are allocated eight total /24 IP subnets, to allow ample room for management, data, and voice subnets, and still offer plenty of room for application-specific subnets.

Reader Tip

For more details about IP subnet number assignment for remote sites, see the "Configuring the Remote-Site WAN Routers" process in the "Wide-Area Network Module" chapter.

Table 2 - Guest and DMZ VLANs

Purpose	Midsize-2500: IP subnet	Midsize-2500: VLAN	Midsize-1000: IP subnet	Midsize-1000: VLAN	Midsize-500: IP subnet	Midsize-500: VLAN
Internet DMZ	192.168.64.0/24	1164	192.168.48.0/24	1148	192.168.32.0/22	1132
Guest Wireless	192.168.76.0/22	1176	192.168.60.0/22	1160	192.168.44.0/22	1144

LAN Module

Business Overview

The LAN is the networking infrastructure that provides wired and wireless access to network communication services and resources for end users and devices spread over a single floor or building. In the age of connected users who access applications and information that help them perform their jobs, develop new ideas, and connect with their customers, the LAN is their access point.

The LAN module simplifies selecting products to build the network, describes enabling user connectivity, and creates a network that supports the connected user. Users' productivity relies on their ability to connect to the applications and information they need to do their job. Applications and information that are stored on the network require network resilience and ease of access, which are critical to the success of the organization.

The sections of the LAN module provide prescriptive guidance based on best practices for building out the core of the network that ties everything together, the client access that provides easy-yet-secure access, and the server farm where the applications and data reside. This prescriptive guidance reduces the time required for you to implement new networks and solutions by building a solid network foundation, and you can customize it to meet your organization's unique needs.

Technical Overview

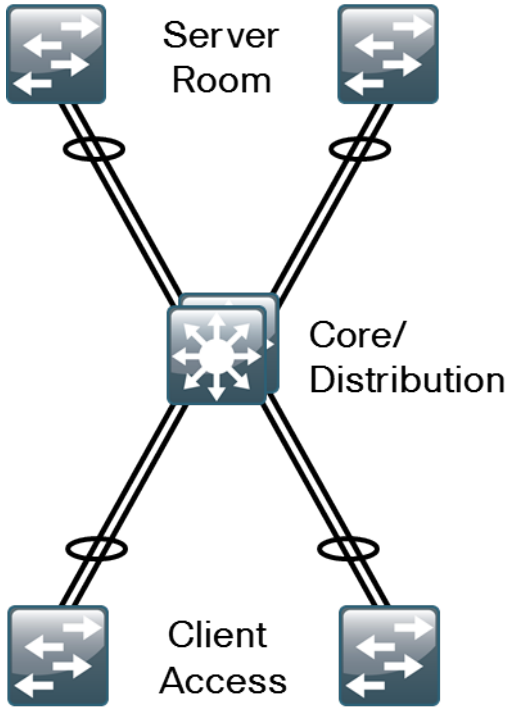
The LAN module provides a design that enables communications between devices in a building or group of buildings, as well as interconnection to the WAN and Internet modules.

Specifically, this module shows you how to deploy the network foundation and services to enable:

- LAN connectivity for up to 2500 connected users.
- LAN core design for backbone interconnect.
- Wired network access for employees.
- Server-room connectivity for application services.
- Wired infrastructure for voice, video, and wireless services.

This design uses a two-tier design model to break the design up into modular groups or layers. By breaking up the design into layers, each layer can focus on specific functions, which simplifies the design and provides easier deployment and management. In flat or meshed network architectures, changes tend to impact a large number of systems. Hierarchical design helps constrain operational changes to a subset of the network, which makes it easy to manage and improves resiliency.

Figure 2 - LAN hierarchical design



As shown in Figure 2, the design includes the following three layers:

- **Core layer**—Central aggregation for the headquarters' LAN
- **Client access layer**—Provides user/endpoint access
- **Server room layer**—Provides connectivity for local application servers

The three layers—core, access, and server room—each provide different functionality and capability to the network. Larger organizations may scale to an additional network tier by adding a distribution or aggregation layer. Based on the target size for the midsize design and the typical connectivity in a LAN this size, this design uses two tiers and the server room layer.

The remote-site LANs will use the same access layer features as the headquarters, which makes the design and the features available in all locations a standard offering.

LAN Core

Business Overview

In the Cisco SBA for Midsize Organizations—Borderless Networks design, the core of the headquarters or central-site LAN forms the hub for all communications from users to their applications or to the Internet, whether located at the headquarters, at a remote site, or connected on the remote-access VPN. Due to the importance to the overall IT operations for the organization, the LAN core design must be resilient to maintain the network's availability, and it must be scalable to grow with the organization.

The design and components used in the LAN core must provide a robust foundation for the flow of information in your organization. The design must be simple, to reduce cost and complexity without sacrificing resiliency or scalability and to minimize servicing and troubleshooting challenges.

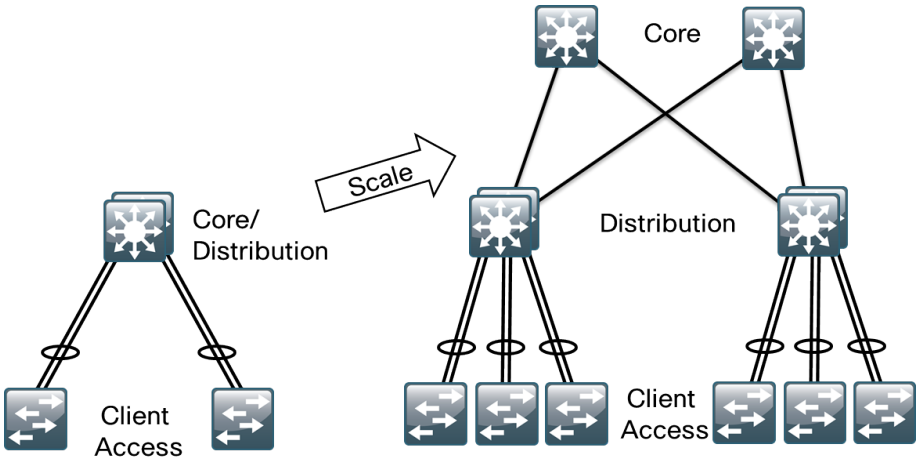
Technical Overview

The LAN core is the hub of communications between all modules in the network, which makes it one of the most important modules in the design. The SBA design provides three options:

- Deployments with up to 600 users are supported by a resilient core stack design using the Cisco Catalyst® 3750 switch.
- Deployments targeted at 1000 users are supported by a resilient Cisco Catalyst 4507R+E chassis equipped with dual supervisor modules.
- Deployments up to 2500 users are supported by a pair of Cisco Catalyst 6500 Series switches with VS-720 Supervisor blades, configured in a highly-available VSS 1440.

A hierarchical design allows the network to scale. The distribution/core layer provides aggregation and other services to the client access layer, such as Layer 3 IP routing and IP default gateway services. A dedicated core layer provides the Layer 3 connection backbone for a larger LAN where larger scale is required. As seen in Figure 3, the two-tier model can scale to three tiers by separating the core layer from the distribution layer to allow the design to grow with the organization's needs.

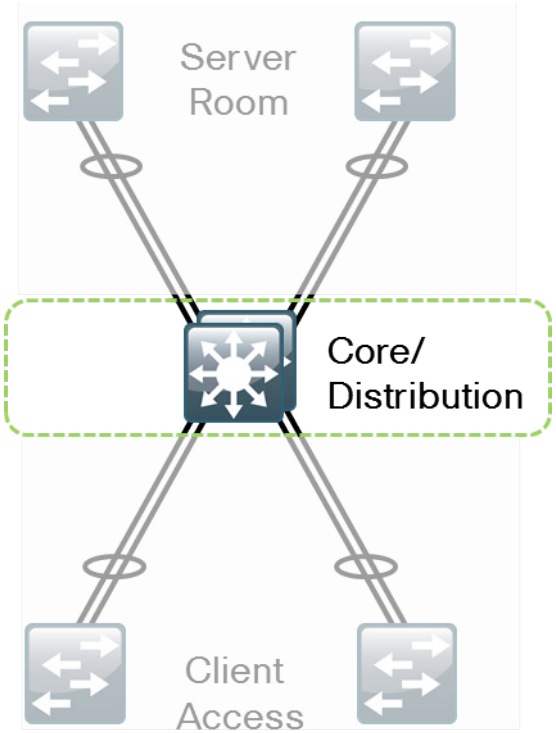
Figure 3 - Scalable LAN design



The SBA design diverges from traditional three-tier core/distribution/access LAN models to provide several benefits. As shown in Figure 4, the main changes with the resilient core design vs. a traditional design are in the core of the network:

- Instead of a pair of standalone core boxes, there is a resilient core providing combined distribution-layer and core-layer services.
- Physically, the core can be a stack of Cisco Catalyst 3750 switches, a highly available Cisco Catalyst 4507R switch, or a Cisco Catalyst 6500 VSS pair.
- Even though the core appears as a single device for configuration and to other devices in the network, it is a fully resilient design.
- The Cisco Catalyst 3750 stack offers independent processors for each switch in the Cisco StackWise stack, as well as resilient power for the stack.
- The Cisco Catalyst 4507R switch has dual supervisors, line cards, and power.
- The Cisco Catalyst 6500 VSS has dual chassis, supervisors, line cards, and power.

Figure 4 - LAN core

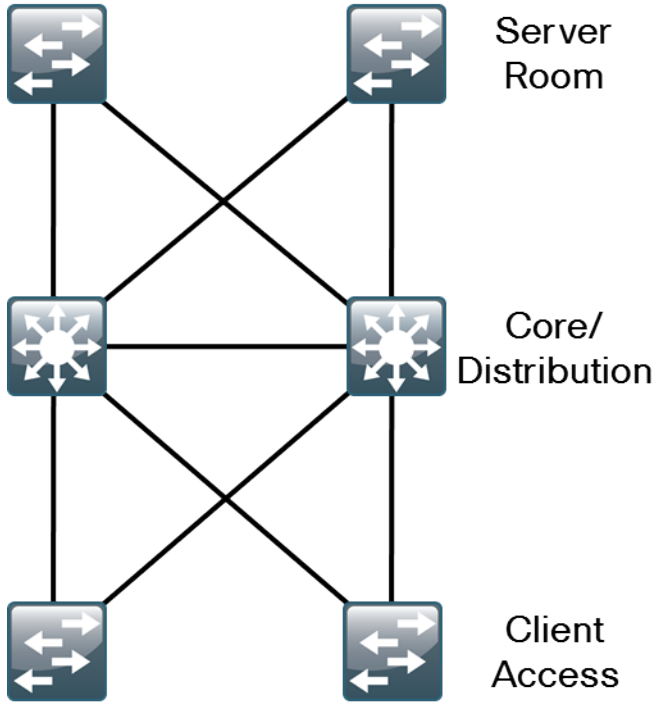


The SBA LAN design allows for easy growth without an outage by adding line cards to the Cisco Catalyst 4507R or 6500 switch or by adding switches to the Cisco Catalyst 3750 stack.

Traditional LAN Design vs. Resilient Core Design

The traditional dual core design shown in Figure 5 has an uplink from each access layer switch to each core switch.

Figure 5 - Traditional LAN design



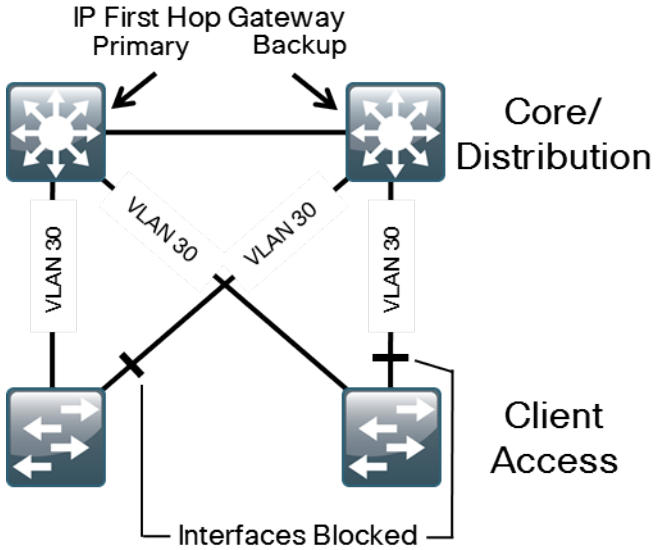
To avoid the longer Spanning Tree Protocol (STP) recovery times, it is possible to carry the VLAN from the access to the core and not trunk the VLAN between the two core switches, which creates a "V" design so there is no looped topology.

This design allows for faster failure recovery; however, it requires a separate VLAN be configured for each access switch and does not allow that VLAN to exist anywhere else on the LAN. In the past, this was an acceptable solution. Today's networks have voice and data VLANs for wired and wireless traffic. Add to that the VLANs needed for security and network management, and the number of VLANs and subnets that need to be configured can become large. Provisioning a large number of unique VLANs and IP subnets for each access switch makes management difficult, makes IP address planning hard, and complicates the design.

If a LAN design uses the same VLAN across multiple access switches, the network must rely on STP to block Layer 2 loops in the topology. STP has two main drawbacks:

- It has a slow recovery time when compared to other technologies.
- To prevent loops, it has to block one of the Gigabit Ethernet links from the access layer, which cuts the available bandwidth in half, as shown in Figure 6.

Figure 6 - Traditional Looped Design with HSRP and VLANs spanning access switches



IPv4 clients only support one default gateway per subnet. To make this single IP gateway address highly available, Cisco uses a First Hop Redundancy Protocol (FHRP) to make sure that the gateway IP address is on an active switch.

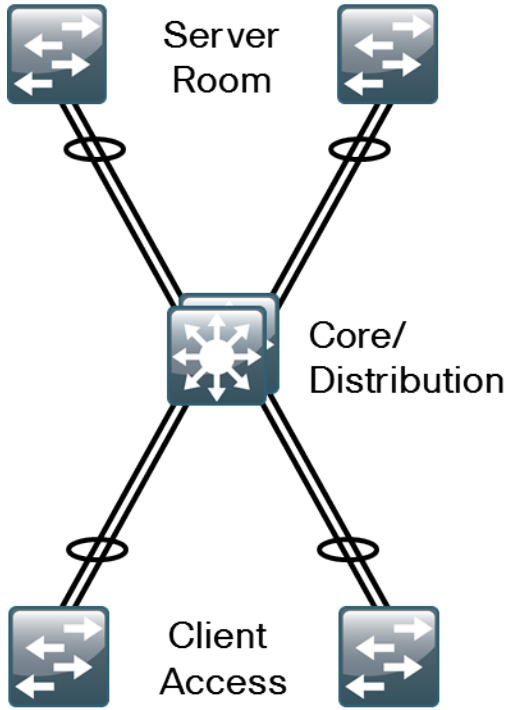
Hot Standby Router Protocol (HSRP), Gateway Load Balancing Protocol (GLBP), and Virtual Router Redundancy Protocol (VRRP) are all FHRPs that you can use to provide IP gateway redundancy.

- HSRP and VRRP are the most common FHRPs, but they only allow hosts on a subnet to talk to one switch at a time, so the redundant link to the core does not carry any traffic.
- GLBP is a newer protocol that allows for some load balancing by splitting the outbound traffic from the clients to multiple core switches. Return traffic, which is typically the majority of the data by volume, is harder to control and may not be load balanced, so the benefit from load balancing is small. Because the traffic is less deterministic, it can be more difficult to troubleshoot than simpler FHRPs.

The Benefits of Resilient Core

With the resilient core model, the link from the core to the access appears to be a single connection. The uplinks from the access to the core are members of a Gigabit EtherChannel link, and for greater resilience, the links are split between switches in the 6500 VSS pair, across multiple blades if the core is a Cisco Catalyst 4507R switch, or across switches if the core is a stack of Cisco Catalyst 3750 switches.

Figure 7 - SBA LAN design



There is no longer a looped topology, because the core only has a single logical link to each access switch, creating a hub-and-spoke topology. With a loop-free topology:

- No failures require STP to reconverge, so recovery times are faster.
- No uplinks are blocked.
- EtherChannel load balances both links from the access switch to the core, so inbound and outbound data is split across the links for a more effective use of the links.
- It is possible to increase the bandwidth to the access layer or server room by increasing the number of links in the EtherChannel to four or eight-gigabit links or by using 10-gigabit links where needed.
- The core has only a single logical interface for each VLAN from the access layer. This eliminates the need to run a FHRP without sacrificing any availability of the IP gateway to the client, and it reduces the complexity of the configuration.
- If the access layer closet is large and requires multiple switches, you can stack the switches and split an EtherChannel uplink across switches in the core stack to minimize the impact of a switch or link failure.
- The core design can scale from a LAN with a few hundred users up to 2500 users. For smaller LANs with fewer access layer switches, you can use the Cisco Catalyst 3750 stack. As the LAN grows, or for networks with up to 1000 users, you can use the Cisco Catalyst 4507R switch. And for midsize networks requiring the highest level of availability or scaling up to 2500 users, you can use the Cisco Catalyst 6500 VSS option.
- The server room switches can be stacked or separate and are connected to the core via EtherChannel uplinks, just like the access layer switches.
- For high availability and load balancing with NIC teaming (802.3ad port channeling), servers can be dual-homed into two standalone switches or connected to separate member switches in a stack.

Reader Tip

This section covers core-specific configuration only. For details about the global configuration, see the Global Configuration Module section in this guide.

Deployment Details

The single, logical, resilient, core design simplifies the switch configuration over traditional dual-core designs.

Process

Configuring the LAN Core

1. Apply platform-specific configuration
2. Set the LAN core global configuration
3. Configure VLAN Trunking Protocol
4. Configure spanning tree
5. Enable unidirectional link detection
6. Configure EtherChannel load-balancing
7. Configure in-band management
8. Configure IP routing
9. Configure VLAN-hopping mitigation
10. Configure LAN core IP Multicast

Procedure 1 Apply platform-specific configuration

The various core platforms require a one-time initial configuration prior to configuring the features and services of the switch. Execute the appropriate platform-specific configuration for the core switch that you have selected.

Option 1. Cisco Catalyst 6500 Virtual Switching System 1440

The Cisco Catalyst 6500 Virtual Switching System 1440 clusters two physical 6500 switches (with a single supervisor in each switch) together as a single logical switch. One of the supervisors acts as the active control plane for both chassis by controlling protocols such as Enhanced IGRP (EIGRP), STP, Cisco Discovery Protocol (CDP), and so forth, and both supervisors actively switch packets in each chassis.

Reader Tip

The following example shows you how to configure the VSS between the two new unconfigured chassis. For information about migrating your switches from an existing in-service dual-chassis role to a VSS system, go to http://www.cisco.com and search for "Migrate Standalone Cisco Catalyst 6500 Switch to Cisco Catalyst 6500 Virtual Switching System."

For an in-depth VSS configuration guide and configuration options, go to http://www.cisco.com and search for the Campus 3.0 Virtual Switching System Design Guide.

In the setup for the Cisco Catalyst 6500 Virtual Switching System 1440, connect two 10-Gigabit Ethernet links between the chassis to provide the Virtual Switch Link (VSL). Use at least two links; however, there are restrictions on which 10-Gigabit Ethernet interfaces can be used for the VSL. This design uses the two 10-Gigabit Ethernet interfaces on each supervisor; the interfaces must be cabled together before the VSS can be configured.

Step 1: Initiate conversion of standalone 6500s to VSS by configuring a host name on each switch.

On the Catalyst 6500 standalone switch #1:

```
Router#config t
Router#(config)#hostname VSS-Sw1
```

On the Catalyst 6500 standalone switch #2:

```
Router#config t
Router#(config)#hostname VSS-Sw2
```

Tech Tip

Each VSS switch pair must have a unique domain assigned that the pair shares. The domain number 100 is used in this example. Each switch is also given a unique number in the domain, switch 1 or switch 2.

Figure 8 - VSS Domain

VSL 10GbE EtherChannel Switch #2 Switch #1 Virtual Switch Domain 100
On the standalone switch #1:
VSS-Sw1(config)#switch virtual domain 100
VSS-Sw1(config-vs-domain)# switch 1
On the standalone switch #2:
VSS-Sw2(config)#switch virtual domain 100
VSS-Sw2(config-vs-domain)# switch 2

Step 2: Configure the VSL.

The VSL is a critical component of the VSS. Use unique port-channel numbers on each switch even though they connect to each other because both switches eventually become a single logical switch. This example uses port-channel number 101 on switch 1 and port-channel number 102 on switch 2. For the physical interfaces of the VSL EtherChannel, this example uses the 10 Gigabit Ethernet interfaces on the supervisor.

On standalone switch #1:

```
VSS-Sw1(config)#interface port-channel 101
VSS-Sw1(config-if)#switch virtual link 1
VSS-Sw1(config-if)#no shutdown
VSS-Sw1(config)#interface range tengigabit 5/4-5
VSS-Sw1(config-if)#channel-group 101 mode on
VSS-Sw1(config-if)#no shutdown
```

On standalone switch #2:

```
VSS-Sw2(config)#interface port-channel 102
VSS-Sw2(config-if)#switch virtual link 2
VSS-Sw2(config-if)#no shutdown
VSS-Sw2(config)#interface range tengigabit 5/4-5
VSS-Sw2(config-if)#channel-group 102 mode on
VSS-Sw2(config-if)#no shutdown
```

At this point you should be able to see that port-channel 101 and 102 are up and both links are active, but the switch is not in VSS mode yet.

```
VSS-Sw1# show etherchannel 101 port
VSS-Sw2# show etherchannel 102 port
Ports in the group:
-------------------
Port: Te5/4
------------
Port state = Up Mstr In-Bndl
Port: Te5/5
------------
Port state = Up Mstr In-Bndl
```

Step 3: Convert each switch to virtual mode operation. At the enable prompt (not in configuration mode) on each switch, run the following command.

```
VSS-Sw1# switch convert mode virtual
VSS-Sw2# switch convert mode virtual
```

Step 4: When asked if you want to proceed, answer yes.

Each switch now renumbers its interfaces from interface y/z (where *y* is the slot number and *z* is the interface number) to interface x/y/z (where *x* is the switch number, *y* is the module number in that switch, and *z* is the interface on that module). This numbering scheme allows the two chassis to be addressed and configured as a single system from a single supervisor, which is the supervisor with the active control plane.

Step 5: When you are prompted to save the configuration to bootflash, press Enter to accept the destination filename and location on each switch.

Both switches reload and become a VSS, and then one of the switches is resolved as the ACTIVE supervisor for the VSS cluster. All configuration commands now must be entered on the single active switch console; the standby switch console displays the Standby prompt.

Step 6: To check that the both switches see each other, they are in Stateful Switchover (SSO) mode, and the second supervisor is in standby hot status, enter the following command.

```
VSS-Sw1#show switch virtual redundancy
```

Step 7: To recognize that the two Catalyst 6500 switches are now operating as a single VSS system, rename the switch host name.

```
VSS-Sw1(config)#hostname 6500VSS
6500VSS(config)#
```

Step 8: To configure dual-active detection, use a Gigabit Ethernet interface on each VSS switch chassis, and cable them together (similar to a VSL link) in a back-to-back fashion.

A critical aspect of the Cisco Catalyst 6500 VSS 1440 is that a single supervisor is active for the control plane in both switches. Recall that each supervisor is active for its respective chassis, and it switches data packets from input interfaces to output interfaces, but a single supervisor is active for EIGRP, STP, and so on for the control plane. The VSL allows the supervisors to stay in synchronization.

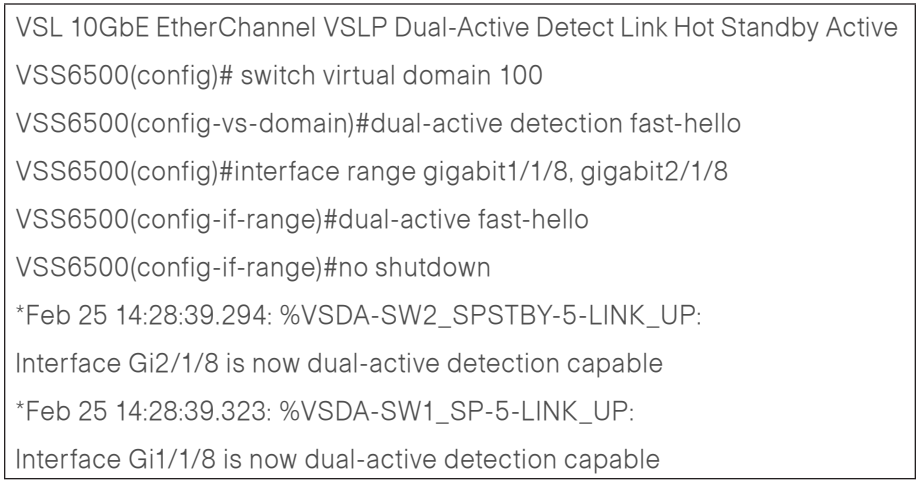
In the event that all VSLs are severed or both supervisors become active, the previously active supervisor shuts down all of its interfaces, and the standby supervisor becomes active.

There are three methods for detecting this dual-active condition:

- Ethernet Fast-Hello (VSLP) packet mode link
- Port Aggregation Protocol (PAgP) hellos between an adjacent switch to the VSS
- Bidirectional Forwarding Detection (BFD) configuration between supervisors

This design uses the Fast-Hello (VSLP) packet mode link for dual-active detection. This link does not require high bandwidth because it is only a detection link with control plane hellos on it.

Figure 9 - VSLP



Step 9: Set a virtual MAC address for the VSS system so that either active supervisor will use the same MAC address pool, regardless of which supervisor is active, even across a system reboot.

Tech Tip

By default, the VSS system uses the default chassis-based MAC-address pool assigned to the switch that is resolved to be the active switch when the switches initialize. Although the MAC addresses do not change when the active supervisor is switched to the standby, it is best to avoid gratuitous Address Resolution Protocol (ARP) updates to connected devices. If both switches are reloaded at the same time and the opposite supervisor comes up first and becomes the active supervisor, it would use the MAC address pool assigned to that switch.

```
6500-VSS(config)# switch virtual domain 100
6500-VSS(config-vs-domain)# mac-address use-virtual
Configured Router mac address is different from operational
value. Change will take effect after config is saved and
the entire Virtual Switching System (Active and Standby) is
reloaded.
```

Step 10: Save the running configuration, and then reload the entire system (both chassis).

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

When the switches initialize after this final reload, the VSS programming is complete.

Step 11: Enable QoS globally, and modify the global default class of service (CoS) to differentiated services code point (DSCP) mapping.

Tech Tip

On the Catalyst 6500 Series switches, QoS is enabled globally and primarily configured at the port level. When you enable QoS with the **mls qos** command, default queuing is enabled on all interfaces, and they are considered untrusted. All connections in the core are configured to trust DSCP.

Even though this design is configured to trust DSCP markings, it is a best practice to ensure proper mapping of CoS to DSCP for Voice over IP (VoIP). This mapping is accomplished by overriding the default mapping of CoS 5 "voice bearer traffic" to DSCP 40, with DSCP 46, which is the Expedited Forwarding per-hop behavior for voice.

```
mls qos
mls qos map cos-dscp 0 8 16 24 32 46 48 56
!
macro name EgressQoS
mls qos trust dscp
wrr-queue queue-limit 10 25 10 10 10 10 10
wrr-queue bandwidth 1 25 4 10 10 10 10
priority-queue queue-limit 15
wrr-queue random-detect 1
wrr-queue random-detect 2
wrr-queue random-detect 3
wrr-queue random-detect 4
wrr-queue random-detect 5
wrr-queue random-detect 6
wrr-queue random-detect 7
wrr-queue random-detect max-threshold 1 100 100 100 100
wrr-queue random-detect min-threshold 1 80 100 100 100
wrr-queue random-detect max-threshold 2 100 100 100 100
wrr-queue random-detect min-threshold 2 80 100 100 100
wrr-queue random-detect max-threshold 3 80 90 100 100
wrr-queue random-detect min-threshold 3 70 80 90 100
wrr-queue random-detect min-threshold 4 70 80 90 100
wrr-queue random-detect max-threshold 4 80 90 100 100
wrr-queue random-detect min-threshold 5 70 80 90 100
wrr-queue random-detect max-threshold 5 80 90 100 100
wrr-queue random-detect min-threshold 6 70 80 90 100
wrr-queue random-detect max-threshold 6 80 90 100 100
wrr-queue random-detect min-threshold 7 60 70 80 90
wrr-queue random-detect max-threshold 7 70 80 90 100
mls qos queue-mode mode-dscp
wrr-queue dscp-map 1 1 8
wrr-queue dscp-map 2 1 0
wrr-queue dscp-map 3 1 14
wrr-queue dscp-map 3 2 12
wrr-queue dscp-map 3 3 10
wrr-queue dscp-map 4 1 22
wrr-queue dscp-map 4 2 20
wrr-queue dscp-map 4 3 18
wrr-queue dscp-map 5 1 30
wrr-queue dscp-map 5 2 28
wrr-queue dscp-map 5 3 26
wrr-queue dscp-map 6 1 38
wrr-queue dscp-map 6 2 36
wrr-queue dscp-map 6 3 34
wrr-queue dscp-map 7 1 16
wrr-queue dscp-map 7 2 24
wrr-queue dscp-map 7 3 48
wrr-queue dscp-map 7 4 56
priority-queue dscp-map 1 32 40 46
@
macro name EgressQoS-Gig
mls qos trust dscp
wrr-queue queue-limit 20 25 40
priority-queue queue-limit 15
wrr-queue bandwidth 5 25 40
wrr-queue random-detect 1
```

```
wrr-queue random-detect 2
wrr-queue random-detect 3
wrr-queue random-detect max-threshold 1 100 100 100 100 100
100 100 100
wrr-queue random-detect min-threshold 1 80 100 100 100 100 100
100 100
wrr-queue random-detect max-threshold 2 100 100 100 100 100
100 100 100
wrr-queue random-detect min-threshold 2 80 100 100 100 100 100
100 100
wrr-queue random-detect max-threshold 3 70 80 90 100 100 100
100 100
wrr-queue random-detect min-threshold 3 60 70 80 90 100 100
100 100
wrr-queue cos-map 1 1 1
wrr-queue cos-map 2 1 0
wrr-queue cos-map 3 1 2
wrr-queue cos-map 3 2 3
wrr-queue cos-map 3 3 6
wrr-queue cos-map 3 4 7
priority-queue cos-map 1 4 5
@
```

Option 2. Cisco Catalyst 4507R+E Platform

Step 1: To make consistent deployment of QoS easier, define two macros for each platform that you will use in later procedures to apply the platform-specific QoS configuration.

```
class-map match-any VOIP_DATA_CLASS
match cos 5
class-map match-any VOIP_SIGNAL_CLASS
match cos 3
!
policy-map CISCOPHONE-POLICY
class VOIP_DATA_CLASS
set dscp ef
police 128k bc 8000
conform-action transmit
exceed-action drop
class VOIP_SIGNAL_CLASS
set dscp cs3
police 32k bc 8000
conform-action transmit
exceed-action drop
class class-default
set dscp default
police 10m bc 8000
conform-action transmit
exceed-action set-dscp-transmit cs1
!
class-map match-any PRIORITY-QUEUE
match dscp ef
match dscp cs5
match dscp cs4
class-map match-any CONTROL-MGMT-QUEUE
match dscp cs7
match dscp cs6
match dscp cs3
match dscp cs2
class-map match-any MULTIMEDIA-CONFERENCING-QUEUE
match dscp af41 af42 af43
class-map match-any MULTIMEDIA-STREAMING-QUEUE
match dscp af31 af32 af33
class-map match-any TRANSACTIONAL-DATA-QUEUE
match dscp af21 af22 af23
class-map match-any BULK-DATA-QUEUE
match dscp af11 af12 af13
class-map match-any SCAVENGER-QUEUE
match dscp cs1
policy-map 1P7Q1T
class PRIORITY-QUEUE
priority
class CONTROL-MGMT-QUEUE
bandwidth remaining percent 10
class MULTIMEDIA-CONFERENCING-QUEUE
```

```
bandwidth remaining percent 10
class MULTIMEDIA-STREAMING-QUEUE
bandwidth remaining percent 10
class TRANSACTIONAL-DATA-QUEUE
bandwidth remaining percent 10
dbl
class BULK-DATA-QUEUE
bandwidth remaining percent 4
dbl
class SCAVENGER-QUEUE
bandwidth remaining percent 1
class class-default
bandwidth remaining percent 25
dbl
!
macro name AccessEdgeQoS
qos trust device cisco-phone
service-policy input CISCOPHONE-POLICY
service-policy output 1P7Q1T
@
!
macro name EgressQoS
service-policy output 1P7Q1T
@
```

Step 2: When you configure a Catalyst 4507R+E with two Supervisor 7-Es, configure the switch to use Stateful Switchover (SSO) when moving the primary supervisor functionality between modules. To enable a fast transparent data plane failover, SSO synchronizes active process information as well as configuration information between supervisor modules.

```
redundancy
mode sso
```

Option 3. Cisco Catalyst 3750 Core Platform

When there are multiple switches configured in a stack, one of the switches controls the operation of the stack and is called the stack master. When three or more switches are configured as a stack, configure the stack master switch functionality on a switch that does not have uplinks configured.

Step 1: To set the stack master switch, run the following command.

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

Step 2: The default behavior when the stack master switch fails is for the newly active stack master switch to assign a new stack MAC address. This new MAC address assignment can cause the network to reconverge because Link Aggregation Control Protocol (LACP) and many other protocols rely on the stack MAC address and must restart. Use the **stack-mac persistent timer 0** command to ensure that the original master MAC address remains the stack MAC address after a failure.

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

Step 3: Since AutoQoS may not be configured on this device, manually configure the global QoS settings by entering the following commands.

```
mls qos map policed-dscp 0 10 18 to 8
mls qos map cos-dscp 0 8 16 24 32 46 48 56
mls qos srr-queue input bandwidth 70 30
mls qos srr-queue input threshold 1 80 90
mls qos srr-queue input priority-queue 2 bandwidth 30
mls qos srr-queue input cos-map queue 1 threshold 2 3
mls qos srr-queue input cos-map queue 1 threshold 3 6 7
mls qos srr-queue input cos-map queue 2 threshold 1 4
mls qos srr-queue input dscp-map queue 1 threshold 2 24
mls qos srr-queue input dscp-map queue 1 threshold 3 48 49 50
51 52 53 54 55
mls qos srr-queue input dscp-map queue 1 threshold 3 56 57 58
59 60 61 62 63
mls qos srr-queue input dscp-map queue 2 threshold 3 32 33 40
41 42 43 44 45
mls qos srr-queue input dscp-map queue 2 threshold 3 46 47
mls qos srr-queue output cos-map queue 1 threshold 3 4 5
mls qos srr-queue output cos-map queue 2 threshold 1 2
mls qos srr-queue output cos-map queue 2 threshold 2 3
```

```
mls qos srr-queue output cos-map queue 2 threshold 3 6 7
mls qos srr-queue output cos-map queue 3 threshold 3 0
mls qos srr-queue output cos-map queue 4 threshold 3 1
mls qos srr-queue output dscp-map queue 1 threshold 3 32 33 40
41 42 43 44 45
mls qos srr-queue output dscp-map queue 1 threshold 3 46 47
mls qos srr-queue output dscp-map queue 2 threshold 1 16 17 18
19 20 21 22 23
mls qos srr-queue output dscp-map queue 2 threshold 1 26 27 28
29 30 31 34 35
mls qos srr-queue output dscp-map queue 2 threshold 1 36 37 38
39
mls qos srr-queue output dscp-map queue 2 threshold 2 24
mls qos srr-queue output dscp-map queue 2 threshold 3 48 49 50
51 52 53 54 55
mls qos srr-queue output dscp-map queue 2 threshold 3 56 57 58
59 60 61 62 63
mls qos srr-queue output dscp-map queue 3 threshold 3 0 1 2 3
4 5 6 7
mls qos srr-queue output dscp-map queue 4 threshold 1 8 9 11
13 15
mls qos srr-queue output dscp-map queue 4 threshold 2 10 12 14
mls qos queue-set output 1 threshold 1 100 100 50 200
mls qos queue-set output 1 threshold 2 125 125 100 400
mls qos queue-set output 1 threshold 3 100 100 100 400
mls qos queue-set output 1 threshold 4 60 150 50 200
mls qos queue-set output 1 buffers 15 25 40 20
mls qos
!
macro name EgressQoS
mls qos trust dscp
queue-set 2
srr-queue bandwidth share 1 30 35 5
priority-queue out
@
```

Step 4: (Optional) Configure IOS DHCP server. If there is no external server for address assignment and you want to run an IOS DHCP server on the core switch, enter the following.

```
ip dhcp excluded-address 10.10.0.1 10.10.0.10
ip dhcp pool access
network 10.10.0.0 255.255.255.0
default-router 10.10.0.1
domain-name [cisco.local]
dns-server [DNS server IP]
```

Tech Tip

The example configuration prevents the IOS DHCP server from assigning addresses 1-10 for network 10.10.0.0/24.

Procedure 2 Set the LAN core global configuration

Step 1: To enable infrastructural requirements such as management access and network time configuration for the LAN Access switch, apply configuration described in the Global Configuration Module section earlier in this guide.

Procedure 3 Configure VLAN Trunking Protocol

VLAN Trunking Protocol (VTP) allows network managers to configure a VLAN in one location of the network and have that configuration dynamically propagate out to other network devices. However, in the SBA design, VLANs are defined once during switch setup with few, if any, additional modifications. The benefits of dynamic propagation of VLAN information across the network are not worth the potential for unexpected behavior due to operational error.

Step 1: Set the switch to ignore VTP autoconfiguration.

```
vtp mode transparent
```

Procedure 4 Configure spanning tree

Although this architecture is built without any Layer 2 loops, you must still enable spanning tree. By enabling spanning tree, you ensure that if any physical or logical loops are accidentally configured, no actual Layer 2 loops occur. Rapid per VLAN Spanning Tree Plus (Rapid PVST+) greatly improves the detection of indirect failures or linkup restoration events over classic spanning tree (802.1D)

Step 1: Enable Rapid PVST+, and set the core switch to be the spanning-tree root for the entire VLAN range.

```
spanning-tree mode rapid-pvst
spanning-tree vlan 4-4094 root primary
```

Procedure 5 Enable unidirectional link detection

Unidirectional Link Detection Protocol (UDLD) is a Layer 2 protocol that enables devices connected through fiber-optic or twisted-pair Ethernet cables to monitor the physical configuration of the cables and detect when a unidirectional link exists. When UDLD detects a unidirectional link, it disables the affected interface and alerts you.

Step 1: Enable UDLD.

```
udld enable
```

Procedure 6 Configure EtherChannel load-balancing

You should configure all LAN switches similarly to normalize the method in which traffic is load-shared across the member links of the EtherChannel.

Step 1: Configure the switch to use the traffic source and destination IP address when calculating which link to send the traffic across.

```
port-channel load-balance src-dst-ip
```

Procedure 7 Configure in-band management

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

Step 1: Configure the loopback interface with an address from the management IP address block that the core switch summarizes to the rest of the network. Use a 32-bit address (host) mask.

```
interface Loopback1
  ip address 10.10.15.254 255.255.255.255
```

Step 2: Configure management and infrastructure services to use the loopback interface as their source address.

```
snmp-server trap-source Loopback1
ip ssh source-interface Loopback1
ntp source Loopback1
```

Procedure 8 Configure IP routing

EIGRP is the IP routing protocol used in this design because it is easy to configure, does not require a large amount of planning, has flexible summarization and filtering, and can scale to large networks.

Step 1: Enable IP routing.

```
ip routing
```

Tech Tip

The Cisco Catalyst 6500 does not require the **ip routing** command; it is enabled by default on that platform.

Step 2: Enable EIGRP for the IP address space that the network will be using. If needed for your network, you can enter multiple network statements.

```
router eigrp 1
network 10.10.0.0 0.1.255.255
```

Step 3: Disable auto-summary of the IP networks, and configure all routed links to be passive by default.

```
no auto-summary
passive-interface default
```

Step 4: To ensure maximum resiliency, configure the switch to use the Loopback 1 IP address for the EIGRP router ID.

```
eigrp router-id 10.10.15.254
nsf
```

Tech Tip

Verify that **eigrp stub connected summary** is not configured in your EIGRP routing instance. This command may have been automatically configured due to platform licensing changes.

Procedure 9 Configure VLAN-hopping mitigation

There is a remote possibility that an attacker can create a double 802.1Q encapsulated packet. If the attacker has specific knowledge of the 802.1Q native VLAN, a packet could be crafted that when processed, the first or outermost tag is removed when the packet is switched onto the untagged native VLAN. When the packet reaches the target switch, the inner or second tag is then processed, and the potentially malicious packet is switched to the target VLAN.

At first glance, this appears to be a serious risk. However, the traffic in this attack scenario is in a single direction, and no return traffic can be switched by this mechanism. Additionally, this attack cannot work unless the attacker knows the native VLAN ID. An easy way to remove the remote risk of this type of attack is to configure an unused VLAN on all switch-to-switch 802.1Q trunk links from the access layer to the core.

Step 1: Define a hard-to-guess, unused VLAN for the native VLAN.

```
vlan 999
```

Tech Tip

VLAN-hopping mitigation must be applied on all switch downlinks.

Procedure 10 Configure LAN core IP Multicast

IP multicast allows a single IP data stream to be replicated by the infrastructure (routers and switches) and sent from a single source to multiple receivers. Using IP multicast is much more efficient than multiple individual unicast streams or a broadcast stream that would propagate everywhere. IP Telephony Music on Hold and IP Video Broadcast Streaming are two examples of IP Multicast applications.

In this design, you'll implement a basic sparse-mode multicast configuration that can be enhanced with additional configuration to support Anycast RP. Anycast RP is used to provide a simple-yet-scalable way to provide a highly resilient multi-site rendezvous point (RP) environment.

Step 1: Enable IP multicast routing

IP Multicast routing must be enabled to allow on the platforms in the global configuration mode.

```
ip multicast-routing
```

Tech Tip

The Cisco Catalyst 3750 Series switches instead require the **ip multicast-routing distributed** command.

Step 2: Configure a multicast rendezvous point.

The rendezvous-point address is assigned to a loopback interface, similar to the management interface.

```
interface loopback 2
  ip address 10.10.15.252 255.255.255.255
  ip pim sparse-mode
```

Step 3: Define multicast rendezvous point and multicast subnet.

Every Layer 3 switch and router must be configured with the address of the IP multicast RP. Use the **rp-address** command in conjunction with an access-list to limit the network size for which the RP is responsible. This configuration provides for future scaling and control of the IP multicast environment and can change based on network needs and design.

```
ip pim rp-address 10.10.15.252 10
access-list 10 permit 239.1.0.0 0.0.255.255
```

Step 4: Configure IP Multicast support on Layer 3 interfaces.

All Layer 3 interfaces in the network must be enabled for sparse-mode multicast operation.

```
ip pim sparse-mode
```

LAN Access

Business Overview

Organizations rely on the flow of information to conduct business in today's competitive global economy. The ability to access applications—to make informed business decisions, check email correspondence from internal and external associates, or relay business directives to a dispersed workforce—relies on the ability to move information around the organization.

User productivity relies on easy access to applications, resources, and information. Whether a user is located in the headquarters or working at a remote office, consistent methods of connecting to the network and consistent services, once connected, increase user productivity.

Communication is transforming from flat written text or voice conversations to a multimedia experience where audio, video, and text combine to improve the receivers' understanding and retention. As organizations evolve to deliver these richer modes of communications, they face the challenge of combining these various modes onto a single infrastructure that provides a scalable, cost-effective, and secure foundation for delivery.

Technical Overview

The access layer provides high-speed, user–controlled, and user-accessible device connectivity. Because the access layer is the connection point between the network and client devices, it plays a role in ensuring that the network is protected from human error and from malicious attacks. This protection includes ensuring that devices connecting to the network:

- Do not attempt to provide services to unauthorized end users.
- Do not attempt to take over the role of any other device on the network.
- Meet the organization's requirements before being allowed on the network.

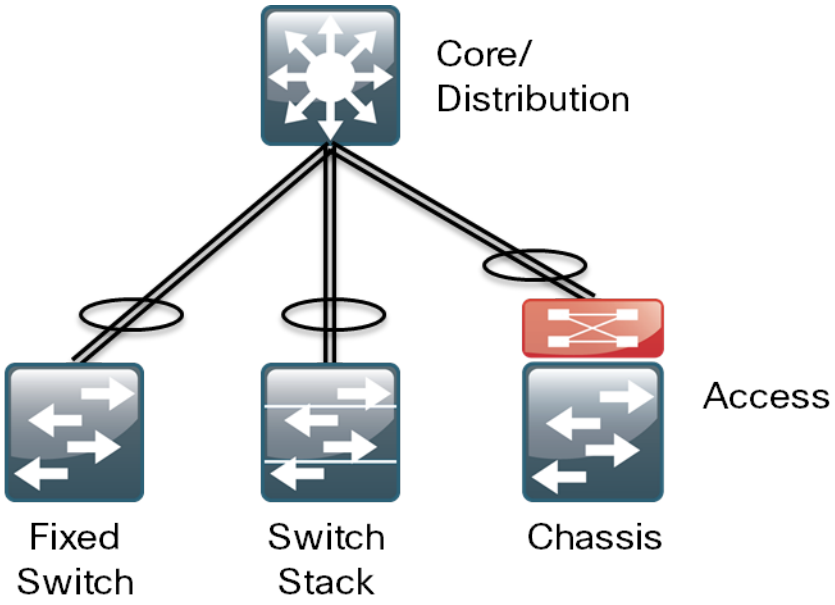
The access layer also provides a set of network services that support advanced technologies. Voice and video are commonplace in today's organizations, and the network must provide services that enable these technologies. The access layer provides Power over Ethernet Plus (PoE+) for IP phones and wireless access points, QoS for congestion control, and automated provisioning of VLANs to the connected IP phones.

In the SBA design, the access layer configuration is very simple. The same port configuration can be used for a standalone computer, an IP phone, an IP phone with an attached computer, or a wireless access point. To add

security for end hosts and the network at the access layer, several port-level features have been enabled, including the following:

- Port security limits the number of MAC addresses that can be active on a single port to protect against MAC flooding attacks.
- DHCP snooping prevents rogue DHCP servers from operating on the network and helps protect against DHCP-starvation attacks.
- Address Resolution Protocol (ARP) inspection ties an IP address to a MAC address and protects against ARP-spoofing attacks.
- IP source guard prevents attacks that use spoofed source IP addresses.

Figure 10 - Access layer options



Cisco SBA for Midsize Organizations—Borderless Networks accommodates LAN access-switching requirements with four product lines that include 10/100/1000 access ports, Gigabit Ethernet and 10-Gigabit Ethernet uplinks, and PoE+:

- The Cisco Catalyst 2960-S series is an economical fixed-configuration switch with stacking capability and multiple uplink options. Catalyst 2960-S switches are offered to address access-switch requirements for price-sensitive networks. The Catalyst 2960-S family offers high performance, as expected from the Catalyst LAN switch family, although the 2960-S provides a subset of the features found on other Cisco Catalyst switches. For example, advanced capabilities in Medianet, EnergyWise, and TrustSec features are limited or unavailable on the Catalyst 2960-S switch family.
- The Cisco Catalyst 3560-X series is a fixed-configuration, non-stackable switch with modular uplinks that provides flexibility and features for many access-level switching environments with lower port-density requirements.
- The Cisco Catalyst 3750-X series is a fixed-port stackable switch with modular uplinks capable of growing as port density requirements increase. Catalyst 3750-X stackable switches offer resilience by the various stack members maintaining the stack's function, even if a stack member is render unavailable due to a failure. The stack members share each other's power supplies with StackPower interconnections, so if a stack member's power cord is unplugged, or if a power supply fails, all stack members will maintain their availability.
- The Cisco Catalyst 4500 E-series offers a flexible, chassis-based modular switch, with a wide range of line-card configuration options for larger, higher density and deployments requiring the highest levels of availability at that access layer. Cisco Catalyst 4500 E-Series chassis offer many options for port flexibility and deployment resilience. Resilient supervisors provide optimal availability. Cisco IOS SSO provides lossless fallback to the resilient supervisor if the primary supervisor becomes unavailable. If resilience is not required, resilient supervisors and power supplies can be omitted, reducing cost while offering an upgrade path.

This section explains how to implement each of the procedures necessary to complete the access layer configuration of your network.

Process

Configuring the Access Layer

1. Apply platform-specific configuration
2. Apply global configuration
3. Configure core downlink to access switch
4. Configure link from access switch to core
5. Configure access switch access ports

Procedure 1 Apply platform-specific configuration

Some platforms require a one-time initial configuration prior to configuring the features and services of the switch. If you do not have a platform listed in the following steps, you can skip those steps.

Option 1. Catalyst 2960-S and 3750-X platform configuration

When there are multiple Catalyst 2960-S or 3750-X Series switches configured in a stack, one of the switches controls the operation of the stack and is called the stack master.

When three or more switches are configured in a stack, configure a switch that does not have uplinks configured as the stack master.

Step 1: To set the stack master, run the following command.

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

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

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

Step 3: To make consistent deployment of QoS easier, define two macros for each platform that you will use in later procedures to apply the platform specific QoS configuration.

```
macro name AccessEdgeQoS
auto qos voip cisco-phone
@
!
macro name EgressQoS
mls qos trust dscp
queue-set 2
srr-queue bandwidth share 1 30 35 5
priority-queue out
@
```

Option 2. Catalyst 4507R+E platform configuration

Step 1: To make consistent deployment of QoS easier, define two macros for each platform that you will use in later procedures to apply the platform specific QoS configuration.

```
class-map match-any VOIP_DATA_CLASS
match cos 5
class-map match-any VOIP_SIGNAL_CLASS
match cos 3
!
policy-map CISCOPHONE-POLICY
class VOIP_DATA_CLASS
set dscp ef
police 128k bc 8000
conform-action transmit
exceed-action drop
```

```
class VOIP_SIGNAL_CLASS
set dscp cs3
police 32k bc 8000
conform-action transmit
exceed-action drop
class class-default
set dscp default
police 10m bc 8000
conform-action transmit
exceed-action set-dscp-transmit cs1
!
class-map match-any PRIORITY-QUEUE
match dscp ef
match dscp cs5
match dscp cs4
class-map match-any CONTROL-MGMT-QUEUE
match dscp cs7
match dscp cs6
match dscp cs3
match dscp cs2
class-map match-any MULTIMEDIA-CONFERENCING-QUEUE
match dscp af41 af42 af43
class-map match-any MULTIMEDIA-STREAMING-QUEUE
match dscp af31 af32 af33
class-map match-any TRANSACTIONAL-DATA-QUEUE
match dscp af21 af22 af23
class-map match-any BULK-DATA-QUEUE
match dscp af11 af12 af13
class-map match-any SCAVENGER-QUEUE
match dscp cs1
policy-map 1P7Q1T
class PRIORITY-QUEUE
priority
class CONTROL-MGMT-QUEUE
bandwidth remaining percent 10
class MULTIMEDIA-CONFERENCING-QUEUE
bandwidth remaining percent 10
class MULTIMEDIA-STREAMING-QUEUE
bandwidth remaining percent 10
class TRANSACTIONAL-DATA-QUEUE
bandwidth remaining percent 10
dbl
class BULK-DATA-QUEUE
bandwidth remaining percent 4
dbl
class SCAVENGER-QUEUE
bandwidth remaining percent 1
class class-default
bandwidth remaining percent 25
dbl
!
macro name AccessEdgeQoS
qos trust device cisco-phone
service-policy input CISCOPHONE-POLICY
service-policy output 1P7Q1T
@
!
macro name EgressQoS
service-policy output 1P7Q1T
@
```

Step 2: If a Catalyst 4507R+E is configured with two Cisco Catalyst 4500 Supervisor Engine 6L-Es for access switches that require the highest level of availability, configure the switch to use SSO when two supervisors must determine and synchronize the primary role. To enable a fast transparent data plane failover, SSO synchronizes active process information as well as configuration information between supervisor modules.

```
redundancy
  mode sso
```

Procedure 2 Apply global configuration

The LAN Access switch requires basic global configuration.

Step 1: To enable infrastructure requirements, such as management access and network time configuration, apply the configuration described in the Global Configuration Module section earlier in this guide.

Step 2: Configure VLAN Trunking Protocol (VTP).

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

The benefits of dynamic propagation of VLAN information across the network are not worth the potential for unexpected behavior due to operational error. For this reason, VTP transparent mode is configured in this architecture. Set the switch to ignore VTP auto-configuration.

```
vtp mode transparent
```

Step 3: Configure spanning tree.

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

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

```
spanning-tree mode rapid-pvst
```

Step 4: Enable unidirectional link detection (UDLD).

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

```
udld enable
```

Step 5: Configure EtherChannel load balancing for access-switch uplinks similarly to the configuration applied on core switches.

```
port-channel load-balance src-dst-ip
```

Step 6: Configure Virtual LANs on the switch.

The access-layer devices use Virtual LANs (VLANs) to separate traffic from different devices into three logical networks:

- The data VLAN provides access to the network for all attached devices other than IP phones. This VLAN is configured on all user-facing interfaces.
- The voice VLAN provides access to the network for IP phones. This VLAN is configured on all user-facing interfaces.
- The management VLAN provides in-band access to the network for the switches' management interfaces. The management VLAN is not configured on any user-facing interface, and the VLAN interface of the switch is the only member.

Configure the data and voice VLANs on the switch.

```
vlan [data vlan],[voice vlan],[management vlan]
```

Step 7: Configure in-band management.

Configure the switch with an IP address so that it can be managed via in-band connectivity, and define a default route for the management LAN.

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

Tech Tip

Do not use the **ip default-gateway** command on the Catalyst 4500 because it has IP routing enabled by default, and this command will not have any effect. Instead use the following command on the Catalyst 4500.

```
ip route 0.0.0.0 0.0.0.0 [default router]
```

Step 8: Configure DHCP snooping.

DHCP snooping is a DHCP security feature that blocks DHCP replies on an untrusted interface. An untrusted interface is any interface on the switch not specifically configured as a known DHCP server or path towards a known DHCP server.

When you enable DHCP snooping on a VLAN, the switch intercepts and safeguards DHCP messages within the VLAN. This ensures that an unauthorized DHCP server cannot serve out addresses to end-devices.

The DHCP snooping feature tracks MAC address, IP address, lease time, binding type, VLAN number, and interface information that correspond to the local untrusted interfaces on the switch. DHCP snooping stores that information in the DHCP binding table.

To configure DHCP snooping, enter the following global switch commands.

```
ip dhcp snooping vlan [data vlan], [voice vlan]
no ip dhcp snooping information option
ip dhcp snooping
```

Step 9: Configure Dynamic ARP Inspection (DAI).

DAI mitigates ARP poisoning, preventing some kinds of man-in-the-middle attacks.

DAI uses the data generated by the DHCP snooping feature and intercepts and validates the IP-to-MAC address relationship of all ARP packets on untrusted interfaces. ARP packets that are received on trusted interfaces are not validated, and invalid packets on untrusted interfaces are discarded.

To configure ARP inspection, enter the following global switch commands.

```
ip arp inspection vlan [data vlan], [voice vlan]
```

Procedure 3 Configure core downlink to access switch

The links to access layer switches and server-room switches are Layer 2 EtherChannels. Connect the access layer EtherChannel uplinks to separate switches in the core layer switches or stack, and in the case of the Cisco Catalyst 4507R+E core layer, connect the uplinks to separate redundant modules for additional resiliency.

Step 1: Add the VLANs that the downlink will carry to the core switch's VLAN database.

```
vlan [data vlan],[voice vlan]
```

Step 2: Configure two or more physical interfaces to be members of the EtherChannel. LACP ensures that a proper EtherChannel is formed.

```
interface range [interface type] [port 1], [interface type] [port 2]
  switchport
  macro apply EgressQoS
  channel-protocol lacp
  channel-group [number] mode active
```

Step 3: Configure an 802.1Q trunk for the connection to the access layer. Prune the VLANs allowed on the trunk to only those VLANs that are active on the access switch. The port-channel number must match channel-group configured in Step 2.

```
interface Port-Channel[number]
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan [data vlan],[voice vlan],[mgmt vlan]
  switchport mode trunk
  no shutdown
```

Tech Tip

The Catalyst 4500 does not require the **switchport trunk encapsulation dot1q** command.

Step 4: If the VLANs on the downlink did not already exist on the core switch, add a switched virtual interface (SVI) for every access layer VLAN the VLANs can route to the rest of the network.

If you did not provision IOS DHCP scopes on your core switch, use the **ip helper-address** command to allow remote DHCP servers to provide IP addresses for this network. The helper command points to the DHCP server address; if you have more than one DHCP server, you can list multiple helper commands on an interface.

```
interface vlan [number]
  ip address [ip address] [mask]
  ip helper-address [dhcp server ip]
  ip pim sparse-mode
  no shutdown
```

Step 5: Add VLAN-hopping mitigation for the trunk.

```
interface Port-channel [number]
 switchport trunk native vlan 999
```

Procedure 4 Configure link from access switch to core

The physical interfaces that are members of a Layer 2 EtherChannel are configured prior to configuring the logical port-channel interface. This allows for minimal configuration because most of the commands entered to a port-channel interface are copied to its members' interfaces and do not require manual replication. This procedure details how to connect an access layer device to the LAN core.

Step 1: Configure interfaces as members of EtherChannel.

Configure two or more physical interfaces to be members of the EtherChannel. LACP ensures that a proper EtherChannel is formed.

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

Tech Tip

The Catalyst 2960-S does not require the **switchport** command.

Step 2: To allow the upstream device to provide Layer 3 services to all the VLANs defined on the access layer switch, configure the 802.1 Q trunk.

The VLANs allowed on the trunk are pruned to only the VLANs that are active on the access switch. DHCP snooping and DAI are set to trust. When using EtherChannel, the interface type will be port-channel, and the number must match the channel-group configured in .

```
interface Port-channel1
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan [data vlan],[voice vlan],[mgmt
vlan]
 switchport mode trunk
 ip arp inspection trust
 ip dhcp snooping trust
 logging event link-status
 macro apply EgressQoS
 no shutdown
```

Tech Tip

The Catalyst 2960-S and 4500 do not require the **switchport trunk encapsulation dot1q** command.

Step 3: Add VLAN-hopping mitigation for the uplink trunk.

```
vlan 999
interface Port-channel1
 switchport trunk native vlan 999
```

Procedure 5 Configure access switch access ports

To make configuration easier when the same configuration will be applied to multiple interfaces on the switch, use the **interface range** command. This command allows you to run a command once and have it apply to many interfaces at the same time. Since most of the interfaces in the access layer are configured identically, it can save a lot of time. For example, the following command allows you to enter commands on all 24 interfaces (Gig 0/1 to Gig 0/24) simultaneously.

```
interface range Gigabitethernet 0/1-24
```

Step 1: Configure switch interfaces to support clients and IP phones.

The host interface configurations support PCs, phones, or wireless access points. Inline power is available on switches that support 802.3AF/AT for capable devices.

```
interface range [interface type] [port number]-[port number]
switchport access vlan [data vlan]
switchport mode access
switchport voice vlan [voice vlan]
```

Step 2: Because only end-device connectivity is provided at the access layer, shorten the time it takes for the interface to go into a forwarding state by enabling portfast, disabling 802.1q trunking, and disabling channel grouping.

```
switchport host
```

Step 3: To enable QoS, run the following command.

```
macro apply AccessEdgeQoS
```

Step 4: Configure port security on the interface.

The number of MAC addresses required on an interface can vary. This design uses a number that allows flexibility in the organization while still protecting the network infrastructure.

Configure 11 MAC addresses to be active on the interface at one time; additional MAC addresses are considered to be in violation, and their traffic will be dropped.

```
switchport port-security maximum 11
switchport port-security
```

Step 5: Set an aging time that will remove learned MAC addresses from the secured list after 2 minutes of inactivity.

```
switchport port-security aging time 2
switchport port-security aging type inactivity
```

Step 6: Configure the restrict option to drop traffic from MAC addresses that are in violation but not shut down the port. This configuration ensures that an IP phone can still function on this interface when there is a port security violation.

```
switchport port-security violation restrict
```

Step 7: Configure DHCP Snooping and ARP Inspection on the Interface

Allow ARP inspection and DHCP snooping to process 100 packets per second of traffic on the port.

```
ip arp inspection limit rate 100
ip dhcp snooping limit rate 100
```

Step 8: Configure IP Source Guard on the interface.

IP Source Guard prevents packets from spoofing its source IP address to obscure its true source. IP Source Guard uses information from DHCP snooping to dynamically configure a port access control list (PACL) on the interface that denies any traffic from IP addresses that are not in the DHCP binding table.

```
ip verify source
```

Tech Tip

The Catalyst 4500 does not support the **ip verify source** command. Instead use the following command:

```
ip verify source vlan dhcp-snooping
```

Step 9: Configure bridge protocol data unit (BPDU) guard on the interface.

BPDU guard protects against a user plugging a switch into an access port, which could cause a catastrophic undetected spanning-tree loop.

If a portfast-configured interface receives a BPDU, an invalid configuration exists, such as the connection of an unauthorized device. The BPDU guard feature prevents loops by moving a nontrunking interface into an errdisable state when a BPDU is received on an interface when portfast is enabled.

To disable the interface if another switch is plugged into the port, run the following command.

```
spanning-tree bpduguard enable
```

Step 10: (Optional): Configure QoS for trusted access devices.

In some cases, you may want to trust the QoS markings from an access port device like a video endpoint or wireless access point. To trust QoS from a device on an interface, enter the following commands.

```
no auto qos voip
auto qos trust dscp
```

Server Room

Business Overview

Young organizations and businesses often begin their IT practices with application servers sitting under desks or in closets with switches—and perhaps some storage tapes for ad hoc backups stacked on top. As the organization grows and their reliance on data grows with it, the need to provide a more stable environment for their critical applications forces change. Whether it is the fear of an outage delaying productivity, data loss that could harm the perception of an organization, or regulatory compliance, the IT person or group is forced to build a more suitable environment.

The server room represents the first move into a serious IT environment onsite with the business. An example environment will have controlled cooling and power, two to three equipment racks for application servers, the supporting network connectivity, and a small backup system. Cisco SBA recognizes the importance of the server room facility and its importance in the overall organization function. The design provides a small yet resilient and scalable Ethernet LAN foundation to connect the application servers to the users located throughout the rest of the organization's network. As organizations scale beyond the server room to data centers with many application servers and larger storage environments, the *Cisco SBA for Midsize Organizations—Data Center Deployment Guide* provides a methodology for a smooth transition. Organizations that have deployed a centralized data center may still have a need to host servers at smaller regional sites. The SBA server room design can fill this requirement as well.

Technical Overview

In the SBA, the server room provides basic compute and storage capability for business operations and is designed to accommodate up to 24 physical servers. The design uses the Cisco Catalyst 3560-X and Cisco Catalyst 3750-X Series stackable Ethernet LAN switches, with 10/100/1000 support to accommodate a wide range of server Ethernet interface speeds.

The Cisco StackWise Plus feature of the Catalyst 3750-X series provides a resilient, high-speed backplane for the server room environment and the ability to dual-home servers to the server room LAN for increased resiliency. With two or more switches in the stack, and dual homing to servers and the LAN core switches, your server room is protected from single points of failure. The Catalyst 3750-X switches in a stack provide automated control plane failover in the event that the master switch experiences an issue. The option of dual power supplies and Cisco StackPower with the Catalyst 3750-X Series switches provides more resilience to the server room design. The Catalyst 3560-X does not provide the same level of resilience as the 3750-X, but is suitable for single connected servers and less critical systems.

In the SBA design, the server farm switches are connected to the core with an EtherChannel so that two Gigabit Ethernet ports combine to make a single 2-Gigabit channel. It is possible to increase the number of links to the core from the server farm to four or eight for more bandwidth if needed, or if very high bandwidth is required, 10 Gigabit Ethernet links can be used to connect the appropriate core switch ports to 10-Gigabit ports on uplink modules installed in the server room switches.

Reader Tip

The *Cisco SBA for Midsize Organizations—Data Center Design Overview* and *the Cisco SBA for Midsize Organizations—Data Center Deployment Guide* can guide you through the migration from the server room in the SBA foundation design to a more advanced business operations and applications environment.

Deployment Details

This section includes the procedures you need to perform to configure your server room.

Process

Configuring the Server Room LAN

1. Configure Catalyst 3750-X platform
2. Configure global QoS settings
3. Configure device resiliency features
4. Configure spanning tree
5. Enable UDLD
6. Configure EtherChannel load-balancing
7. Configure VLANs on the switch
8. Configure in-band management
9. Configure core downlink to access switch
10. Configure VLAN-hopping mitigation
11. Configure server room uplink ports
12. Configure server access ports

Procedure 1 is required only for Cisco Catalyst 3750-X switches. If you will use a Cisco Catalyst 3560-X for your server room switch, you can skip to Procedure 2.

Procedure 1 Configure Catalyst 3750-X platform

When there are multiple switches configured in a stack, one of the switches controls the operation of the stack and is called the stack master. When three or more switches are configured as a stack, configure the stack master switch functionality on a switch that does not have uplinks configured.

By default, when the stack master switch fails, the newly active stack master switch assigns a new stack MAC address. This new MAC address assignment can cause the network to have to reconverge because LACP and many other protocols rely on the stack MAC address and must restart. As such, you use the **stack-mac persistent timer 0** command to ensure that the original master MAC address remains the stack MAC address after a failure.

Step 1: Apply the configuration described in the Global Configuration Module section earlier in this guide.

Step 2: To set the stack master switch, enter the following command.

```
switch [switch number] priority 15
stack-mac persistent timer 0
```

Procedure 2 Configure global QoS settings

Step 1: Since AutoQoS may not be configured on this device, manually configure the global QoS settings by entering the following commands.

```
mls qos map policed-dscp 0 10 18 to 8
mls qos map cos-dscp 0 8 16 24 32 46 48 56
mls qos srr-queue input bandwidth 70 30
mls qos srr-queue input threshold 1 80 90
mls qos srr-queue input priority-queue 2 bandwidth 30
mls qos srr-queue input cos-map queue 1 threshold 2 3
mls qos srr-queue input cos-map queue 1 threshold 3 6 7
mls qos srr-queue input cos-map queue 2 threshold 1 4
mls qos srr-queue input dscp-map queue 1 threshold 2 24
mls qos srr-queue input dscp-map queue 1 threshold 3 48 49 50
51 52 53 54 55
mls qos srr-queue input dscp-map queue 1 threshold 3 56 57 58
59 60 61 62 63
mls qos srr-queue input dscp-map queue 2 threshold 3 32 33 40
```

```
41 42 43 44 45
mls qos srr-queue input dscp-map queue 2 threshold 3 46 47
mls qos srr-queue output cos-map queue 1 threshold 3 4 5
mls qos srr-queue output cos-map queue 2 threshold 1 2
mls qos srr-queue output cos-map queue 2 threshold 2 3
mls qos srr-queue output cos-map queue 2 threshold 3 6 7
mls qos srr-queue output cos-map queue 3 threshold 3 0
mls qos srr-queue output cos-map queue 4 threshold 3 1
mls qos srr-queue output dscp-map queue 1 threshold 3 32 33 40
41 42 43 44 45
mls qos srr-queue output dscp-map queue 1 threshold 3 46 47
mls qos srr-queue output dscp-map queue 2 threshold 1 16 17 18
19 20 21 22 23
mls qos srr-queue output dscp-map queue 2 threshold 1 26 27 28
29 30 31 34 35
mls qos srr-queue output dscp-map queue 2 threshold 1 36 37 38
39
mls qos srr-queue output dscp-map queue 2 threshold 2 24
mls qos srr-queue output dscp-map queue 2 threshold 3 48 49 50
51 52 53 54 55
mls qos srr-queue output dscp-map queue 2 threshold 3 56 57 58
59 60 61 62 63
mls qos srr-queue output dscp-map queue 3 threshold 3 0 1 2 3
4 5 6 7
mls qos srr-queue output dscp-map queue 4 threshold 1 8 9 11
13 15
mls qos srr-queue output dscp-map queue 4 threshold 2 10 12 14
mls qos queue-set output 1 threshold 1 100 100 50 200
mls qos queue-set output 1 threshold 2 125 125 100 400
mls qos queue-set output 1 threshold 3 100 100 100 400
mls qos queue-set output 1 threshold 4 60 150 50 200
mls qos queue-set output 1 buffers 15 25 40 20
mls qos
!
macro name EgressQoS
mls qos trust dscp
queue-set 2
srr-queue bandwidth share 1 30 35 5
priority-queue out
@
```

Procedure 3 Configure device resiliency features

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

The benefits of dynamic propagation of VLAN information across the network are not worth the potential for unexpected behavior due to operational error. For this reason, VTP transparent mode is configured in this architecture.

Step 1: Set the switch to ignore VTP auto-configuration.

```
vtp mode transparent
```

Procedure 4 Configure spanning tree

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

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

Step 1: Enable spanning tree.

```
spanning-tree mode rapid-pvst
```

Procedure 5 Enable UDLD

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

Step 1: Enable UDLD.

```
udld enable
```

Procedure 6 Configure EtherChannel load-balancing

EtherChannels are used extensively in this design because of their resiliency capabilities. You should configure all LAN switches similarly to normalize the method in which traffic is load-shared across the member links of the EtherChannel.

Step 1: Configure the switch to use the traffic source and destination IP address when calculating which link to send the traffic across.

```
port-channel load-balance src-dst-ip
```

Procedure 7 Configure VLANs on the switch

Configure Virtual LANs on the switch for all VLANs to which the server needs connectivity.

Step 1: Configure the data, voice, and management VLANs on the switch.

```
vlan [server vlan 1],[server vlan 2],[management vlan]
```

Procedure 8 Configure in-band management

Step 1: Configure a switched virtual interface (SVI) with an IP address for in-band management

```
interface Vlan [management vlan]
  ip address [ip address] [subnet mask]
  no shutdown
ip default-gateway [gateway]
```

Procedure 9 Configure core downlink to access switch

The links to server-room switches are Layer 2 EtherChannels. Connect the server-room EtherChannel uplinks to separate stack members or interface modules in the core switch.

Step 1: Add the VLANs to the core switch's VLAN database that the downlink will carry.

```
vlan [server vlan 1],[server vlan 2]
```

Step 2: Configure two or more physical interfaces to be members of the EtherChannel. LACP ensures that a proper EtherChannel is formed.

```
interface range [interface type] [port 1], [interface type] [port 2]
  switchport
  macro apply EgressQoS
  channel-protocol lacp
  channel-group [number] mode active
```

Tech Tip

The Catalyst 4500 requires that the MTU be set to something other than 1500 on 10-gigabit interface when using resilient Supervisor 7-Es. Run the following additional command only for 10-gigabit interfaces on a Catalyst 4500 with resilient Supervisor 7-Es.

```
mtu 1520
```

Step 3: Configure an 802.1Q trunk for the connection to the access layer. Prune the VLANs allowed on the trunk to only those VLANs that are active on the access switch. The port-channel number must match channel-group configured in Step 2.

```
interface Port-Channel[number]
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan [server vlan 1],[server vlan 2],[mgmt vlan]
  switchport mode trunk
  no shutdown
```

Tech Tip

The Catalyst 4500 does not require the **switchport trunk encapsulation dot1q** command.

Step 4: If the VLANs on the downlink did not already exist on the core switch, add an (SVI) for every access-layer VLAN that the VLANs can route to the rest of the network.

If you did not provision IOS DHCP scopes on your core switch, use the **ip helper-address** command to allow remote DHCP servers to provide IP addresses for this network. The address to which the helper command points is the DHCP server; if you have more than one DHCP server, multiple helper commands can be listed on an interface.

```
interface vlan [number]
  ip address [ip address] [mask]
  ip helper-address [dhcp server ip]
  ip pim sparse-mode
  no shutdown
```

Procedure 10 Configure VLAN-hopping mitigation

Step 1: Add VLAN-hopping mitigation for the trunk.

```
interface Port-channel [number]
 switchport trunk native vlan 999
```

Procedure 11 Configure server room uplink ports

This procedure details how to connect a server room switch to the LAN core.

Step 1: Configure EtherChannel to core.

Configure two or more physical interfaces to be members of the EtherChannel and then set LACP to active on both sides, to ensure that a proper EtherChannel is formed and does not cause any issues.

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

Step 2: Configure the 802.1Q trunk.

Use an 802.1Q trunk to connect to this upstream device, which allows it to provide the Layer 3 services to all the VLANs defined on the server room switch. The VLANs allowed on the trunk are pruned to only the VLANs that are active on the server room switch.

```
interface Port-channel1
switchport trunk encapsulation dot1q
switchport trunk allowed vlan [server vlan 1],[server vlan
2],[management vlan]
switchport mode trunk
no shutdown
```

Step 3: Add VLAN-hopping mitigation for the uplink trunk.

```
vlan 999
interface Port-channel1
 switchport trunk native vlan 999
```

Procedure 12 Configure server access ports

Step 1: Configure switch interfaces to offer basic server connectivity.

```
interface range [interface type] [port number]-[port number]
  switchport access vlan [server vlan 1]
  switchport mode access
```

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

```
switchport host
```

Step 3: To trust the QoS markings on the traffic from the servers based on the QoS macro configuration, enter the following command.

```
macro apply EgressQoS
```

Reader Tip

It is possible that your server or application may require special configuration like trunking or port channeling. Refer to vendor documentation for this information.

Security Module

Business Overview

With most networks connected to the Internet, which are vulnerable to a constant barrage of worms, viruses, and targeted attacks, organizations must vigilantly protect their network, user data, and customer information.

Organizations that rely on a data network to support day-to-day activities face security challenges that affect many aspects of the network's function:

- Organizations need to provide users access to Internet services (email and web).
- Users in remote locations need access to services inside the organization.
- Organizations need to provide controlled access to data and/or services for the public, partners, and customers.
- Organizations need to improve employee productivity by controlling Internet access to work-related locations.
- Organizations need to manage security risk associated with Internet connectivity.

The Security module focuses on the security aspects of the Internet Edge, the server room and the core.

The Internet edge provides connectivity for traffic traversing between the organization and the Internet. This includes traffic to and from the organization, the Internet, and DMZs. An organization's Internet edge deployment needs to enforce the organization's security policy and function as a real-world representation of that policy. As part of this policy, employees' appropriate use of Internet services is an important consideration to maintain productivity, avoid legal issues, and reduce costs associated with non-work-related bandwidth consumption.

Internet edge allows you to provide users with access to the services and data they require to perform their roles, regardless of the user's location.

The server room houses the organization's critical assets and requires additional protection. This design employs a more granular security policy, specific to the applications deployed in the server room. Limiting the permitted traffic in the server room to only what is specifically required will limit the exposure of these important servers to attacks.

In Borderless Networks, a user could be an employee, a contractor, a partner, or a customer. Each user has different needs for access, data, and services.

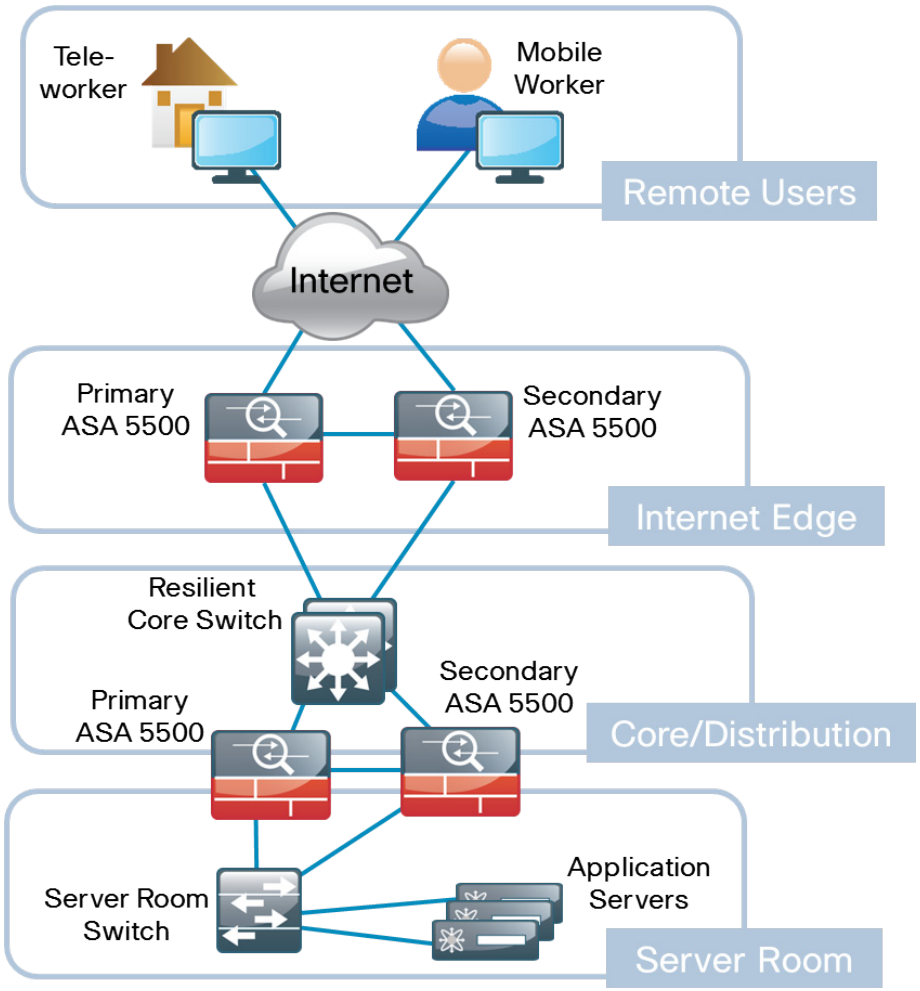
As users' Internet access requirements broaden, the risk associated with such access must be managed. This risk can be broken down into two fundamental types: direct attacks, where specific information or resources are sought for misappropriation, and indirect attacks, where malicious software agents are planted to gather information or consume resources over a longer term. The result of not protecting the organization against this activity includes loss of intellectual property, data theft, resource misuse, and even potential legal liability.

Technical Overview

The Internet edge is the point in the network where the company network connects to the Internet; this is the perimeter of the corporate network, separating your core network—including your users and important assets—from the open, unsecured Internet.

At the Internet edge, it is common to have a firewall, a VPN appliance, and an intrusion prevention system (IPS) appliance. In this design, the Cisco Adaptive Security Appliance (Cisco ASA) is deployed at the Internet edge and performs these functions in a single, low-cost device. Cisco ASA is also deployed in the server room to provide more granular access policies as well as IPS functions. In the core, an IPS appliance is deployed to monitor all the user traffic for an additional layer of inspection.

Figure 11 - Security module



Reader Tip

In the Security Module, basic Cisco ASA Firewall setup and VPN configuration are each addressed in their own sections. IPS is also covered in its own section because dedicated IPS appliances and router-integrated IPS are also deployed at other places throughout the network. As regulatory requirements vary widely, this document does not offer detailed coverage of specific regulatory requirements.

Security Policy Development

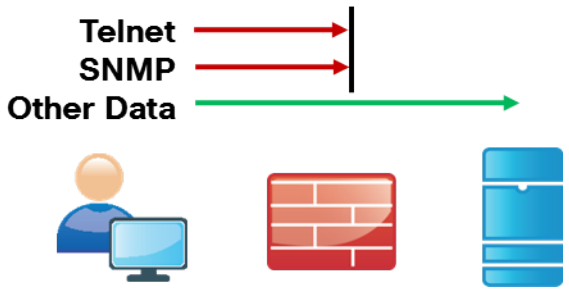
A business should have an IT security policy as a starting point in defining its firewall policy. If there is no companywide security policy, it will be very difficult to define an effective policy for the business while maintaining a secure computing environment.

Reader Tip

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

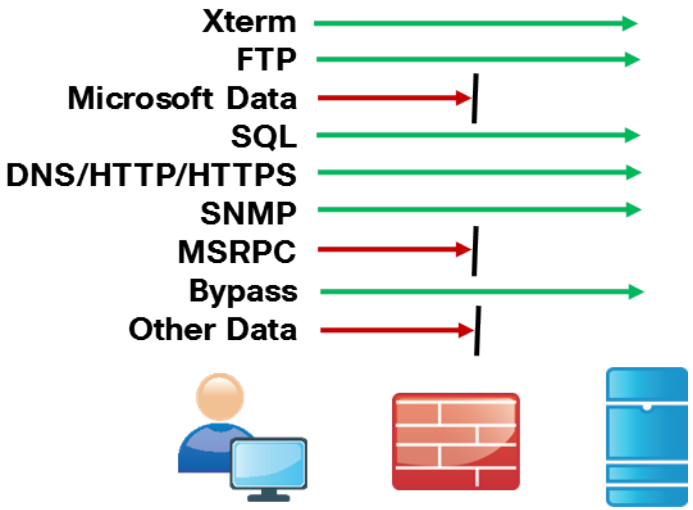
Network security policies can be broken down into two basic categories: "whitelist" policies and "blacklist" policies. A blacklist policy denies traffic that specifically poses the greatest risk to network resources.

Figure 12 - Blacklist security policy



Inversely, a whitelist security policy offers a higher implicit security posture, blocking all traffic except that which must be allowed (at a sufficiently granular level) to enable applications. Other traffic is blocked and does not need to be monitored to assure that unwanted activity is not occurring, reducing the volume of data that will be forwarded to an intrusion detection system (IDS) or IPS and minimizing the number of log entries that must be reviewed in the event of an intrusion or data loss.

Figure 13 - Whitelist security policy



Whitelist policies can be identified by the last rule of the policy rule-set; whitelist policies always end with a rule to deny any traffic that has not been denied or allowed by previous rules. Cisco ASA firewalls implicitly add a deny-all rule at the end of an access-list. Blacklist policies include an explicit rule, prior to the implicit deny-all rule, to allow any traffic that is not explicitly allowed or denied.

A blacklist policy is simpler to maintain and less likely to interfere with network applications; a whitelist policy is the best-practice option if you have the opportunity to examine the network's requirements and adjust the policy to avoid interfering with desired network activity. Whitelist policies are generally better positioned to meet regulatory requirements because only traffic that must be allowed to conduct business is allowed.

Whether you choose a whitelist or blacklist policy basis, IDS or IPS can monitor 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. IPS can detect and prevent known attacks as they occur and provide detailed information to track the malicious activity to its source. IDS or IPS may also be required by the regulatory oversight to which a network is subject (for example, PCI 2.0).

A blacklist policy that blocks high-risk traffic offers a lower-impact, less-secure option (as compared to a whitelist policy) in cases where either:

- A detailed study of the network's application activity is impractical.
- The network availability requirements prohibit application troubleshooting.

If identifying all of the application requirements is not practical, an organization can apply a blacklist policy with logging enabled so that a detailed study of the policy can be developed. With network-behavior details in hand, it is easier for an organization to develop a more effective whitelist policy.

By leaving the majority of the network access open, the server room's resources are exposed to greater risk of compromise. When using a less-restrictive policy for data access between the user network and the server room, strongly consider using IDS or IPS to minimize the likelihood of data security compromise or to provide a forensic trail in the event data tampering or loss is discovered. Applying IPS properly can reduce the likelihood of unwanted network activity.

To effectively evaluate security policy requirements, answer these questions:

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

Deployment Details

Cisco ASA is available in several form factors and performance levels. Cisco ASA integrates several different capabilities:

- Network Address Translation (NAT)
- Stateful inspection firewall
- Remote-access SSL VPN
- Remote-access and site-to-site IPsec VPN
- A hardware bay that accommodates Security Service Modules (SSMs), such as the Intrusion Prevention System SSM (AIP-SSM)

Cisco ASA platforms are specified according to several different performance expectations, including throughput, number and type of interfaces, firewall (NAT and inspection) performance expectation, and the number of remote users that are anticipated. Each deployment section offers recommendations for typical devices that are deployed to address varying expectations.

Cisco ASA Firewall for the Internet Edge

At the Internet edge, a resilient pair of Cisco ASAs is deployed to enforce the security policy between the Internet and the internal network, including the DMZ. It will provide NAT for the inside hosts, which are using RFC 1918 private addressing, and it will provide remote-access VPN service for mobile users.

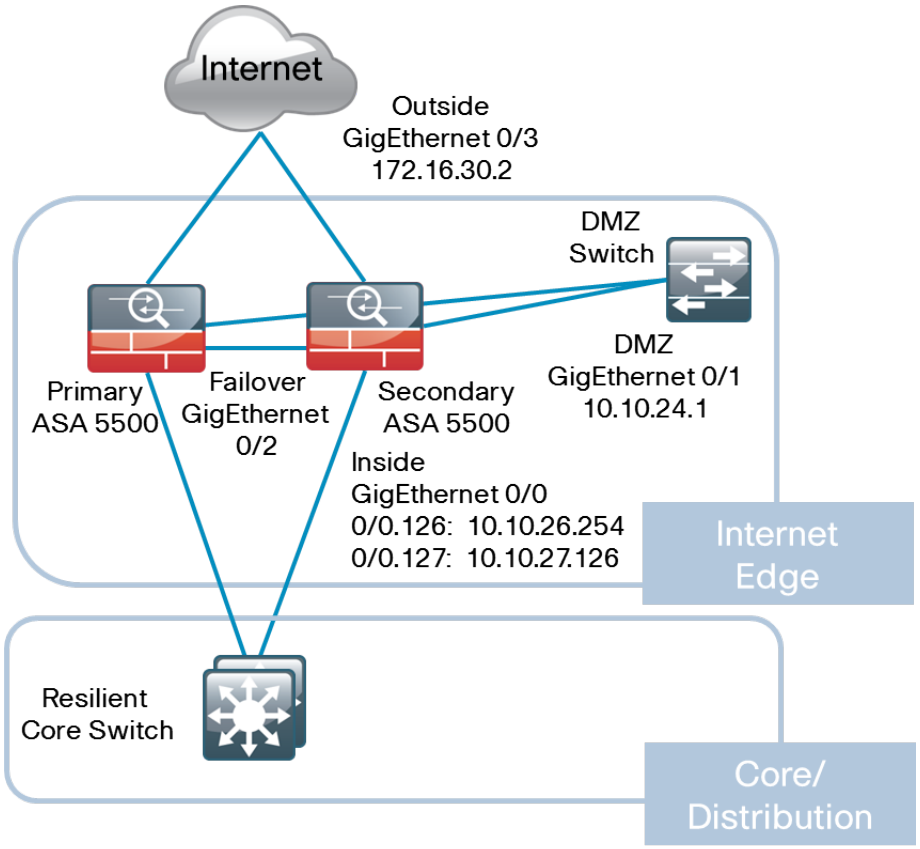
Cisco ASA is set up as a highly available active/standby pair. Active/standby allows the use of the same appliance for firewall and VPN (VPN functionality is disabled on Cisco ASA in active/active).

The Internet link speeds in this design do not surpass the performance of a single Cisco ASA appliance. In the event that the active appliance fails or needs to be taken out of service for maintenance, the secondary appliance will take over all firewall, IPS, and VPN functions.

Cisco ASA is running EIGRP on the inside to simplify the routing configuration; therefore changes to the campus and WAN do not require routing configuration changes on Cisco ASA. There is a DMZ configured in case there is a need for Internet-accessible servers to be hosted on site, but these are not configured in this example. The inside interface is trunked to the core switch with a VLAN interface for corporate Internet traffic and another VLAN configured for wireless guest Internet access.

This design applies the following topology and IP addresses for Cisco ASA firewall connectivity for the Internet Edge. IP addresses and specific interfaces in this example are for demonstration purposes only and will likely differ in your network.

Figure 14 - Cisco ASA connectivity for the Internet edge



Process

Configuring firewall for Internet access for internal network

1. Apply Cisco ASA initial configuration
2. Configure firewall high availability
3. Configure the LAN Core Connection
4. Configure the ASAs' inside interfaces
5. Configure management, logging, and time
6. Configure connectivity to the Internet
7. Configure firewall EIGRP routing
8. Configure address translation
9. Configure basic Internet access rule

Complete each of the following procedures to configure a resilient pair of Cisco ASA 5540s for the Internet edge. The Cisco ASA's network ports are connected as follows:

- GigabitEthernet 0/0 connects to an Internet service provider's gateway device.
- GigabitEthernet 0/1 connects to a DMZ switch.
- GigabitEthernet 0/2 connects via a crossover or straight-through Ethernet cable to the other Internet Edge Cisco ASA for the failover link.
- GigabitEthernet 0/3 connects directly to a trunk port on the LAN core switch.

Reader Tip

Cisco ASA 5520 and 5540 offer Gigabit Ethernet ports. The Cisco ASA 5510 offers Fast Ethernet ports. Port names in the text reflect the Gigabit Ethernet ports of the ASA 5520 and 5540.

Procedure 1 Apply Cisco ASA initial configuration

Initial configuration is applied on the primary (of the high-availability pair) Cisco ASA's command-line interface (CLI) through the console port.

Step 1: Configure the host name and domain name for Cisco ASA.

```
hostname IE-ASA5540
domain-name cisco.local
```

Step 2: Configure an enable password and console/telnet password.

```
enable password [password]
passwd [password]
```

Step 3: Configure an administrative username and password.

```
username admin password [password] privilege 15
```

Tech Tip

All passwords in this document are examples and should not be used in production configurations. Follow your company's policy, or if no policy exists, create a password using a minimum of 8 characters with a combination of uppercase, lowercase, and numbers.

Procedure 2 Configure firewall high availability

For failover to work, both units must be identical, meaning that they need to be the same model, with identical licenses and SSMs. You must cable the secondary Cisco ASA unit similar to the primary. Note the following:

- An Ethernet cable (crossover or straight through) connects the primary and secondary units' failover interfaces. The connection between the failover interfaces is not carried through an Ethernet switch.
- The failover interface is also the state failover interface, meaning that the session state is replicated from the primary to the standby unit on this interface. This can be a substantial amount of data, so Cisco recommends that this be a dedicated interface.

Step 1: Configure failover on the primary Cisco ASA unit.

```
interface GigabitEthernet0/2
  no shutdown
failover
failover lan unit primary
failover lan interface failover GigabitEthernet0/2
failover replication http
failover key [key]
failover link failover GigabitEthernet0/2
failover interface ip failover 10.10.27.130 255.255.255.252
standby 10.10.27.129
```

Step 2: Configure failover on the secondary Cisco ASA unit.

```
interface GigabitEthernet0/2
  no shutdown
failover
failover lan unit secondary
failover lan interface failover GigabitEthernet0/2
failover replication http
failover key [key]
failover link failover GigabitEthernet0/2
failover interface ip failover 10.10.27.130 255.255.255.252
standby 10.10.27.129
```

This step causes the Cisco ASA units to synchronize their configuration from the primary unit to the secondary. This is the only configuration that you need to apply on the secondary unit.

Step 3: (Optional) You can tune the failover timers to speed up failover in the event of a device or link failure. With the default, depending on the failure, Cisco ASA can take from 2 to 25 seconds to failover to the standby unit. Tuning the failover poll times can reduce that to 0.5 to 5 seconds, depending on the failure.

On an appliance with low to average load, the poll times can be tuned down without performance impact.

Tune the failover timers.

```
failover polltime unit 1 holdtime 3
failover polltime interface 1 holdtime 5
```

Procedure 3 Configure the LAN Core Connection

Use a pair of Ethernet VLAN trunks to connect the Cisco ASAs' inside interfaces to the LAN core.

Step 1: Define the LAN's Internet Edge VLAN.

```
vlan 127
 name core-ie-asa
```

Step 2: Configure switchports to connect to the Cisco ASAs.

```
interface GigabitEthernet1/2/48
 description To IE-ASA5540a
!
interface GigabitEthernet2/2/48
  description To IE-ASA5540b
!
interface range GigabitEthernet1/2/48,GigabitEthernet2/2/48
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 127
 switchport mode trunk
```

Tech Tip

The Catalyst 4500 does not require the **switchport trunk encapsulation dot1q** command.

Step 3: Configure the Internet edge switched virtual interface.

```
interface Vlan127
  ip address 10.10.27.1 255.255.255.128
  no shutdown
```

Reader Tip

Multicast is not configured on the core's Layer 3 interfaces that connect to the Internet Edge firewalls, because multicast is not used for any services that connect through the firewalls.

Step 4: Configure the core to form EIGRP adjacencies for the Internet Edge VLAN.

```
router eigrp 1
  no passive-interface Vlan127
```

Procedure 4 Configure the ASAs' inside interfaces

A pair of Ethernet VLAN trunks is used to connect the Cisco ASAs' inside interfaces to the LAN core.

All Cisco ASA interfaces have a security-level setting. The higher the number, the more secure the interface. Inside interfaces are typically assigned 100, the highest security level. Outside interfaces are generally assigned 0.

By default, traffic can pass from a high-security interface to a lower-security interface. In other words, traffic from an inside network is permitted to an outside network, but not conversely.

Step 1: Clear any name, security-level, and ip-address settings and then enable the interface.

```
interface GigabitEthernet0/0
  no nameif
  no security-level
  no ip address
  no shutdown
```

Step 2: Configure a VLAN 127 subinterface on GigabitEthernet 0/0 for connectivity to the inside network. You configure the interface as a VLAN trunk to allow flexibility to add additional connectivity (such as a guest wireless VLAN).

```
interface GigabitEthernet0/0.127
  vlan 127
  nameif inside
  security-level 100
  ip address 10.10.27.126 255.255.255.128 standby 10.10.27.125
```

Tech Tip

The interfaces have a standby IP address in addition to the main address. This is part of the firewall failover configuration that is used to determine if the interface is connected and available to the network. Interfaces that will not be monitored do not need a standby address.

Step 3: Configure failover to monitor the inside interface.

```
monitor-interface inside
```

Procedure 5 Configure management, logging, and time

Now that the Cisco ASA units are connected to the inside LAN, configure the devices so that they synchronize time with an NTP server, and set up the management and logging configuration.

Step 1: Configure time synchronization, logging, and SNMP monitoring.

```
ntp server 10.10.48.17
clock timezone PST -8 0
clock summer-time PDT recurring
logging enable
logging trap informational
logging buffered informational
logging host inside 10.10.48.13
snmp-server host inside 10.10.48.35 community [cisco]
snmp-server community [cisco]
snmp-server enable traps snmp authentication linkup linkdown
coldstart warmstart
```

Step 2: Configure the Cisco ASA units to offer remote management access for any internal network via HTTPS and SSH.

```
http server enable
http 10.10.0.0 255.254.0.0 inside
ssh 10.10.0.0 255.254.0.0 inside
ssh version 2
```

Procedure 6 Configure connectivity to the Internet

The outside interface is connected to an Internet service provider's (ISP) Internet gateway device that provides an Ethernet connection.

The ISP will provide you with details for your Internet connection, including:

- IP addresses and subnet mask
- IP address that you will use for the gateway
- DNS server addresses

Step 1: Configure GigabitEthernet 0/3 as the outside interface with an address provided by your ISP, and then assign the interface's name and security level.

```
interface GigabitEthernet0/3
  nameif outside
  security-level 0
  ip address 172.16.30.2 255.255.255.224 standby 172.16.30.3
  no shutdown
```

Step 2: Configure a static default route to the Internet.

```
route outside 0.0.0.0 0.0.0.0 172.16.30.1 1
```

Procedure 7 Configure firewall EIGRP routing

Redistributing static routes causes Cisco ASA to advertise a default route to the rest of the network. If a specific network cannot be accessed, the traffic will follow the default route to Cisco ASA, and the appliance will send the traffic out to the Internet.

Step 1: Configure Cisco ASA to exchange EIGRP dynamic routing with the LAN.

```
router eigrp 1
   network 10.10.0.0 255.255.0.0
   passive-interface default
   no passive-interface inside
   redistribute static
```

The only routers that the Cisco ASA should exchange routing information with are connected to the inside interface; we do not want advertise any internal information to the DMZ(s) or the outside network. Therefore, all of the firewalls' interfaces except the inside interface are set to "passive."

Procedure 8 Configure address translation

Now that the basic configuration has been applied and the device is reachable on the network, configuration will switch to the Cisco ASA's GUI, Adaptive Security Device Manager (ASDM).

Because the inside network is numbered using RFC 1918 addressing that is not Internet-routable, configure NAT to translate the inside private addresses to an outside public address.

Step 1: In a web browser, open Cisco ASDM by browsing to the IP address of the Cisco ASA's inside interface (for example: https://10.10.27.126/).

Step 2: If the browser prompts you with a security certificate warning, accept the warning, and then click **Run ASDM**.

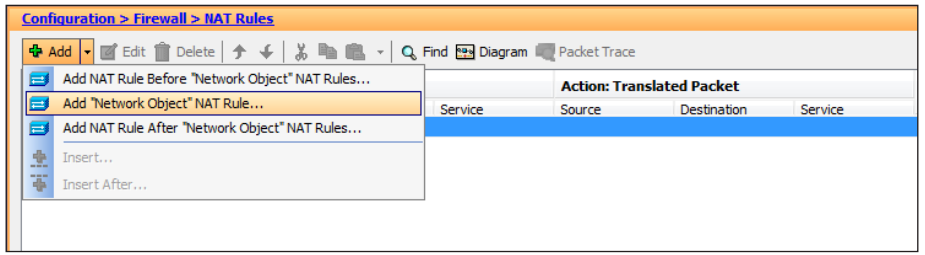
Tech Tip

ASDM requires that you have downloaded and installed an appropriate Java package from http://www.java.com on your management workstation.

Step 3: As Cisco ASDM starts, if Java prompts you with another certificate warning, accept the warning.

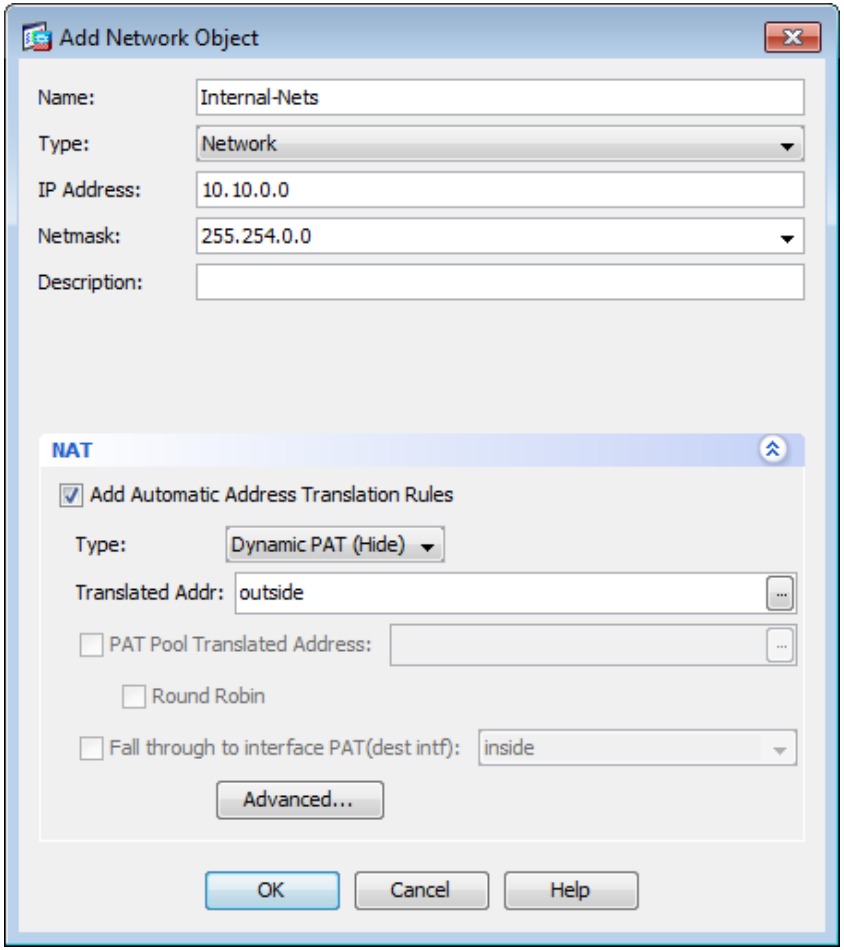
Step 4: Log in with the username **admin** and the password that you defined earlier in the Cisco ASA configuration.

Step 5: Browse to **Configuration > Firewall > NAT Rules**, click the drop-down arrow next to **Add**, and then click **Add "Network Object" NAT Rule**.



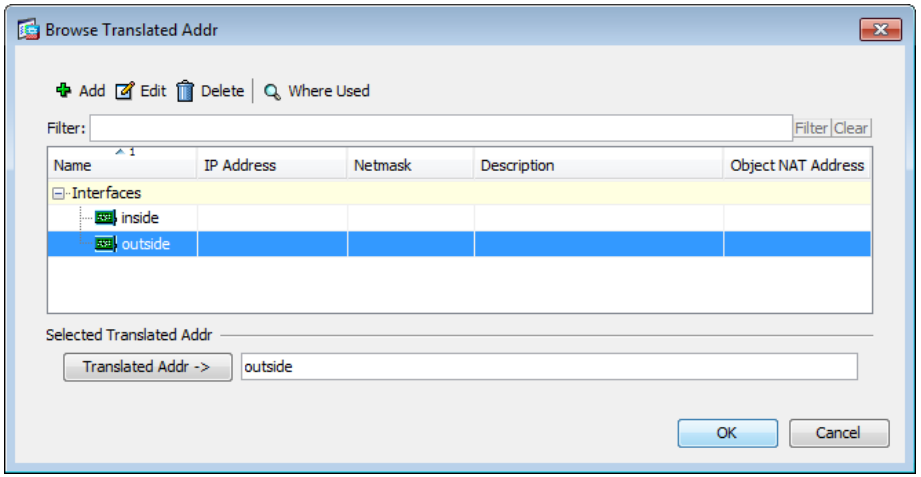
Step 6: In the **Add Network Object** window, apply these configuration values:

- Name: Internal-Nets
- Type: Network
- IP Address: 10.10.0.0
- Netmask: 255.254.0.0
- Description: All Internal Networks
- Verify that the **Add Automatic Network Translation Rules** box is selected.
- Type: **Dynamic PAT (Hide)**



Step 7: In the **Add Network Object** window, next to **Translated Address**, click the ellipses.

Step 8: In the **Browse Translated Address** window, select (double-click) the **outside** interface, and then click **OK**.



Step 9: In the **Add Network Object** window, review the configuration, and then click **OK**.

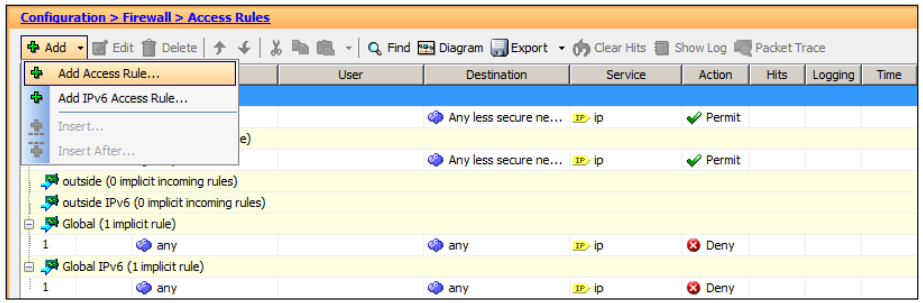
The preceding steps will apply this configuration.

```
object network Internal-Nets
  subnet 10.10.0.0 255.254.0.0
  description All Internal Networks
  nat (any,outside) dynamic interface
```

Procedure 9 Configure basic Internet access rule

Define a firewall policy that allows hosts in the LAN and DMZ to reach the Internet.

Step 1: In ASDM, browse to **Configuration > Firewall > Access Rules**, click the drop-down arrow next to **Add**, and then select **Add Access Rule**.



Step 2: In the **Add Access Rule** window, apply these configuration values:

- Interface: -- Any --
- Action: Permit

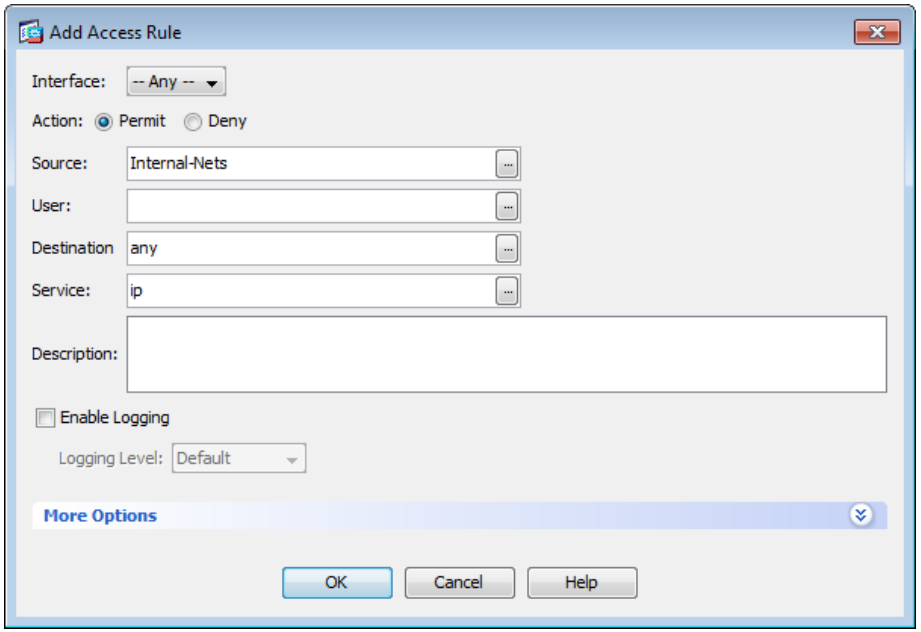
Step 3: In the **Source** field, enter the name of the **Internal-nets** object that you created earlier in Procedure 8, Step 6.

Tech Tip

If you begin typing an object name, ASDM will offer a list of object names that begin with the characters you have defined. You can typically type the first few letters of the object name, andthen select the appropriate item from the list. You also have the option of clicking the ellipses, and picking object names from the list.

Step 4: In the **Destination** field, choose or type **any.**

Step 5: Ensure the **Enable Logging** box is cleared.



The preceding steps will apply this configuration:

```
access-list global_access line 1 extended permit ip object
Internal-Nets any  log disable
access-group global_access global
```

This concludes the initial configuration process for the Internet edge Cisco ASA firewall.

Process

Configuring Internet Edge Cisco ASA for DMZ Services

1. Configure the ASA's DMZ interface
2. Configure the DMZ switch
3. Add DMZ NAT rule to ASA
4. Add DMZ firewall rule to ASA

The Internet Edge Cisco ASA offers firewall service for a demilitarized zone (DMZ) to provide web and file-transfer services for the Internet.

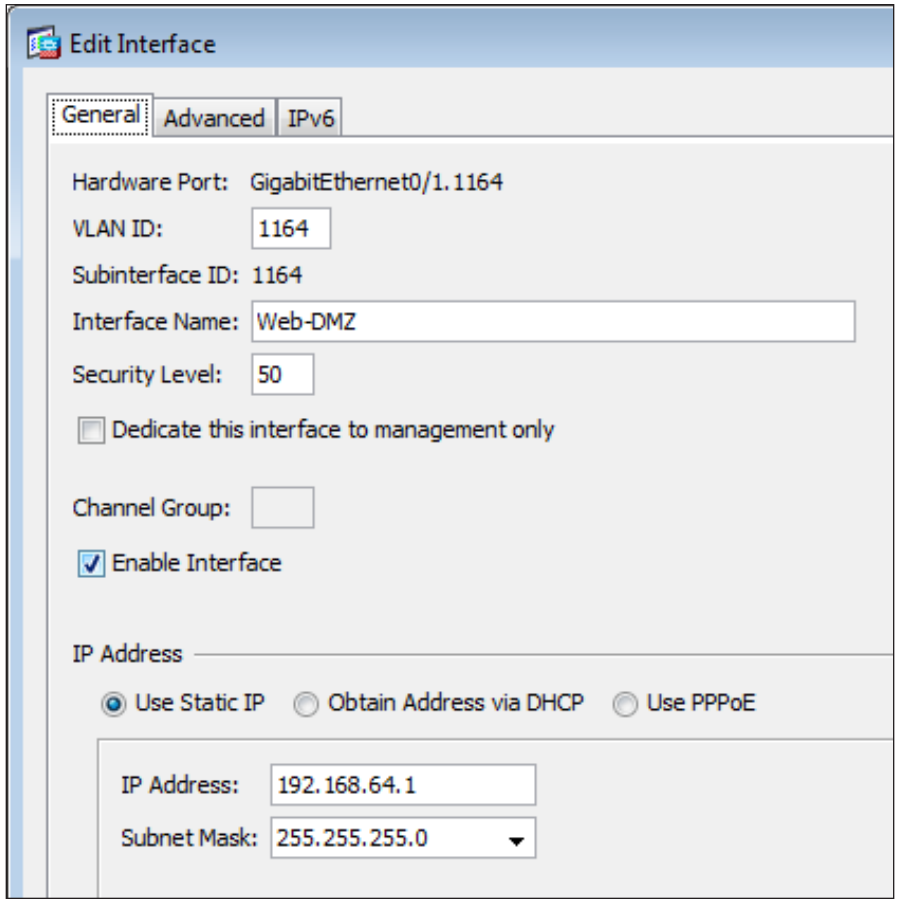
Procedure 1 Configure the ASA's DMZ interface

GigabitEthernet 0/1 provides connectivity for DMZ hosts that provide services for the Internet and guest-network users. To provide flexibility to add additional DMZ VLANs, the DMZ interface is a VLAN trunk connected to a Layer 2 Ethernet switch.

Step 1: In ASDM, browse to **Configuration > Device Setup > Interfaces**, click **Add**, and then select **Interface.**

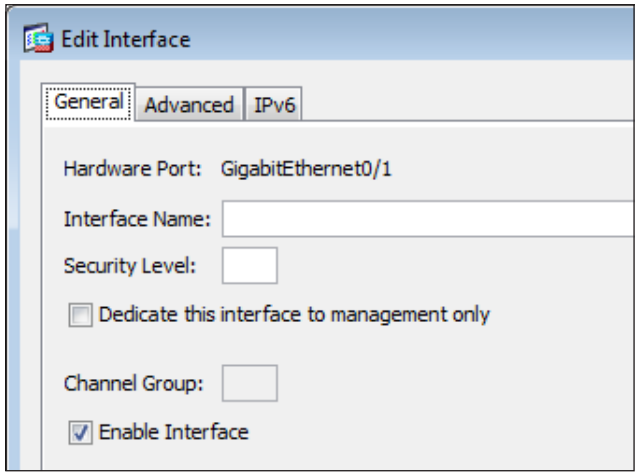
Step 2: In the **Add Interface** window, enter the following configuration details, and then click **OK**.

- Hardware Port: **GigabitEthernet0/1**
- VLAN ID: **1164**
- Subinterface ID: **1164**
- Interface Name: **Web-DMZ**
- Security Level: **50**
- Be certain that the **Dedicate This Interface to Management Only** box is cleared and the **Enable Interface** box is selected.
- Description: **Web and File Transfer DMZ**
- IP Address:: **192.168.64.1**
- Subnet Mask: **255.255.255.0**



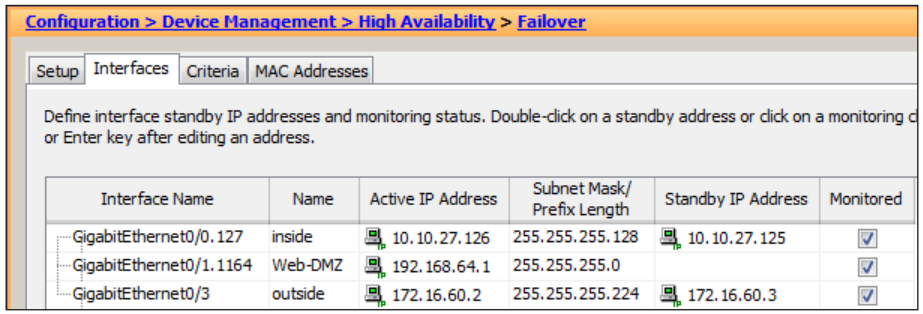
Step 3: In the **Configuration > Device Setup > Interfaces** window, select the line for the **GigabitEthernet0/1** physical interface, and then click **Edit.**

Step 4: In the **Edit Interface** dialog box, select **Enable Interface**, ensure that no other values (IP address, name, security level) are configured on this interface, and then click **OK**.



Step 5: Browse to **Configuration > Device Management > High Availability > Failover**, and then select the **Interfaces** tab.

Step 6: For the **Web-DMZ** interface, select **Monitored**, and then click **Apply**.



This procedure will result in this configuration:

```
interface GigabitEthernet0/1
 no nameif
 no security-level
 no ip address
 no shutdown
!
interface GigabitEthernet0/1.1164
 description Web and File Transfer DMZ
 vlan 1164
 nameif Web-DMZ
 security-level 50
 ip address 192.168.64.1 255.255.255.0
 no shutdown
!
monitor-interface Web-DMZ
```

Procedure 2 Configure the DMZ switch

The two-member DMZ switch stack provides high-performance, resilient Ethernet switching for devices that connect to the Cisco ASAs' DMZ ports. One Ethernet trunk port on each switch stack member is connected to the DMZ ports on the firewall pair. The DMZ switch stack differs from all of the rest of the switches in the LAN, because the Ethernet Management port is used for out-of-band management access to the switch, instead of using in-band management like the rest of the LAN switches.

Reader Tip

The DMZ switche's management ports are FastEthernet ports and, as such, must be connected to a switch that can negotiate a 100Mb/sec Ethernet connection

The following configuration is executed on the DMZ switch's CLI.

Step 1: Apply the configuration described in the Global Configuration Module.

Step 2: Configure a management IP address on the management port.

```
interface FastEthernet0
  ip address 10.10.15.21 255.255.255.128
```

Step 3: Connect the DMZ switch stack members' management ports to the server room switch, and then configure the server-room switch ports as access ports to the management VLAN.

```
interface range GigabitEthernet1/0/21
  switchport mode access
  switchport access vlan 115
  no shutdown
```

Tech Tip

The DMZ switch carries no Layer 3 interfaces, so the switch's management ports can be safely connected to the inside LAN. To avoid a path for network attack or compromise, do not add additional Layer 3 interfaces to the switch.

Step 4: Add the web DMZ VLAN to the DMZ switch's VLAN database.

```
vlan 1164
  name web-dmz
```

Step 5: Configure the trunks that connect to the ASAs' DMZ ports.

```
interface range GigabitEthernet1/0/24,GigabitEthernet2/0/24
  switchport trunk encapsulation dot1q
  switchport mode trunk
  switchport trunk allowed vlan add 1164
```

Step 6: Configure DMZ switch ports where web and file-transfer servers will be connected as access ports.

```
interface GigabitEthernet1/0/13
 description Web and file-transfer server access port
 switchport mode access
 switchport access vlan 1164
```

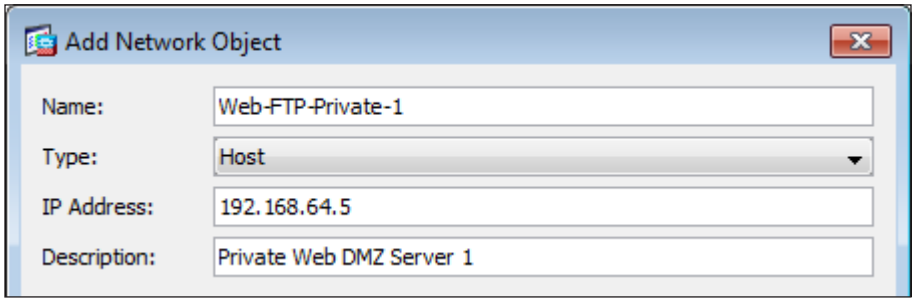
Procedure 3 Add DMZ NAT rule to ASA

To expose the DMZ servers to the Internet, Cisco ASA must carry a NAT rule that translates the private addresses used in the DMZ to the routable addresses on the appliance's outside interface.

Step 1: In ASDM, browse to **Configuration** > **Firewall** > **NAT Rules**, click **Add**, and then select **Add "Network Object" NAT Rule**.

Step 2: In the **Add Network Object** window, enter the following configuration details:

- Name: Web-FTP-Private-1
- Type: Host
- IP Address: 192.168.64.5
- Description: Private Web DMZ Server 1



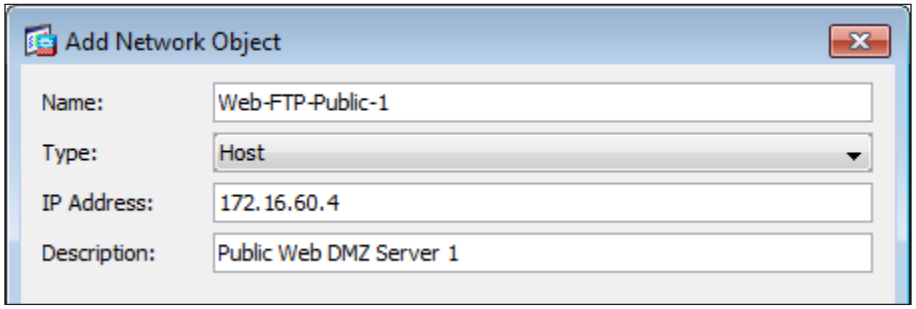
Step 3: Next to **NAT**, click the drop-down arrow, ensure that **Add Automatic Address Translation Rules** is checked, and then in the **Type** box, choose **Static**.

Step 4: For **Translated Address**, click the ellipses.

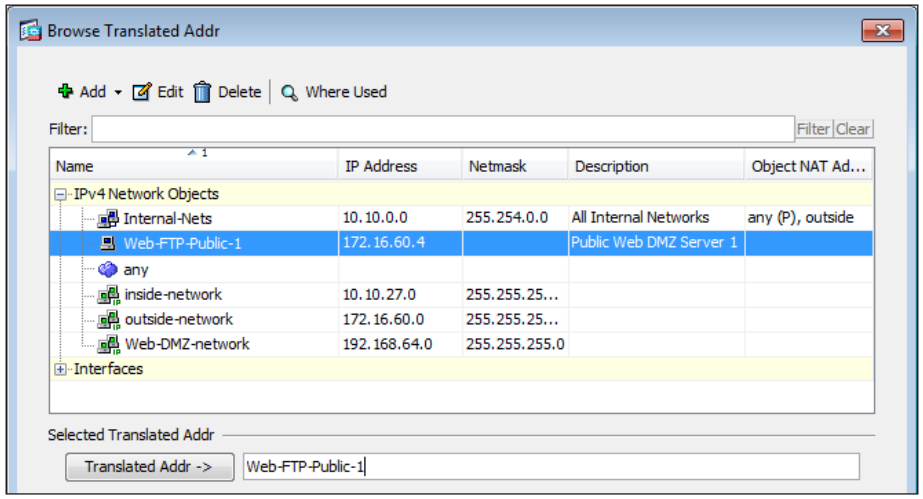
Step 5: In the **Browse Translated Addr** window, click **Add**, and then select **Network Object**.

Step 6: In the **Add Network Object** dialog box, enter the following, and then click **OK**.

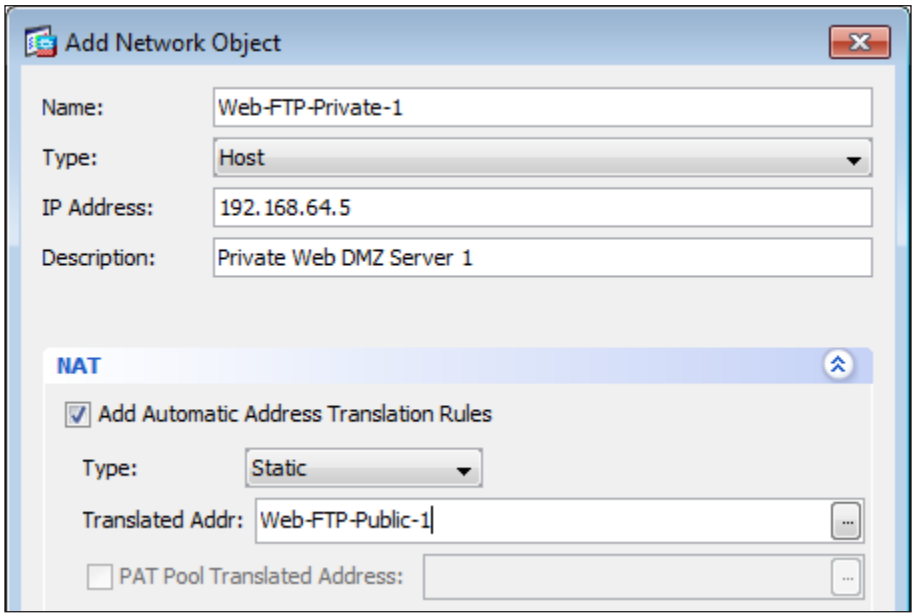
- Name: Web-FTP-Public-1
- Type: Host
- IP Address: 172.16.60.4
- Description: Public Web DMZ Server 1



Step 7: In the **Browse Translated Addr** window, select the host object that you just defined, and then click **OK**.



Step 8: On the **Add Network Object** window, verify your configuration, and then click **OK**.



This procedure will result in this configuration.

```
object network Web-FTP-Private-1
  host 192.168.64.5
  description Private Web DMZ Server 1
object network Web-FTP-Public-1
  host 172.16.60.4
  description Public Web DMZ Server 1
object network Web-FTP-Private-1
  nat static Web-FTP-Public-1
```

Procedure 4 Add DMZ firewall rule to ASA

The NAT rule configured above translates the DMZ addresses to Internet-routable addresses, but you still need access rules to expose DMZ services such as web and FTP.

Step 1: In ASDM, browse to **Configuration** > **Firewall** > **Access Rules**, click **Add**, and then click **Add Access Rule...**

Tech Tip

ASDM displays all default and configured IPv4 and IPv6 rules configured. The view can be simplified by selecting the "IPv4 Only" radio button at the bottom of the panel.

Step 2: In the **Add Access Rule** window, in the **Interface** list, choose **Any**.

Step 3: Beside **Action**, choose **Permit**.

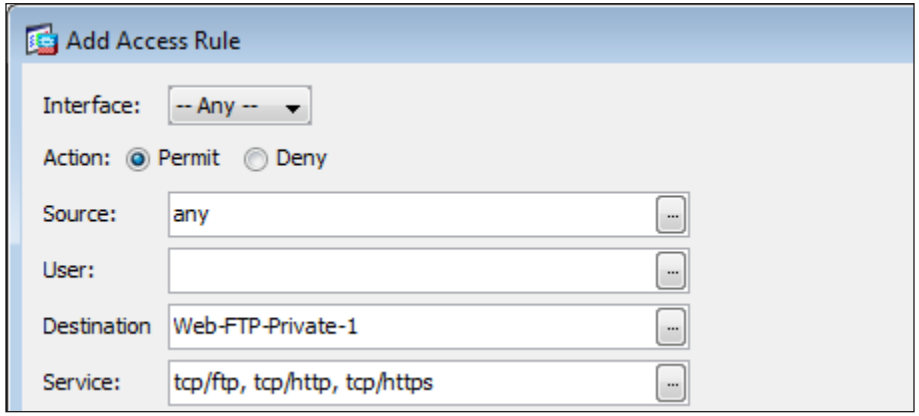
Step 4: In the **Source** field, leave the default value, **any**.

Step 5: In the **Destination** field, enter the name of the Web-FTP-Private-1 object that you created in the DMZ NAT configuration procedure.

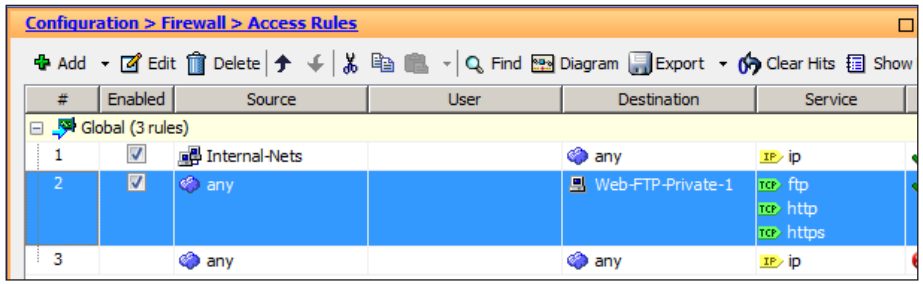
Step 6: In the **Service** field, enter ftp, http, and https, separated by commas, and select **tcp ftp (21)**, **tcp http (80)**, and **tcp https (443)** from the options presented, and then click **OK**.

Tech Tip

ASDM offers suggestions of services that match the first few letters of service names that you type in the Services field. If you have trouble finding the service you're looking for, you can click the ellipsis and pick your service from the list.



Step 7: In the **Configuration** > **Firewall** > **Access Rules** window, verify that the rules in the following figure are applied in your firewall policy in the correct order. The additional rules for DMZ access should follow your rule allowing access from internal networks to everywhere.



When you are finished modifying your access rules, click **Apply**. The configuration changes are sent to the device.

This procedure will result in this configuration.

```
object-group service DM_INLINE_TCP_1 tcp
  port-object eq ftp
  port-object eq http
  port-object eq https
access-list global_access line 2 extended permit tcp any
object Web-FTP-Private-1 object-group DM_INLINE_TCP_1
```

Process

Configuring Internet Edge Cisco ASA for Guest WLAN Service

1. Add guest VLAN interface on the firewall
2. Configure guest VLAN on the core switch
3. Add DMZ NAT rule to Cisco ASA
4. Add DMZ firewall rules to ASA

The Internet Edge Cisco ASA provides a DMZ for wireless guest access to the Internet. The guest WLAN's connectivity is carried via separate VLAN to the wireless LAN controller, where guests connect to their own SSID.

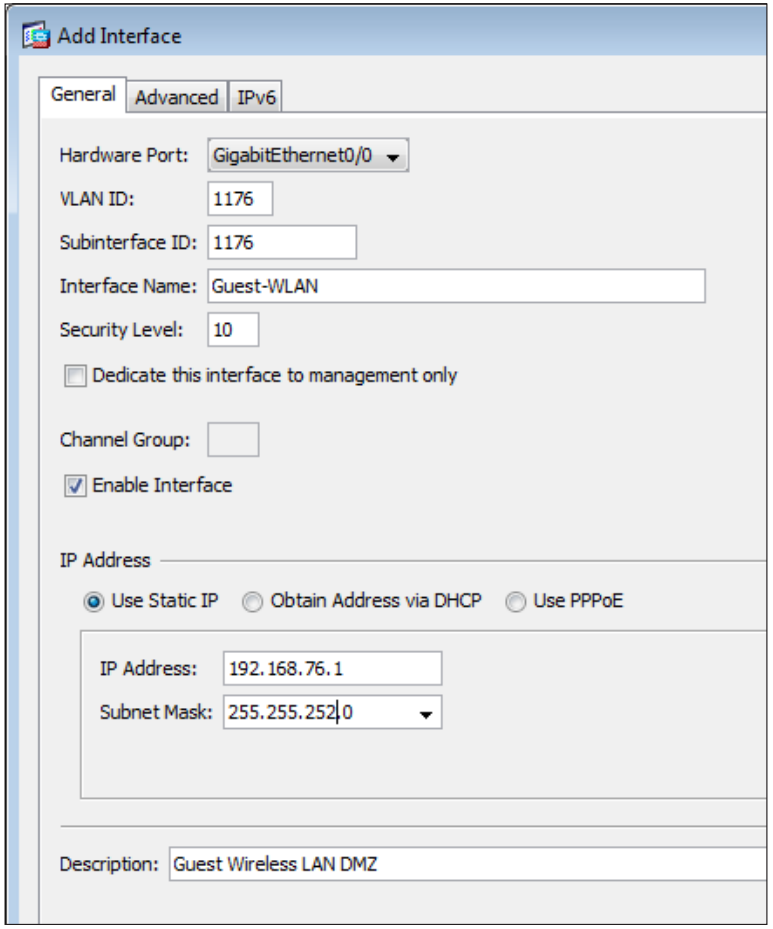
Procedure 1 Add guest VLAN interface on the firewall

An additional VLAN will be added to the Cisco ASA GigabitEthernet 0/0 trunk interface. The firewall's interface is the guest VLAN's default gateway for wireless guest access.

Step 1: In ASDM, browse to **Configuration > Device Setup > Interfaces**. Click **Add**, and then select **Interface.**

Step 2: In the **Add Interface** window, enter the following configuration details, click **OK**, and then click **Apply**.

- Hardware Port: **GigabitEthernet0/0**
- VLAN ID: **1176**
- Subinterface ID: **1176**
- Interface Name: **Guest-WLAN**
- Security Level: **10**
- Be certain that the **Dedicate This Interface to Management Only** box is cleared and the **Enable Interface** box is selected.
- IP Address: **192.168.76.1**
- Security Level: **255.255.252.0**
- Description: **Guest Wireless LAN DMZ**



Tech Tip

The guest LAN does not have a standby address assigned, because the guest interface is carried on the same ethernet VLAN trunk to the core as the inside interface. The guest VLAN's availability is of less concern than that of the inside interface, so the Guest VLAN follows the inside interfaces' failover behavior.

The configuration procedure results in this CLI configuration.

```
interface GigabitEthernet0/0.1176
  vlan 1176
  no shutdown
  description Guest Wireless LAN DMZ
  nameif Guest-WLAN
  security-level 10
  ip address  192.168.76.1 255.255.252.0
```

Procedure 2 Configure guest VLAN on the core switch

The core switch does not carry an SVI for the Guest VLAN because we want to avoid any directly routed connectivity to the LAN.

Step 1: Add the guest VLAN to the core switch's VLAN database.

```
vlan 1176
 name guest-WLAN
```

Step 2: Add the guest VLAN to the trunk ports where the Internet edge firewalls are connected.

```
interface range GigabitEthernet1/2/48,GigabitEthernet2/2/48
 switchport trunk allowed vlan add 1176
```

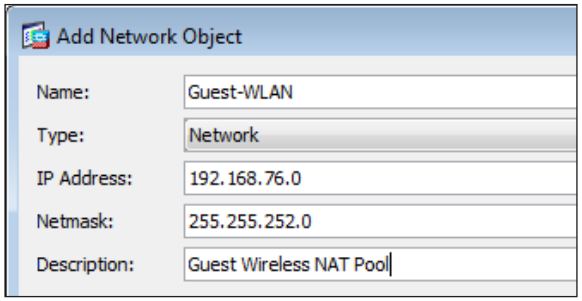
Procedure 3 Add DMZ NAT rule to Cisco ASA

Guest WLAN Internet access is provided by a NAT policy that translates the private addresses assigned to wireless guests to the routable address on the ASA's outside interface.

Step 1: In ASDM, browse to **Configuration > Firewall > NAT Rules**, click **Add**, and select **Add "Network Object" NAT Rule**.

Step 2: In the **Add Network Object** window, fill in these details:

- Name: Guest-WLAN
- Type: Network
- IP Address: 192.168.76.0
- Netmask: 255.255.252.0
- Description: Guest Wireless NAT Pool



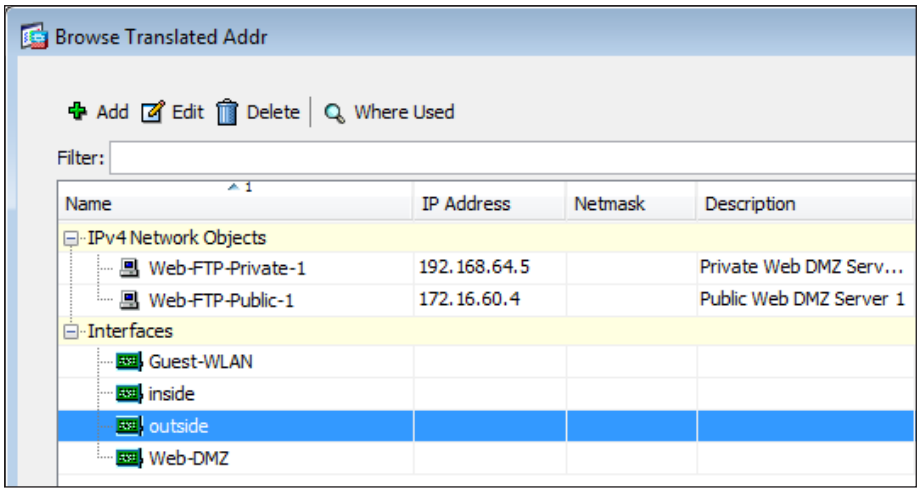
Step 3: Next to NAT, click the drop-down to reveal NAT configuration settings

Step 4: Ensure that **Add Automatic Address Translation Rules** is checked.

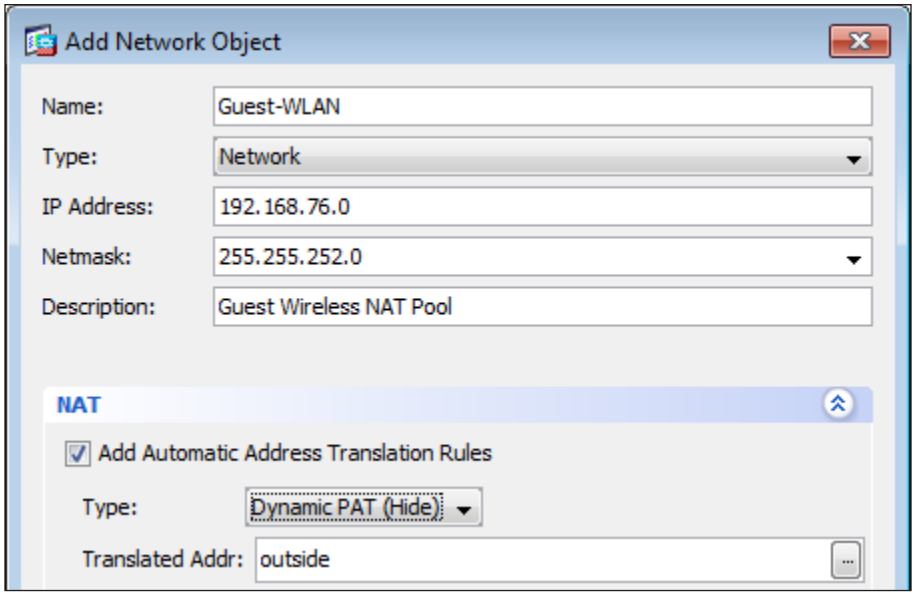
Step 5: In the **Type** list, choose **DynamicPAT**.

Step 6: Next to **Translated Address,** click the ellipses (...).

Step 7: In the **Browse Translated Addr** window, select (double-click) the **outside** interface, and then click **OK**.



Step 8: In the **Add Network Object** window, click **OK**.



This procedure will result in this configuration.

```
object network Guest-WLAN
  subnet 192.168.76.0 255.255.252.0
  description Guest Wireless NAT Pool
  nat (any,outside) dynamic interface
```

Procedure 4 Add DMZ firewall rules to ASA

The NAT rule configured above translates the WLAN DMZ addresses to Internet-routable addresses. An access rule must be configured to prevent the Guest WLAN from reaching internal addresses. Then, another access rule must be configured to allow the guest WLAN to reach all other destinations, which includes the Internet and the DMZ services.

Step 1: In ASDM, browse to **Configuration** > **Firewall** > **Access Rules**. Click **Add**, and then select **Add Access Rule.**

Tech Tip

ASDM displays all default and configured IPv4 and IPv6 rules. The view can be simplified by selecting the **IPv4 Only** radio button at the bottom of the panel.

Step 2: In the **Add Access Rule** window, in the Interface list, choose **Any.**

Step 3: Next to **Action**, select **Deny.**

Step 4: In the **Source** field, enter the name of the **Guest-WLAN-network** object that was created by the WLAN DMZ NAT configuration procedure.

Tech Tip

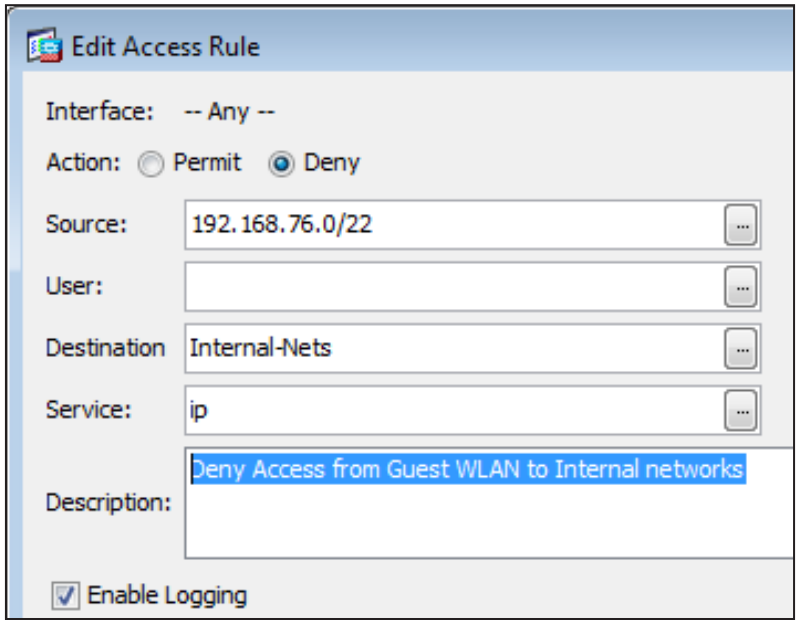
If you begin typing an object name, ASDM will offer a list of object names that begin with the characters you have defined. You can typically type the first few letters of the object name, and then select the appropriate item from the list. You also have the option of clicking the ellipses, and picking object names from the list.

Step 5: In the **Destination** field, enter the name of the **Internal-nets** object that you created earlier in Procedure 8, Step 6.

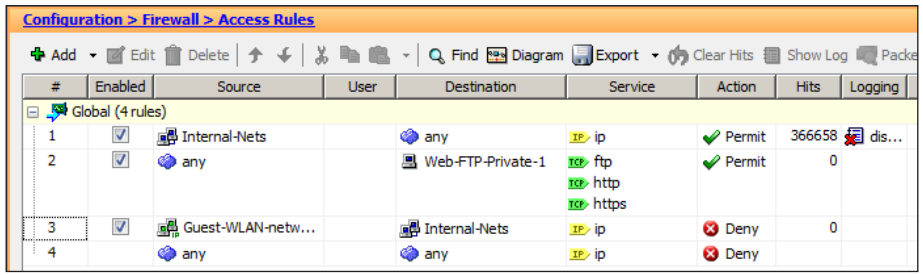
Step 6: In the **Service** field, leave this value at the default, **ip**.

Step 7: In the **Description** field, enter **Deny Access from Guest WLAN to Internal networks**.

Step 8: Select **Enable Logging**.



Step 9: In **Configuration > Firewall > Access Rules**, click **Add**, and then select **Add Access Rule.**



Step 10: In the **Add Access Rule** window, in the **Interface** list, choose **Any.**

Step 11: Next to **Action**, select **Permit**.

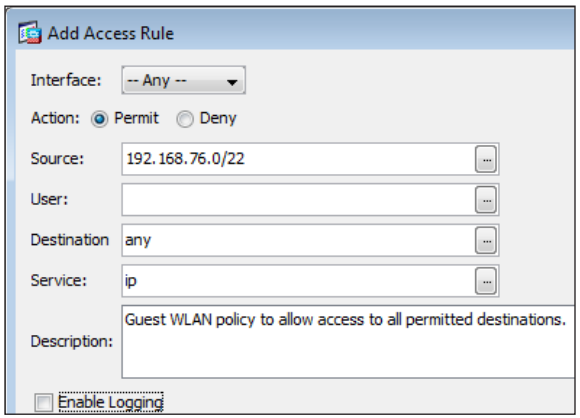
Step 12: In the **Source** field, enter the **Guest-WLAN** network object that was created by the WLAN DMZ NAT configuration procedure.

Step 13: In the **Destination** field, leave this value at the default, **any**.

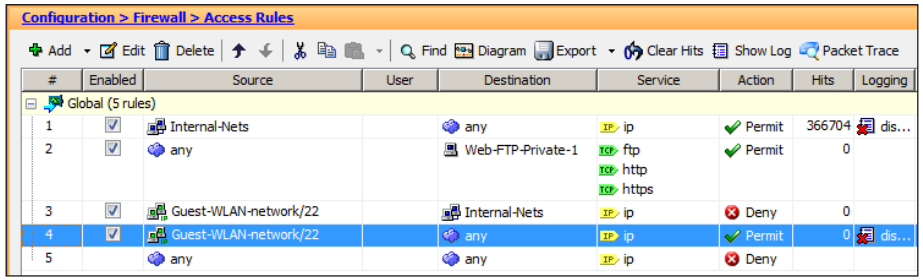
Step 14: In the **Service** field, leave this value at the default, **ip**.

Step 15: In the **Description** field, enter **Guest WLAN policy to allow access to all permitted destinations**.

Step 16: If you want to reduce the volume of log messages, clear **Enable Logging**. If you want to monitor guest Internet access, leave **Enable Logging** selected.



Step 17: In the **Configuration > Firewall > Access Rules** window, verify that these rules are applied in your firewall policy in the correct order. The additional rules for DMZ access should follow your rule allowing access from internal networks to everywhere, with the rule blocking access from guest WLAN users from Internal nets preceding the guest WLAN's permission to all other destinations.



Step 18: When you are finished reviewing the rule order, click **Apply**. The configuration changes are sent to the device.

This procedure will result in this configuration.

```
access-list global_access line 3 remark Deny Access from Guest
WLAN to Internal networks
access-list global_access line 4 extended deny ip 192.168.76.0
255.255.252.0 object Internal-Nets
access-list global_access line 5 remark Guest WLAN policy to
allow access to all permitted destinations.
access-list global_access line 6 extended permit ip
192.168.76.0 255.255.252.0 any  log disable
```

Tech Tip

Note that this configuration only applies to previously existing network objects.

This completes all configuration tasks for the Internet edge Cisco ASA firewall.

Cisco ASA firewall for the server room

For deployment in the server room, Cisco ASA firewall and IPS (as a Security Service Module in the hardware bay) will be deployed to enforce the security policy between the network core and the application server network, and between the different application server networks.

Cisco ASA is set up as a highly available active/standby pair. Active/standby:

- Is much simpler than an active/active configuration.
- Allows the use of the same appliance for firewall and VPN (VPN functionality is disabled on the Cisco ASA in active/active).

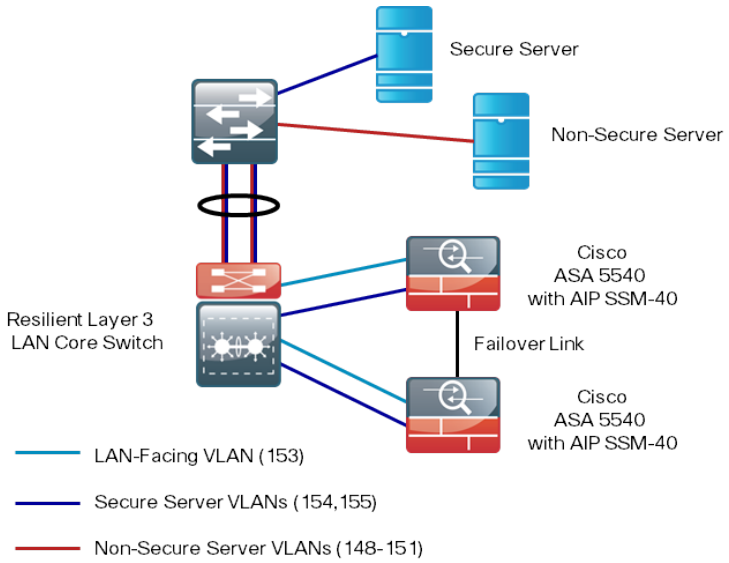
The performance needs in this design do not surpass the performance of a single Cisco ASA appliance.

In the event that the active Cisco ASA appliance fails or needs to be taken out of service for maintenance, the secondary Cisco ASA appliance will take over all firewall and IPSfunctions.

Cisco ASA is running EIGRP on the outside to simplify the routing configuration; therefore changes to the campus and WAN do not require routing-configuration changes on Cisco ASA. One interface is trunked to the core switch with a VLAN interface for each application server network.

This design applies the following topology for Cisco ASA firewall connectivity.

Figure 15 - Cisco ASA connectivity for the server room



Process

Configuring Cisco ASA for the Server Room

1. Apply Cisco ASA initial configuration
2. Configure firewall high availability
3. Configure LAN core untrust-side ports
4. Connect firewall outside to the LAN core
5. Configure management, logging, and time
6. Configure the ASAs' inside interfaces
7. Configure LAN core trust-side ports
8. Add secure VLANs to server room switch
9. Configure firewall EIGRP routing
10. Configure security policy

Complete each of the following procedures to configure Cisco ASA for the Server Room.

Complete each of the following procedures to configure a resilient pair of Cisco ASA 5540s for the Server Room. The Cisco ASA's network ports are connected as follows:

- GigabitEthernet 0/0 connects to a VLAN trunk port offering connectivity to secure server-room LANs
- GigabitEthernet 0/2 connects via a crossover or straight-through Ethernet cable to the other Internet Edge ASA for the Failover link
- GigabitEthernet 0/3 connects directly to an access port on the LAN core switch

Procedure 1 Apply Cisco ASA initial configuration

Initial configuration is applied on the primary (of the high-availability pair) Cisco ASA's CLI through the console port.

Step 1: Configure the host name and domain name for Cisco ASA.

```
hostname SR-ASA5540
domain-name cisco.local
```

Step 2: Configure an enable password and console/telnet password.

```
enable password [password]
passwd [password]
```

Step 3: Configure an administrative username and password.

```
username admin password [password] privilege 15
```

Tech Tip

All passwords in this document are examples and should not be used in production configurations. Follow your company's policy, or if no policy exists, create a password using a minimum of 8 characters with a combination of uppercase, lowercase, and numbers.

Procedure 2 Configure firewall high availability

For failover to work, both units must be identical, meaning that they need to be the same model, with identical licenses and SSMs. You must cable the secondary Cisco ASA unit in a similar way to how you cabled the primary Cisco ASA unit. Note the following:

- An Ethernet cable (crossover or straight through) connects the primary and secondary units' failover interfaces. The connection between the failover interfaces is not carried through an Ethernet switch.
- The failover interface is also the state failover interface, meaning that the session state is replicated from the primary to the standby unit on this interface. This can be a substantial amount of data, so Cisco recommends that this be a dedicated interface.

Step 1: Configure failover on the primary Cisco ASA unit.

```
interface GigabitEthernet0/2
  no shutdown
failover
failover lan unit primary
failover lan interface failover GigabitEthernet0/2
failover replication http
failover key [key]
failover link failover GigabitEthernet0/2
failover interface ip failover 10.10.53.130 255.255.255.252
standby 10.10.53.129
```

Step 2: Configure failover on the secondary Cisco ASA unit.

```
interface GigabitEthernet0/2
  no shutdown
failover
failover lan unit secondary
failover lan interface failover GigabitEthernet0/2
failover replication http
failover key [key]
failover link failover GigabitEthernet0/2
failover interface ip failover 10.10.53.130 255.255.255.252
standby 10.10.53.129
```

This step causes the Cisco ASA units to synchronize their configuration from the primary unit to the secondary. This is the only configuration that you need to apply on the secondary unit.

Step 3: (Optional) You can tune the failover timers to speed up failover in the event of a device or link failure. With the default, depending on the failure, Cisco ASA can take from 2 to 25 seconds to failover to the standby unit. Tuning the failover poll times can reduce that to 0.5 to 5 seconds, depending on the failure.

On an appliance with low to average load, the poll times can be tuned down without performance impact.

Tune the failover timers.

```
failover polltime unit 1 holdtime 3
failover polltime interface 1 holdtime 5
```

Procedure 3 Configure LAN core untrust-side ports

Use a pair of Ethernet ports on the LAN core to provide connections for the Server Room Cisco ASAs' LAN-side (untrusted) interfaces.

Step 1: Define the untrusted VLAN.

```
vlan 153
```

Step 2: Configure core switch ports to connect to the outside of the Cisco ASA Server Room firewalls:

```
interface GigabitEthernet1/2/5
 description SR-ASA5540a-Gi0/3
!
interface GigabitEthernet2/2/5
 description SR-ASA5540b-Gi0/3
!
interface range GigabitEthernet1/2/5,GigabitEthernet2/2/5
 switchport
 switchport access vlan 153
 switchport mode access
 spanning-tree portfast edge
```

Tech Tip

The Catalyst 4500 does not require the switchport trunk encapsulation dot1q command.

Step 3: Configure the Internet edge switched virtual interface.

```
interface Vlan153
  ip address 10.10.53.1 255.255.255.128
  no shutdown
```

Step 4: Configure the core to form EIGRP adjacencies for the Internet Edge VLAN.

```
router eigrp 1
  no passive-interface Vlan153
```

Procedure 4 Connect firewall outside to the LAN core

Next, you configure the firewall so that the interfaces connected to the LAN are the untrusted side of the firewall.

Step 1: Configure Ethernet 0/3 as the outside interface, connected to the network core. The default outside security-level, **0**, will be applied automatically.

```
interface GigabitEthernet0/3
  nameif outside
  security-level 0
  ip address 10.10.53.126 255.255.255.128 standby 10.10.53.125
  no shutdown
```

All Cisco ASA interfaces have a security-level setting. The higher the number, the more secure the interface. Inside interfaces are typically assigned 100, the highest security level. Outside interfaces are generally assigned 0.

By default, traffic can pass from a high-security interface to a lower-security interface. In other words, traffic from an inside network is permitted to an outside network, but not conversely.

Tech Tip

The interfaces have a standby IP address in addition to the main address. This is part of the firewall failover configuration that is used to determine if the interface is connected and available to the network. Interfaces that will not be monitored do not need a standby address.

Step 2: Configure failover to monitor the outside interface.

```
monitor-interface outside
```

Procedure 5 Configure management, logging, and time

Now that the Cisco ASA units are connected to the LAN, configure the devices so that they synchronize time with an NTP server, and set up the management and logging configuration.

Step 1: Configure time synchronization, logging, and SNMP monitoring.

```
ntp server 10.10.48.17
clock timezone PST -8 0
clock summer-time PDT recurring
logging enable
logging trap informational
logging buffered informational
logging host inside 10.10.48.13
snmp-server host inside 10.10.48.35 community [cisco]
snmp-server community [cisco]
snmp-server enable traps snmp authentication linkup linkdown
coldstart warmstart
```

Step 2: Configure the Cisco ASA units to offer remote management access for any internal network via HTTPS and SSH.

```
http server enable
http 10.10.0.0 255.254.0.0 outside
ssh 10.10.0.0 255.254.0.0 outside
ssh version 2
```

Procedure 6 Configure the ASAs' inside interfaces

A pair of Ethernet VLAN trunks is used to connect the Cisco ASAs' inside interfaces to the LAN core. VLAN trunks allow flexibility to offer connectivity for multiple trusted VLANs, as needed. The firewalls carry two inside sub-interfaces, vlan 154 and vlan 155, on the interface.

Step 1: Clear any name, security-level, and ip-address settings, and then enable the interface.

```
interface GigabitEthernet0/0
  no nameif
  no security-level
  no ip address
  no shutdown
```

Step 2: Configure the firewalls' inside subinterfaces for connectivity to the trusted VLANs on the LAN core switch.

```
interface GigabitEthernet0/0.154
  vlan 154
  nameif SRVLAN154
  security-level 100
ip address 10.10.54.1 255.255.255.0 standby 10.10.54.2
!
interface GigabitEthernet0/0.155
  vlan 155
  nameif SRVLAN155
  security-level 100
ip address 10.10.55.1 255.255.255.0 standby 10.10.55.2
```

Step 3: Configure failover to monitor the inside interfaces.

```
monitor-interface SRVLAN154
monitor-interface SRVLAN155
```

Procedure 7 Configure LAN core trust-side ports

In this configuration, multiple VLAN sub-interfaces are trunked from the Cisco ASA units' GigabitEthernet 0/0 inside interfaces to the LAN core, where the secure VLANs are switched to the server room switches. The 154 and 155 VLANs provide connections for two different application server networks, with different security policy requirements for each. Layer 3 interfaces are not defined on the core switch, to prevent inadvertent alternate paths to the trusted server room VLANs.

Step 1: Add the secure VLANs to the core switch's VLAN database.

```
vlan 154-155
```

Step 2: Configure core switch interfaces to connect to the inside of the Cisco ASA Server Room Firewall.

```
interface GigabitEthernet1/2/6
 description SR-ASA5540a
!
interface GigabitEthernet2/2/6
 description SR-ASA5540b
!
interface range GigabitEthernet1/2/6,GigabitEthernet2/2/6
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 154-155
 switchport mode trunk
```

Procedure 8 Add secure VLANs to server room switch

You must add the secure VLANs to the server room switch, and also define access or trunk ports to offer connectivity for servers that will connect to the secure VLANs.

Step 1: Add the secure VLANs to the core switch's VLAN database.

```
vlan 154-155
```

Step 2: Add the secure VLANs to the server room switch's EtherChannel trunks that connect to the core switch.

```
interface Port-channel1/2/6
 switchport trunk allowed add vlan 154-155
```

Procedure 9 Configure firewall EIGRP routing

The server room Cisco ASA unit will be the default router for the internal application server networks and will peer with the core network on the outside interface by using EIGRP for networks outside of the server room.

Step 1: Configure Cisco ASA to exchange EIGRP dynamic routing with the LAN core.

```
router eigrp 1
   network 10.10.0.0 255.255.0.0
   passive-interface default
   no passive-interface outside
```

Procedure 10 Configure security policy

For each server room VLAN, determine which security policy enables application requirements.

Each VLAN that requires a firewall will need either a permissive (blacklist) or restrictive (whitelist) security policy.

Option 1. Deploy a blacklist security policy

Network security requirements define the network security policies of any given organization. Use these examples only as a basis for implementing policies appropriate for your organization.

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

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. This traffic will be logged to maintain a record of management-traffic access.

Step 1: Enable network administrators to issue SNMP queries from management consoles.

```
object network Mgmt-host-range
 subnet 10.10.48.224 255.255.255.224
 description IP range for server-room management stations
object network Secure-Subnets
 subnet 10.10.54.0 255.255.254.0
access-list outside-access-in line 1 extended permit udp
object Mgmt-host-range object Secure-Subnets eq snmp
access-group outside-access-in in interface outside
```

Step 2: Block Telnet and SNMP access for the rest of the LAN. This traffic will also be logged to record attempts to access network management services.

```
object-group service Mgmt-traffic
  service-object tcp destination eq telnet
  service-object udp destination eq snmp
access-list outside-access-in line 2 extended deny object-
group Mgmt-traffic any object Secure-Subnets
```

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 line 3 extended permit ip any
object Secure-Subnets log disable
```

Tech Tip

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

Option 2. Deploy a whitelist security policy

Network security policy suits the requirements of a specific organization. Use these examples only as a basis for implementing policies appropriate for your organization.

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

Step 1: To control access so only specific hosts may be accessed, enter the following configuration. The policy limits access to addresses within the organization's network. Logging is enabled to allow application-access auditing.

```
object network Internal-Nets
  subnet 10.10.0.0 255.254.0.0
  description All HQ and Remote-Site Subnets
object network Secure-App-1
  host 10.10.54.26
object network Secure-App-2
  host 10.10.54.27
object-group network Secure-Servers-1
  network-object object Secure-App-1
  network-object object Secure-App-2
object-group service App-1-2-Services
  service-object tcp-udp destination eq domain
```

```
  service-object tcp destination eq http
  service-object tcp destination eq https
  service-object tcp destination eq netbios-ssn
  service-object udp destination eq nameserver
  service-object udp destination eq netbios-dgm
  service-object udp destination eq netbios-ns
access-list outside-access-in line 1 extended permit object-
group App-1-2-Services object Internal-Nets object-group
Secure-Servers-1
access-group outside-access-in in interface outside
```

Step 2: To allow IT management staff or network users access to certain resources, enter the following configuration. In this example, management hosts in the IP address range 10.10.48.224-255 are allowed SSH and SNMP access to server room subnets.

```
object network Mgmt-host-range
 subnet 10.10.48.224 255.255.255.224
 description IP range for server-room management stations
object-group service Mgmt-traffic
  service-object tcp destination eq ssh
  service-object udp destination eq snmp
access-list outside_access_in line 2 extended permit object-
group Mgmt-traffic object Mgmt-host-range object-group Secure-
Servers-1
```

Step 3: A bypass rule allows wide-open access to hosts that are added to the appropriate network object group. The bypass rule must be carefully defined to avoid opening access to hosts or services that must otherwise be blocked. In a whitelist policy, the bypass rule is typically only applied whenever firewall policy troubleshooting is required to allow access to an application. Traffic that matches the bypass rule should be logged:

- To collect evidence of application behavior; and,
- To provide a reminder in the firewall logs that the bypass rule is still applied, exposing hosts to wide-open access.

The following policy applies the bypass rule to one of the secure application servers defined above, and places the rule first in the policy list.

```
access-list outside_access_in line 1 extended permit ip object
Internal-Nets object Secure-App-2
```

Tech Tip

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

Step 4: Remove the bypass rule after troubleshooting activities have been completed.

```
no access-list outside_access_in line 1 extended permit ip
object Internal-Nets object Secure-App-2
```

Intrusion Prevention System Configuration

From a security standpoint, IDS and IPS are complementary to firewalls because firewalls are generally access-control devices and are built to block access to an application. In this way, you can use a firewall to remove access to a large number of application ports, reducing the threat to the servers. IDS and IPS sensors watch network and application traffic that is permitted to go through the firewall looking for attacks. If it detects an attack, the IDS sensor generates an alert to inform the organization about the activity. IPS is similar in that it generates alerts due to malicious activity, and it additionally applies action to block attacks.

Cisco offers IDS and IPS in several form factors and performance levels. IDS and IPS can be deployed:

- On its own as a standalone service with the Cisco 4200 series appliances
- Integrated into Cisco ASA with the SSM modules

Promiscuous versus Inline

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

An IDS sensor must use another inline enforcement device to stop malicious traffic. This means that for activity such as single-packet attacks (slammer worm over user datagram protocol), an IDS sensor could not prevent the

attack from occurring. However, an IDS sensor can offer great value when identifying and cleaning up infected hosts.

In an IPS deployment, because the packet flow is sent through the sensor and returned to the ASA, the sensor inspects the actual data packets.

The advantage IPS mode offers is that when the sensor detects malicious behavior, the sensor can simply drop it. This allows the IPS device a much greater capacity to actually prevent attacks.

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

Cisco recommends that you start with an IDS or promiscuous design for initial deployment and then move to IPS once the traffic and performance profile of the network is known and you are confident that no production traffic will be affected.

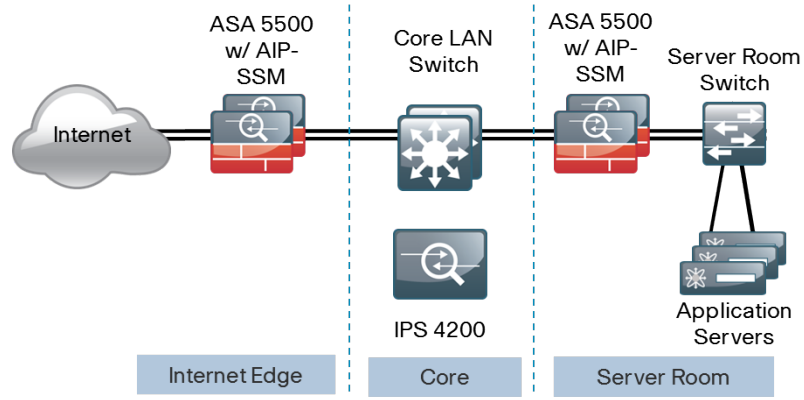
All of the IPS devices deployed in this design are in promiscuous mode. Visibility into what is going on inside a corporate network is a great advantage when following up on possible attack, auditing policy, or troubleshooting network and application problems; the value of IPS in promiscuous mode should not be overlooked.

IDS addresses use cases for each of the deployment scenarios:

- At the Internet edge, you deploy IDS with an AIP-SSM in the resilient Cisco ASA 5500 Firewall. This sensor provides these capabilities:
  - Inspects traffic from the Internet bearing threats directed at endpoints within the organization.
  - Inspects traffic from remote-access VPN users' endpoints that may have been compromised by malware.
- In the network's core, a Cisco IPS 4200 series sensor can look at traffic from specific VLANs. This sensor has the most flexibility. It can inspect traffic in many places:
  - Between wireless and the wired network
  - Between the LAN and WAN
  - From wired and wireless LAN hosts that are infected by malware and must be remediated
  - Specific VLANs that must be subjected to IDS scrutiny
- In the server room, you deploy IPS with an AIP-SSM in the Cisco ASA 5500 Firewall.
  - This sensor can inspect traffic from arbitrary end hosts to servers where the organization's critical data is held.
  - Tune the IDS's configuration to be application-specific for the services supplied by these servers, providing logging and mitigation of activity directed against critical data.

This design has IPS deployed at three key locations in the network.

Figure 16 - Key IPS deployment locations



Cisco IPS version 7.0 added a set of features that allow the system to make informed decisions on whether to permit or block traffic based on reputation. Cisco uses reputation in two key ways on the IPS:

- **Reputation filters**—A small list of IP addresses that have been hijacked or are owned by malicious groups.
- **Global Correlation Inspection**—A rating system for IP address based on prior behavior.

Reputation filters allow the IPS to block all traffic from known bad addresses before any significant inspection is done. Cisco Global Correlation uses the reputation of the attacker, in conjunction with the risk rating associated with the signature that fired, to come up with a new risk rating and drop traffic that is more likely to be malicious.

This process explains how to configure IPS and how to send network traffic to the sensor for inspection.

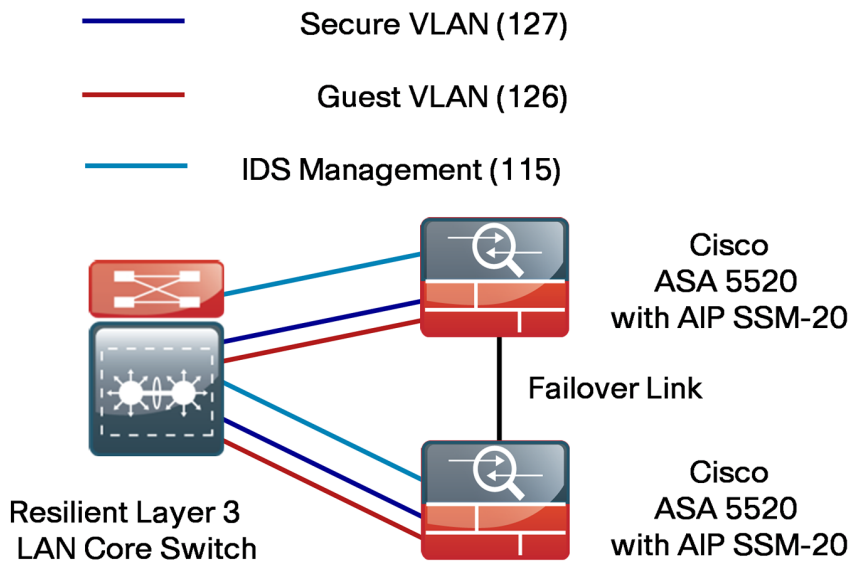
Process

Deploying Cisco Intrusion Prevention System

1. Configure LAN Switch Access Port
2. Applying Initial Configuration
3. Completing Basic Configuration
4. Configure signature updates (Optional)
5. Monitoring IDS activity

To configure Cisco IPS, you first complete the CLI-based configuration and then move to IPS Device Manager, the Cisco IPS GUI. Cisco IPS sensor appliances and modules always use an external management interface for configuration and monitoring, regardless where they are deployed on the network. The sensor's management port is connected to the management VLAN for the portion of the network where the sensor is installed, where the sensors will route to or directly reach the management station.

Figure 17 - Server-room firewall and IPS topology



You use the following values to configure the management interface:

Attribute	Internet Edge IDS	Core IDS	Server Room IDS
Hostname	ie-ids-a/b	hq-ids	sr-ids-a/b
IP Address	10.10.15.21&22	10.10.15.20	10.10.48.23&24
Network Mask	255.255.255.128	255.255.255.128	255.255.255.0
Default Gateway	10.10.15.1	10.10.15.1	10.10.48.1

Procedure 1 Configure LAN Switch Access Port

A LAN switch near the IPS sensor provides connectivity for the sensor's management interface.

Step 1: Configure an access port to the management VLAN on the appropriate switch where the IPS device's management port will be connected:

```
interface GigabitEthernet1/2/23
 switchport
 switchport access vlan 115
 switchport mode access
```

Procedure 2 Applying Initial Configuration

Use the sensor's CLI in order to set up basic networking information, specifically, the IP address, gateway address, and access lists that allow remote-access monitoring.

Step 1: Connect an Ethernet cable between the management port on the IPS device and the switchport that you configured in Procedure 1.

Step 2: Access the IDS sensor's CLI.

If the sensor is an AIP-SSM in a Cisco ASA, log on to Cisco ASA and open a session to the IPS SSM module.

```
ASA5520# session 1
Opening command session with slot 1.
Connected to slot 1. Escape character sequence is
'CTRL-^X'.
```

If the sensor is an IPS 4200-Series Appliance, open a CLI session on the sensor's console port.

Step 3: Log in to the IPS device. The default username and password are both cisco. You will be prompted to change the login password for the "cisco" user.

Step 4: At the IPS module's CLI, open the System Configuration Dialog.

```
sensor# setup
```

Step 5: The IPS module enters the interactive setup. Define the IPS module's host name:

```
--- 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]: ie-ids-a
```

Step 6: Define the IP address and gateway address for the IPS module's external management port.

```
Enter IP interface [192.168.1.62/24,192.168.1.250]:
10.10.15.21/25,10.10.15.1
```

Step 7: To control management access to the IPS module, define the access list. For the Midsize-2500 network, all addresses in the HQ subnet (10.10.0.0/16) will be allowed. Press Enter at a blank prompt to go to the next step.

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

Step 8: Accept the default answer (**no**) for the next three questions.

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

Note the following:

- Global Correlation will be disabled until later in the configuration process.
- An HTTP proxy server address will not be needed for a network that was configured according to this guide.
- You will configure time details in the sensor's GUI console.

Step 9: Accept the default answer (**off**) for the option to participate in the SensorBase Network.

```
Participation in the SensorBase Network allows Cisco to
collect aggregated statistics about traffic sent to your IPS.
SensorBase Network Participation level? [off]:
```

Step 10: The IPS SSP displays your configuration and a brief menu with four options. To save your configuration and exit the System Configuration Dialog, enter **2**.

```
The following configuration was entered.
[removed for brevity]
exit
[0] Go to the command prompt without saving this
configuration.
[1] Return to setup without saving this configuration.
[2] Save this configuration and exit setup.
[3] Continue to Advanced setup.
Enter your selection [3]: 2
Warning: DNS or HTTP proxy is required for global correlation
inspection and reputation filtering, but no DNS or proxy
servers are defined.
--- Configuration Saved ---
Complete the advanced setup using CLI or IDM.
To use IDM, point your web browser at https://<sensor-ip-
address>.
```

Step 11: Repeat steps 1-10 for the IPS sensor installed in the other Cisco ASA chassis. Be sure to use a different IP address on the other sensor's management interface. This process will not need to be repeated for the Core IDS sensor, because there is only one appliance.

Procedure 3 Completing Basic Configuration

Once the basic setup in the System Configuration Dialog is complete, you will use the startup wizard in the integrated management tool, Cisco Adaptive Security Device Manager/IPS Device Manager (ASDM/IDM) for Cisco ASAs, or Cisco IDM for IPS sensors appliances, to complete the remaining IDS configuration tasks:

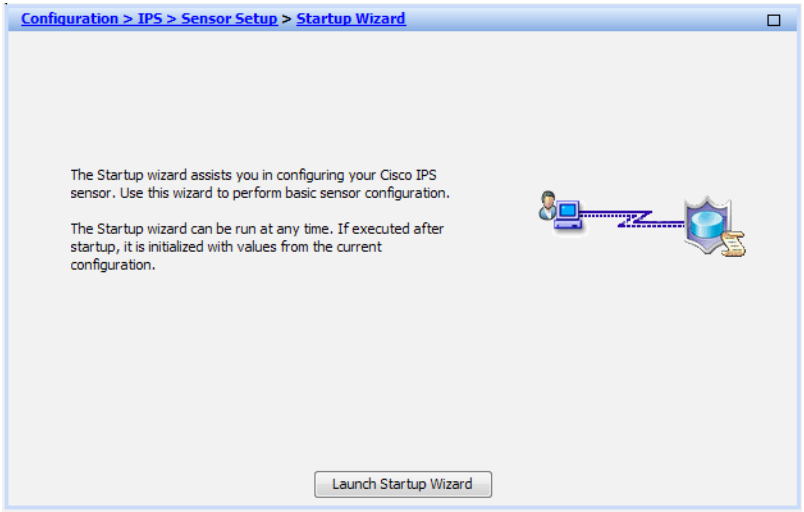
- Configure time settings
- Configure DNS and NTP servers
- Define a basic IDS configuration
- Configure Inspection Service Rule Policy
- Assign interfaces to virtual sensors

This procedure offers two options. Which you use depends on whether you will be configuring AIP-SSM modules installed in Cisco ASA appliances, or whether you will be configuring IPS Sensor appliances.

Option 1. Complete the basic configuration for AIP-SSM modules

Step 1: Open ASDM-IDM by browsing to an IP address on the Cisco ASA, which allows http management access. (for example: https://10.10.27.126/admin)

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



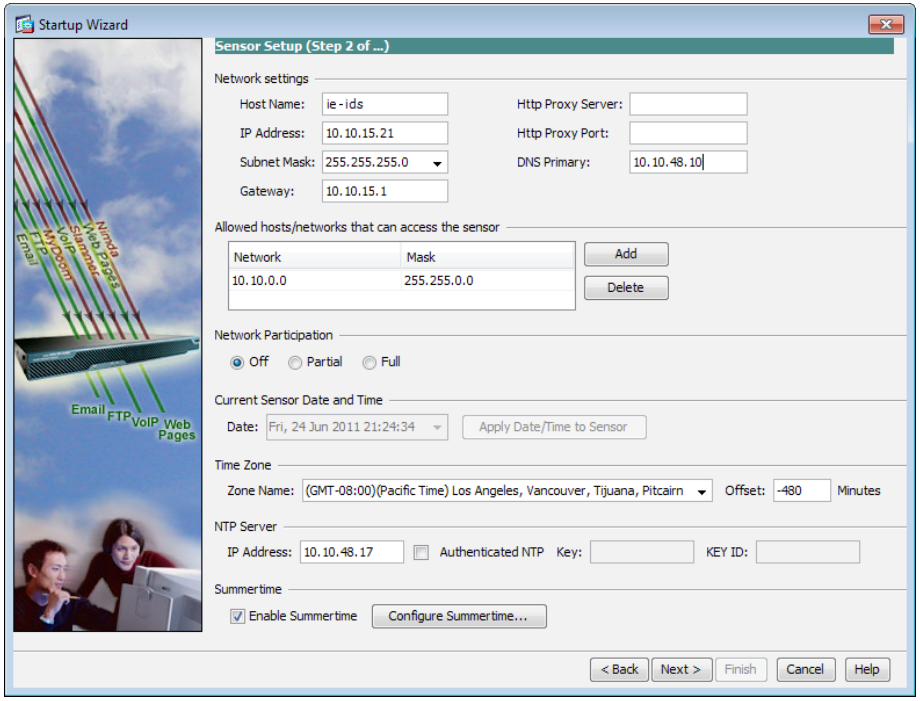
Step 3: Review the Startup Wizard Introduction, and then click **Next**.

Step 4: In Sensor Setup, configure the DNS server address, time zone, and NTP server address. If necessary for your time zone, select **Enable Summertime**.

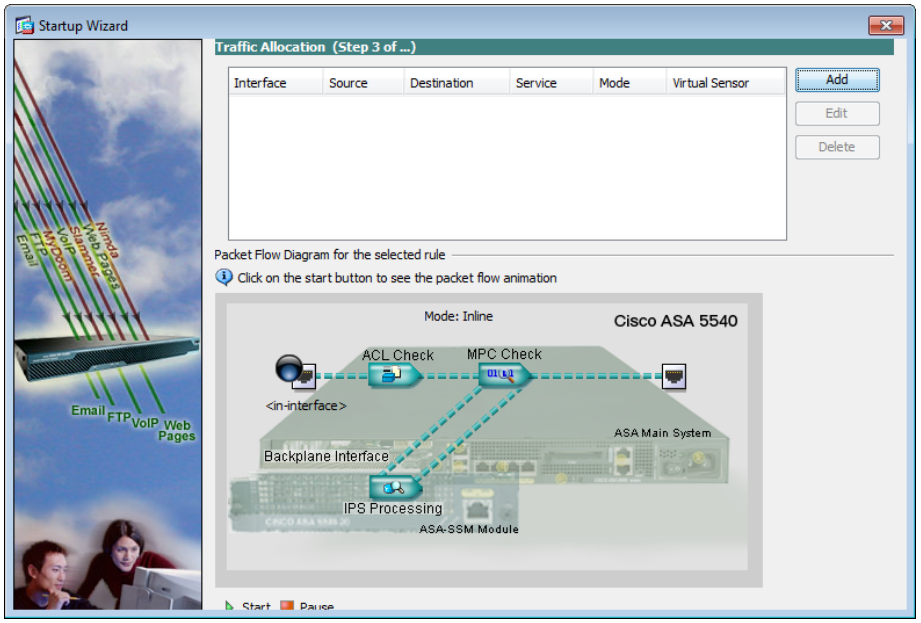
Step 5: Verify that **Authenticated NTP** is clear, and then click **Next**.

Tech Tip

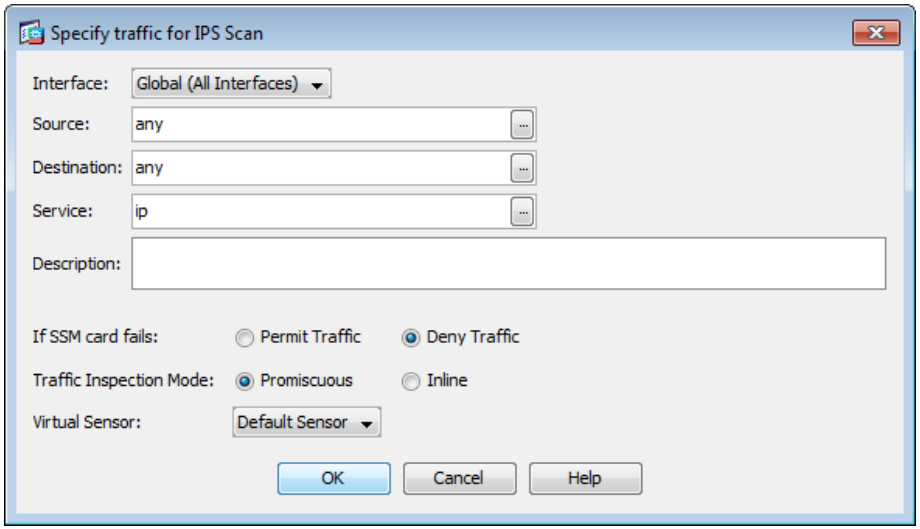
NTP is particularly important for security event correlation if you use a Security Event Information Manager to monitor security activity on your network.



Step 6: In the **Traffic Allocation** window, click **Add**.



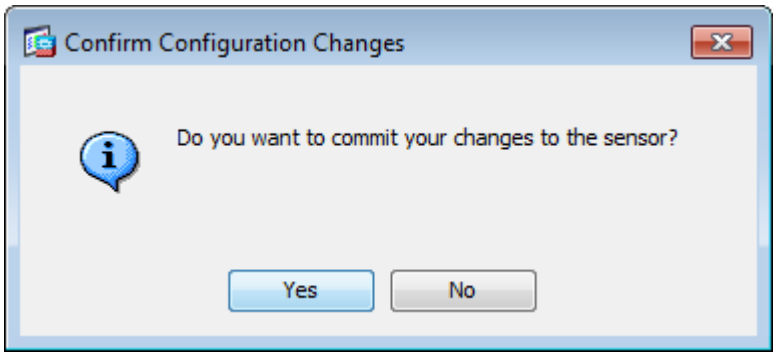
Step 7: In **Specify traffic for IPS Scan under Traffic Inspection Mode**, select **Promiscuous** and then click **OK** (if the ASA already had a default Traffic Allocation policy, IDM will throw a warning that "The Service Rule Policy you are trying to create already exists." You can cancel the window and proceed to Step 8 if you receive this warning).



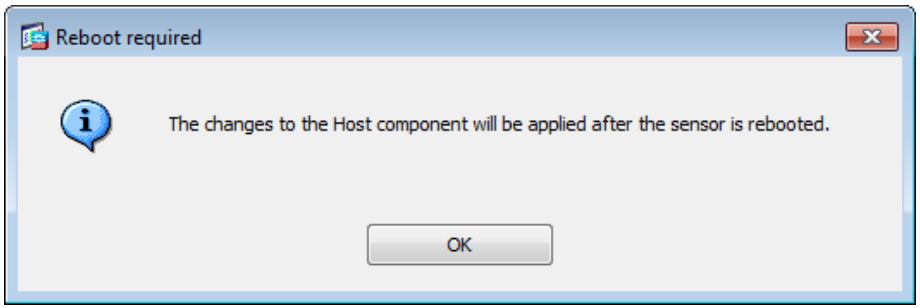
Step 8: Verify the Traffic Allocation Configuration. If you click **Start** below the **Packet Flow Diagram for the selected Rule** panel, the animation will illustrate a packet being copied to the IPS module and the egress interface. The animation may display a different platform that might be incorrect compared to the one that you are configuring.

Step 9: At the bottom of the Startup Wizard screen, click **Finish**.

Step 10: When you are prompted if you want to commit your changes to the sensor, click **Yes**.



Step 11: IDM applies your changes, and replies with a **Reboot required** message. Click **OK**.



If you are configuring the IDS modules in the Internet edge or the server room firewalls, repeat steps 1-10 for the IPS module installed in the other Cisco ASA chassis. There is no configuration synchronization between the two sensors.

Option 2. Complete the basic configuration for IPS 4240

Step 1: Configure Switched Port Analyzer on the core switch ports where the IDS sensor's monitoring port is connected. This text configures a monitor session so that interface GigabitEthernet 6/35 will monitor Port-Channel32, where the WAN router is connected

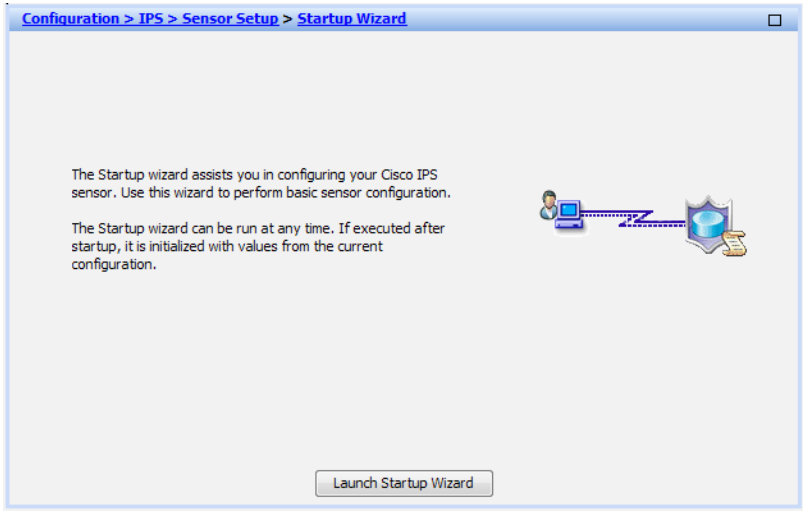
```
interface GigabitEthernet6/35
 description IPS4240 G0/0
 no switchport
 no ip address
 no shutdown
monitor session 1 source interface Port-Channel32
monitor session 1 destination interface GigabitEthernet6/35
```

Reader Tip

Port-Channel32 will be created in the WAN section of this guide. The WAN router's port-channel is described here for monitoring because traffic to and from the remote sites is likely one of the greatest network security threats.

Step 2: Launch IDM by browsing to the management IP address on the Cisco IPS sensor (for example: https://10.10.15.20/).

Step 3: Navigate to **Sensor Setup** > **Startup Wizard**, and click **Launch Startup Wizard**.



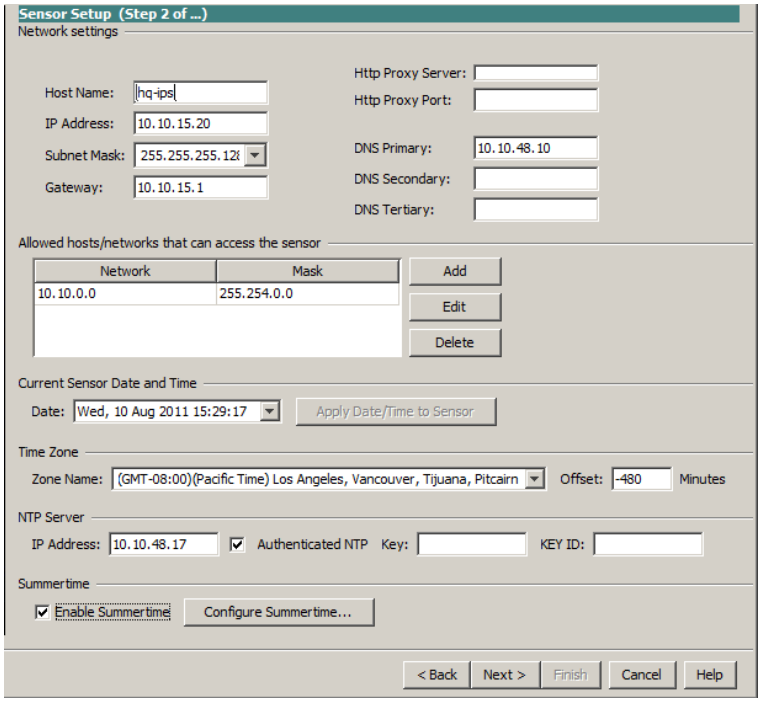
Step 4: Review the Startup Wizard Introduction, and then click **Next**.

Step 5: In **Sensor Setup**, configure the DNS server address, time zone, and NTP server address. If necessary for your time zone, select **Enable Summertime**.

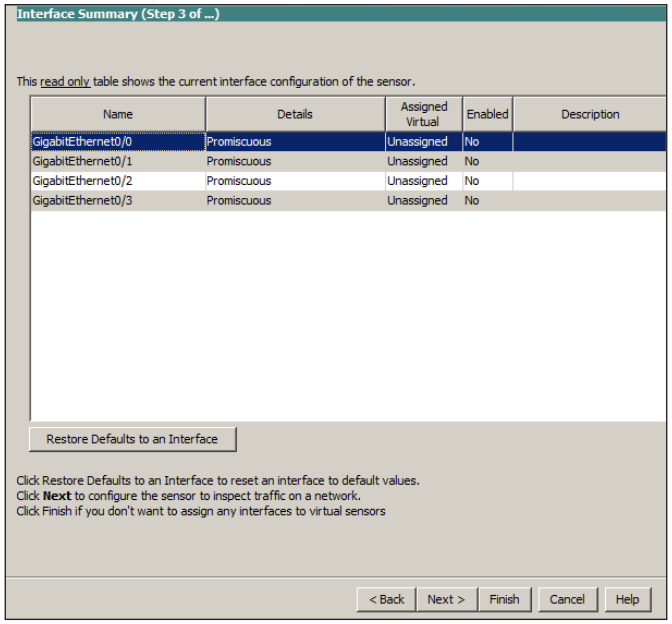
Step 6: Verify that the **Authenticated NTP** check box is clear, and then click **Next**.

Tech Tip

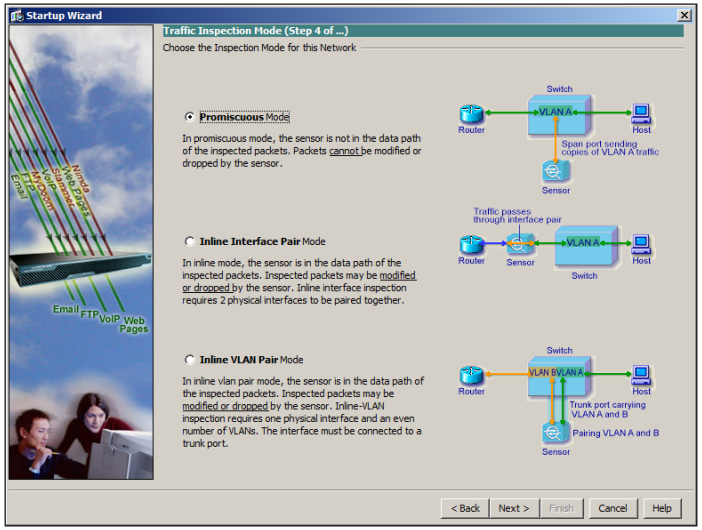
NTP is particularly important for security event correlation if you use a Security Event Information Manager to monitor security activity on your network.



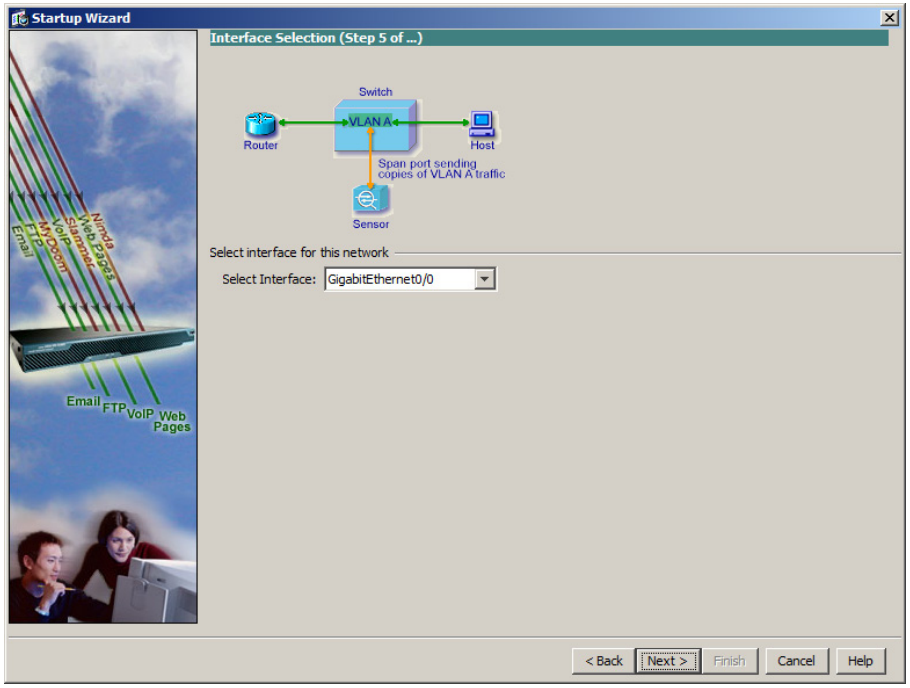
Step 7: On the **Interface Summary** page, click **Next.**



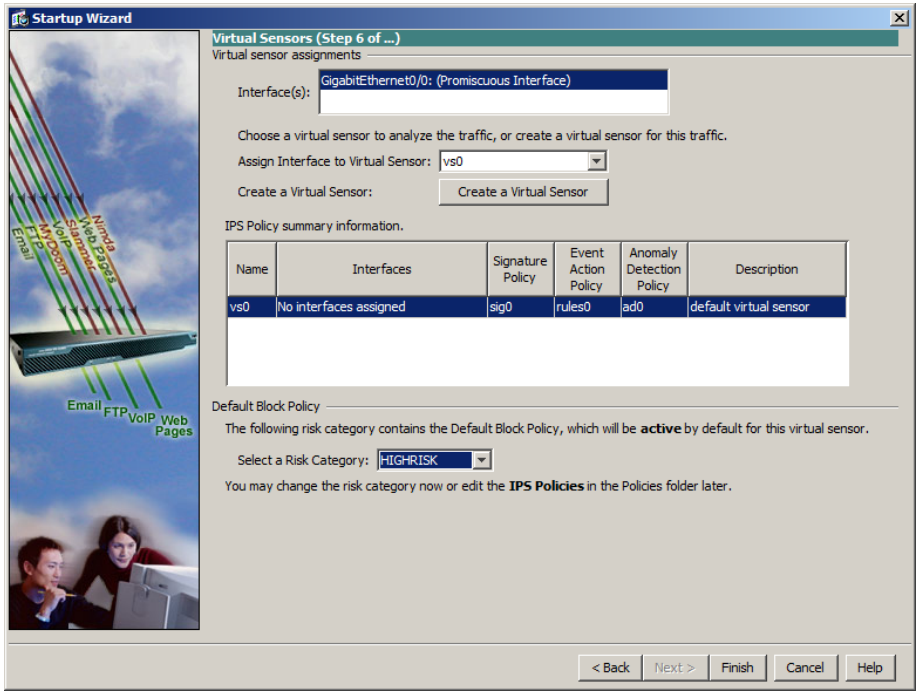
Step 8: On the Traffic Inspection Mode page, select **Promiscuous,** and then click **Next**.



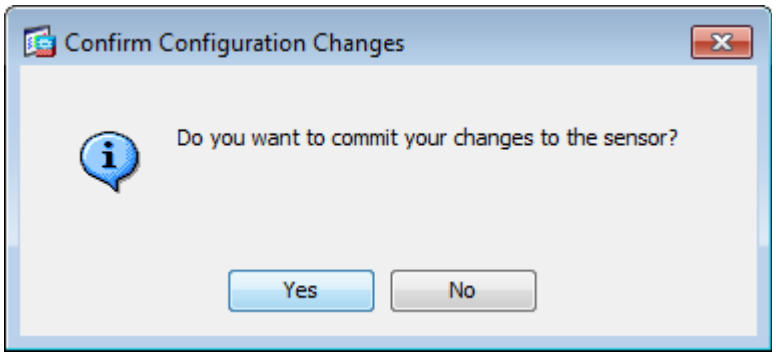
Step 9: On the Interface Selection page, in the **Select Interface** drop-down, select **GigabitEthernet0/0**.



Step 10: On the Virtual Sensors page, review the configuration, and then click **Next.**



Step 11: At the prompt that asks if you want to commit your changes, click **Yes**.



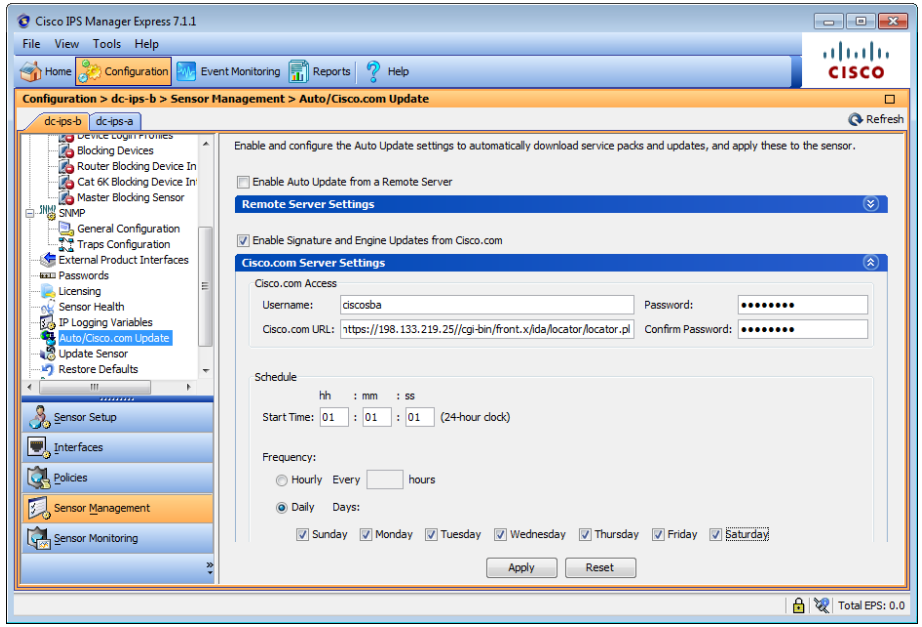
Reader Tip

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

Procedure 4 Configure signature updates (Optional)

IDS and IPS devices are generally only as good as their last update. As a result, it is important that you keep the sensors up-to-date. To this end, the easiest solution is to configure each sensor to retrieve signature updates directly from Cisco.com.

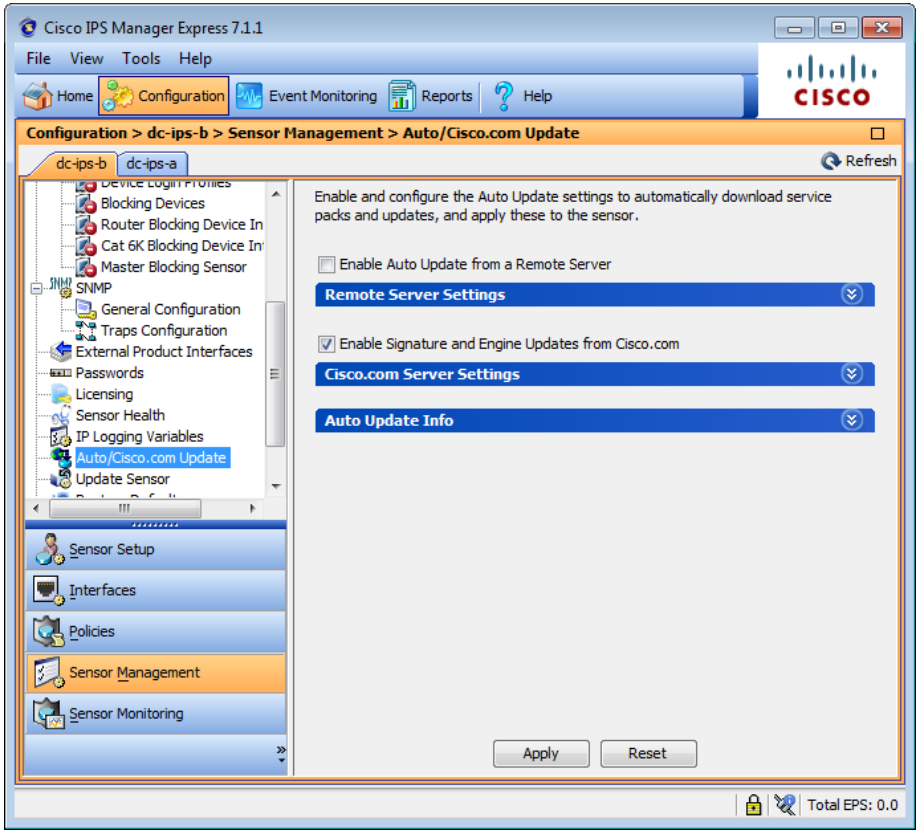
Step 1: To configure an IPS signature update in ASDM-IDM, open **IPS** > **Sensor Management** > **Auto/Cisco.com Update**. Select **Enable Signature and Engine Updates from Cisco.com**, and expand the **Cisco.com Server Settings** pane.



Tech Tip

Note that the update time is defined in Universal Coordinated Time (UTC).

Step 2: Provide a valid cisco.com username and password that holds entitlement to download IPS software updates. Select **Daily**, enter a time between 12:00 AM and 4:00 AM for the update **Start Time**, and then select every day.



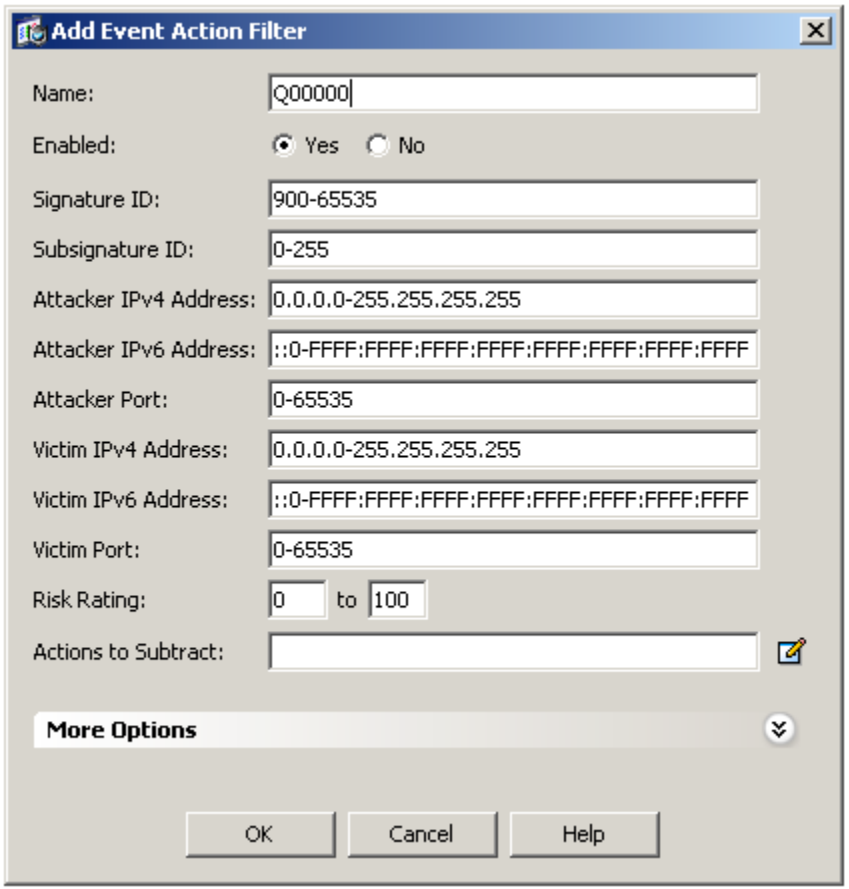
Tech Tip

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 by performing these steps.

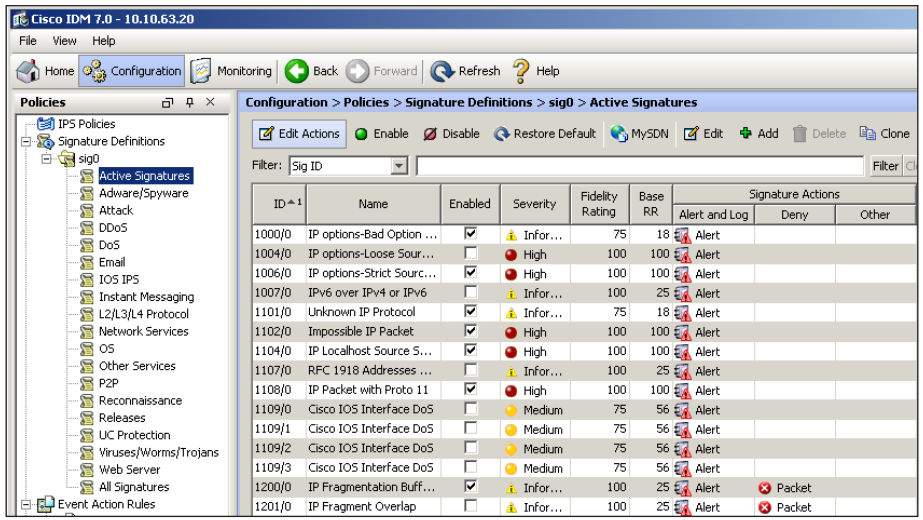
Procedure 5 Monitoring IDS activity

IDS and IPS tuning is a process, rather than a one-time event. IDM and IME both provide the capability to review the alarm events that the sensors report, and determine if the alarms are appropriate. If not, follow these steps to lessen their impact.

Step 1: In **Event Action Filters,** remove an action or alert due to a specific event.



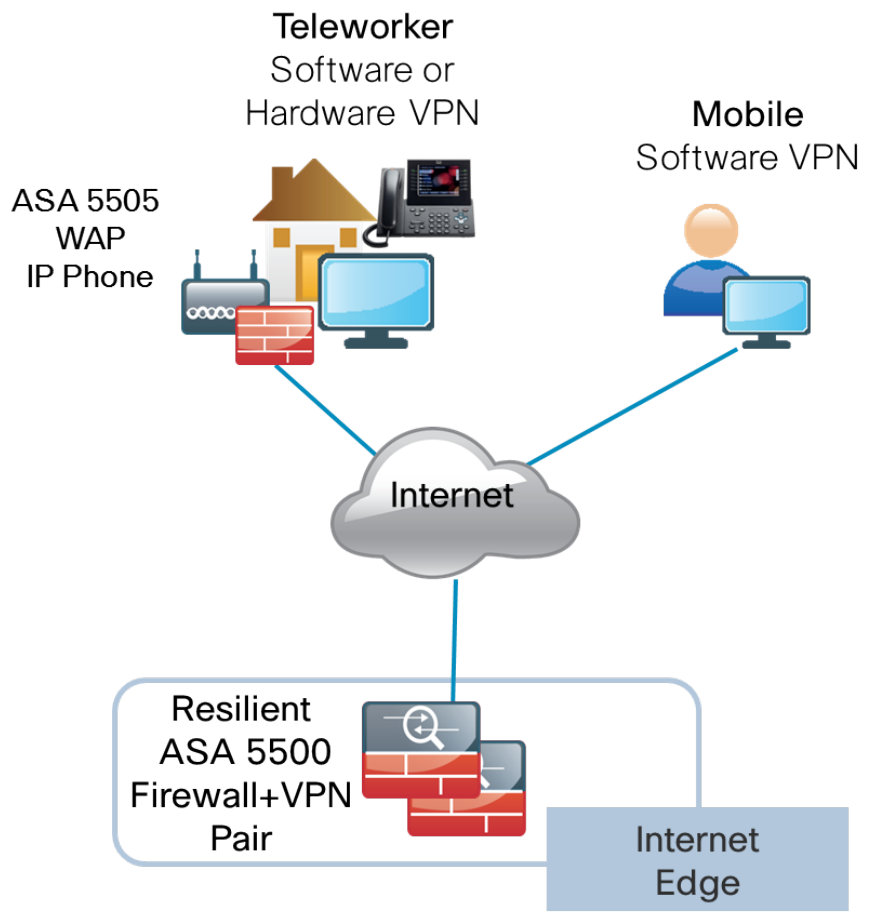
Step 2: Disable or retire a signature or remove an action from the signature-specific settings. This prevents the signature from triggering (retiring also prevents it from taking up resources, but it takes longer to bring it back online if needed later).



Remote-Access VPN

Cisco ASA supports SSL and IPsec client-based VPN remote access, as well as IPsec for hardware client or site-to-site VPN, and SSL web-portal-based clientless remote access. This section describes the basic configuration of remote-access SSL and IPsec VPNs for basic remote access.

Figure 18 - Remote-access VPN



For mobile workers or users that occasionally need remote connectivity, we recommend software clients such as the Cisco VPN Client and Cisco AnyConnect client. IPsec VPN requires the user to have client software already loaded and connectivity profiles configured on their machine to connect. IPsec VPN works best with corporate-owned machines such as laptops.

SSL VPN access uses the web browser-initiated Cisco AnyConnect client. SSL access is:

- More flexible than IPsec VPN.
- Likely to be accessible from more locations than IPsec because few companies block HTTPS access outside their networks.

Process

Configuring AnyConnect Client Remote-Access VPN

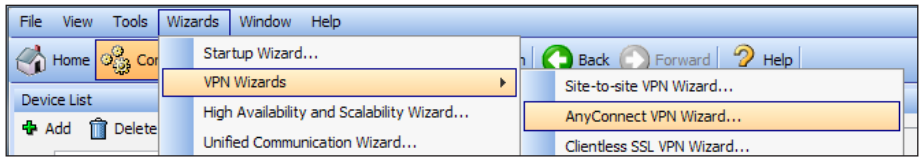
1. Run the AnyConnect VPN Wizard
2. Allow traffic between VPN clients
3. Configure the tunnel default gateway
4. Configure reverse route injection
5. Connect SSL VPN client

You configure Cisco ASA for AnyConnect VPN access by adding a baseline configuration to the default configuration on the appliance. Users authenticate to the local Windows domain controller.

Procedure 1 Run the AnyConnect VPN Wizard

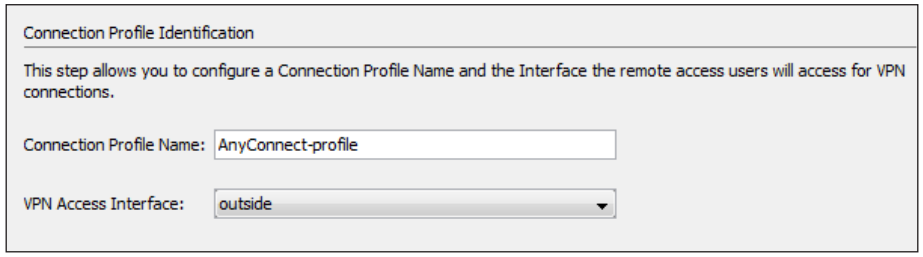
The majority of the VPN Configuration tasks are addressed in the AnyConnect VPN Wizard.

Step 1: In ASDM, start the AnyConnect VPN Wizard by browsing to **Wizards > VPN Wizards > AnyConnect VPN Wizard**.



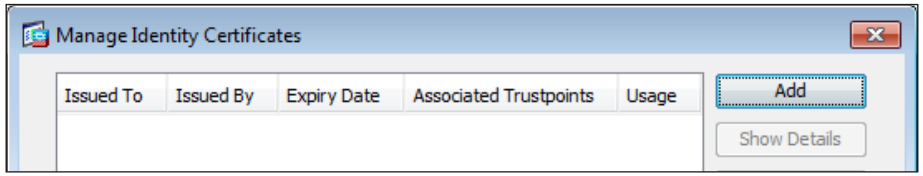
Step 2: On the **Introduction** page, review the text, and then click **Next.**

Step 3: In the **Connection Profile Identification** section, type **AnyConnect-profile** as the **Connection Profile Name**. Verify that the **VPN Access Interface** value is set to **outside,** and then click **Next.**

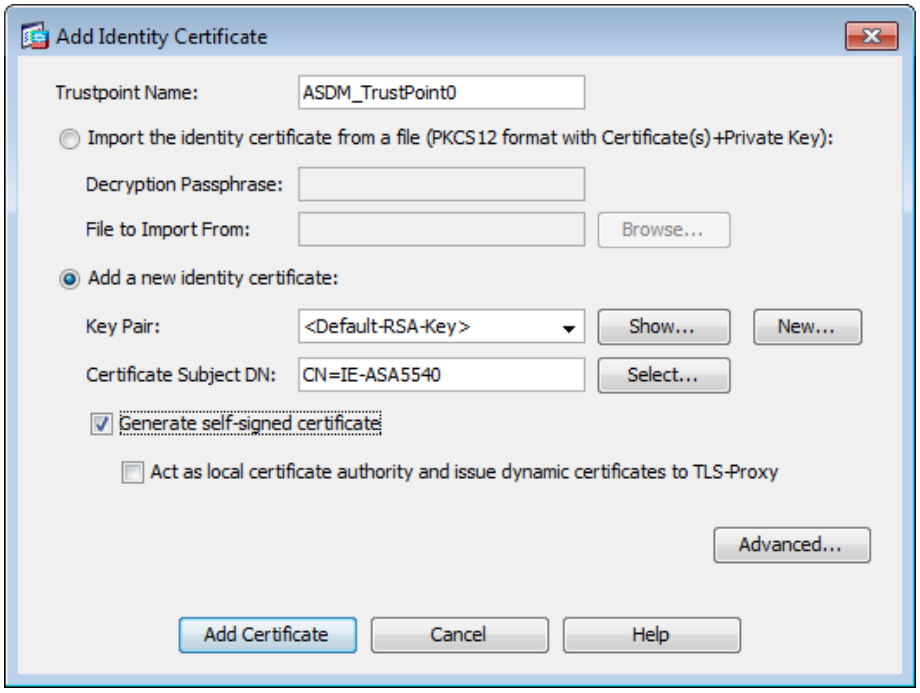


Step 4: On the **VPN Protocols** page, select the SSL and IPsec check boxes. Next to the **Device Certificate** field, click **Manage**.

Step 5: In the **Manage Identity Certificates** dialog box, click **Add**.



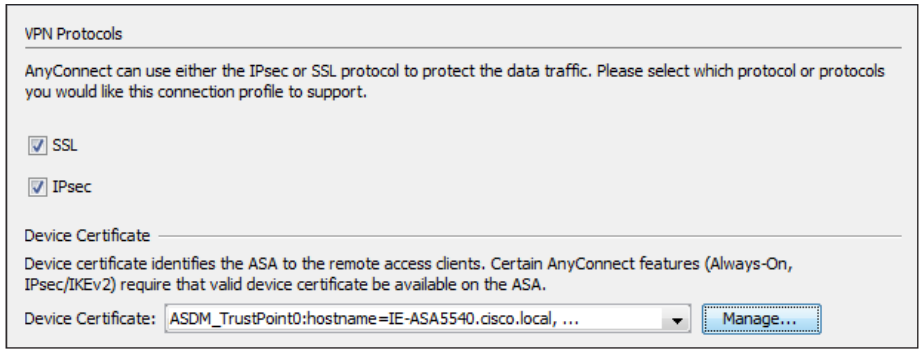
Step 6: In the **Add Identity Certificate** dialog box, select **Add new Identity Certificate**, click **Add a new identity certificate**, select the **Generate self-signed certificate check box**, and then click **Add Certificate**:



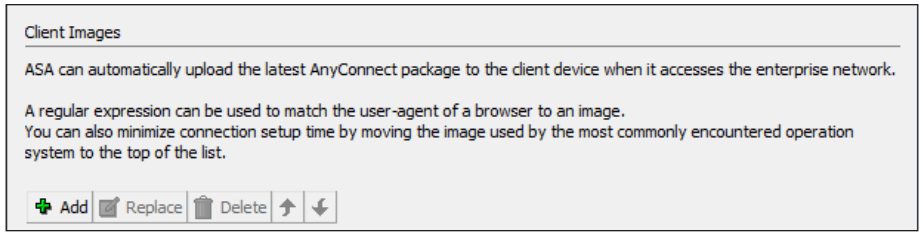
Executing this step will apply this configuration:

```
crypto ca trustpoint ASDM_TrustPoint0
  id-usage ssl-ipsec
  no fqdn
  subject-name CN=IE-ASA5540
  enrollment self
crypto ca enroll ASDM_TrustPoint0 noconfirm
```

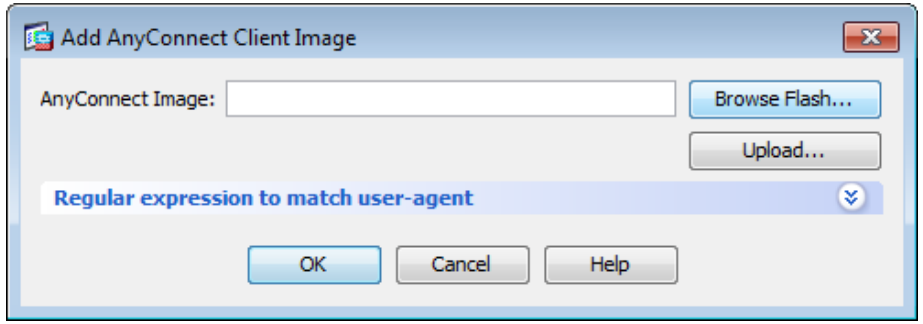
Step 7: On the **Manage Identity Certificates** page, click **OK**. In the **VPN Protocols** pane, verify that the certificate you created is reflected in the **Device Certificate** field, and then click **Next**.



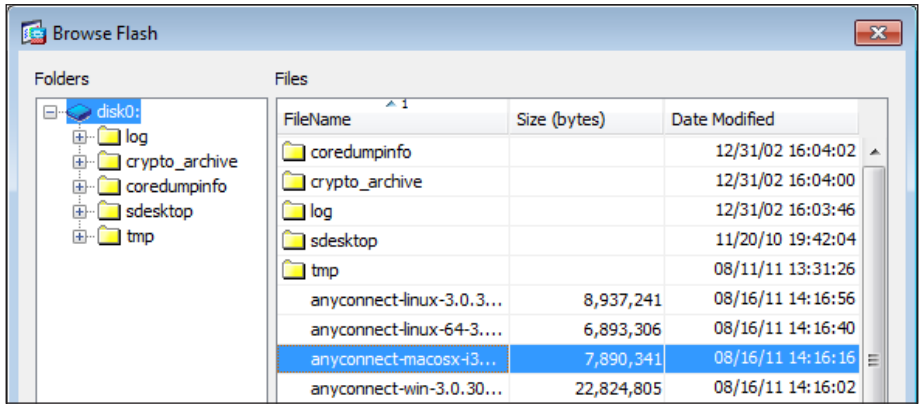
Step 8: In the **Client Images** pane, click **Add**.



Step 9: In the **Add AnyConnect Client Image** dialog box, click **Browse Flash**.



Step 10: In the **Browse Flash** dialog box, select the appropriate AnyConnect client image to support your user community, and then click **OK**.

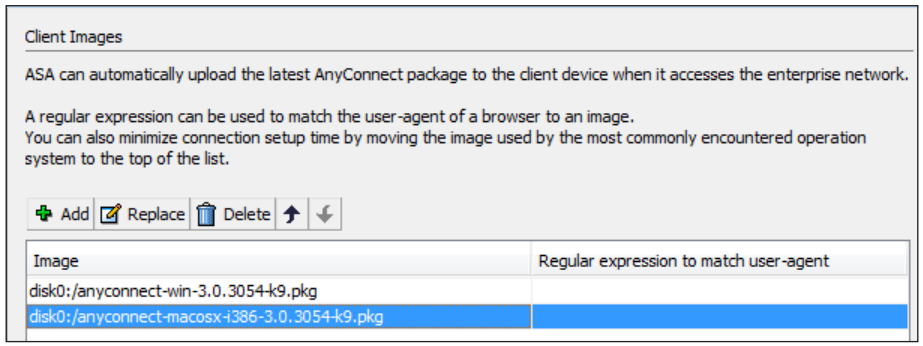


Tech Tip

If your ASA does not already have AnyConnect Client images loaded in the flash disk, you can use the **Upload** button in the **Add AnyConnect Client Image** to install new or updated client images into the ASA's flash disk.

Step 11: In the Add AnyConnect Client Image dialog box, click **OK**. If you must support multiple client platforms, repeat Step 8 through until you have added all required client support.

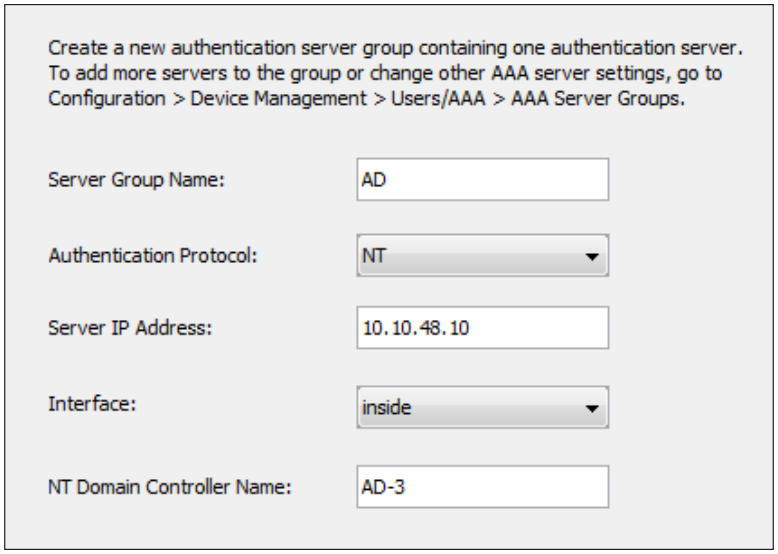
Step 12: In the Client Images pane, verify that all required client images are listed, and then click **Next**.



Step 13: On the **Authentication Methods** page, next to **AAA Server Group**, click **New**.

Step 14: In the **New Authentication Server Group** dialog box, enter the following values and then click **OK**:

- Server Group Name: AD
- Authentication Protocol: NT
- Server IP Address: 10.10.48.10
- Interface: inside
- NT Domain Controller Name: AD-3

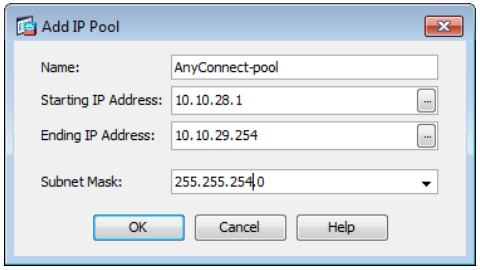


Step 15: On the **Authentication Methods** page, click **Next**.

Step 16: On the **Client Address Assignment** page, in the **IPv4 Address Pool** tab, click **New**.

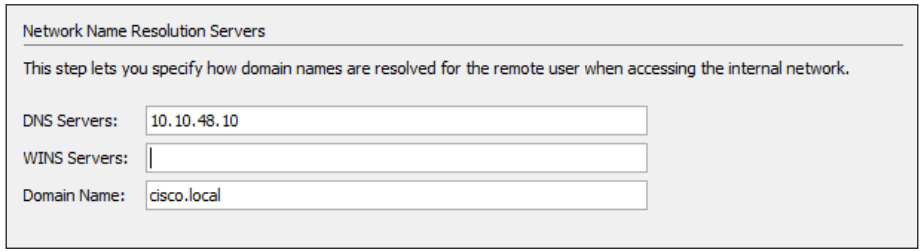
Step 17: In the **Add IP Pool** dialog box, enter the following values and then click **OK**:

- Name: **AnyConnect-pool**
- Starting IP Address: **10.10.28.1**
- Ending IP Address: **10.10.29.254**
- Subnet Mask: **255.255.254.0**



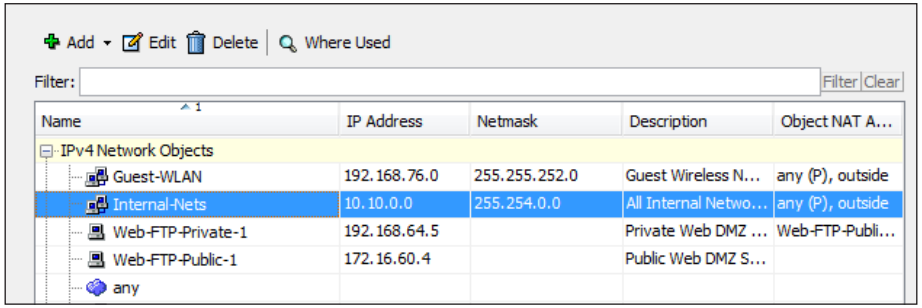
Step 18: On the **Client Address Assignment** page, verify that the pool you just created is selected, and then click **Next**.

Step 19: In the **Network Name Resolution Servers** pane, configure the appropriate values for your network:

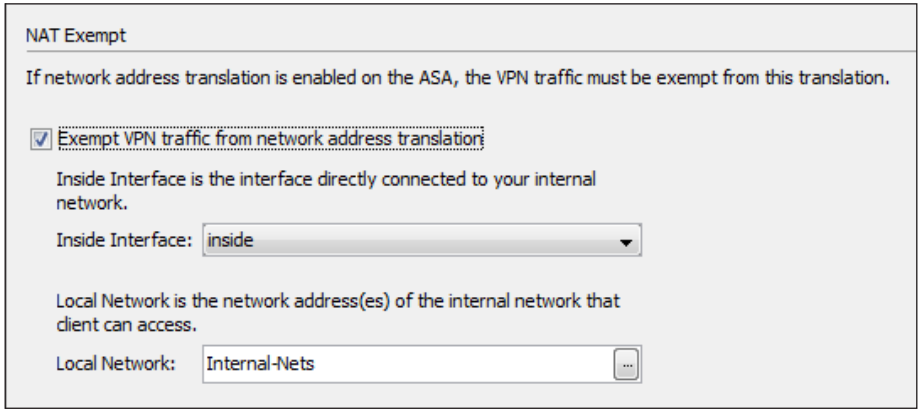


Step 20: In the **NAT Exempt** pane, select the **Exempt VPN Traffic from network address translation** check box. Select **inside** as the value for the inside interface, and click the ellipses (...) next to **Local Network**.

Step 21: In the **Browse Local Network** dialog box, select **Internal-Nets**, and then click **OK**:



Step 22: In the **NAT Exempt** pane, verify the configuration and then click **Next**.



Step 23: In the VPN Wizard's Step 9, verify that the **Allow Web Launch** check box is selected, and then click **Next**.

Step 24: Verify the configuration summary, and then click **Finish**.

Executing these configuration steps will apply the following CLI configuration:

```
webvpn
        enable outside
      object network NETWORK_OBJ_10.10.28.0_23
        subnet 10.10.28.0 255.255.254.0
      webvpn
        tunnel-group-list enable
        anyconnect image disk0:/anyconnect-win-3.0.3054-k9.pkg 1
        anyconnect image disk0:/anyconnect-macosx-i386-
3.0.3054-k9.pkg 2
        anyconnect enable
      ! write client profile "disk0:/AnyConnect-profile_client_
profile.xml" to ASA
      webvpn
        anyconnect profiles AnyConnect-profile_client_profile
disk0:/AnyConnect-profile_client_profile.xml
      exit
      aaa-server AD protocol nt
      aaa-server AD (inside) host 10.10.48.10
        timeout 5
        nt-auth-domain-controller AD-3
      exit
      ssl trust-point ASDM_TrustPoint0 outside
      ip local pool AnyConnect-pool 10.10.28.1-10.10.29.254 mask
255.255.254.0
      group-policy GroupPolicy_AnyConnect-profile internal
      group-policy GroupPolicy_AnyConnect-profile attributes
        vpn-tunnel-protocol ssl-client ikev2
        webvpn
          anyconnect profiles value AnyConnect-profile_client_
profile type user
      exit
      group-policy GroupPolicy_AnyConnect-profile attributes
        dns-server value 10.10.48.10
        wins-server none
        default-domain value cisco.local
exit
tunnel-group AnyConnect-profile type remote-access
tunnel-group AnyConnect-profile general-attributes
  default-group-policy GroupPolicy_AnyConnect-profile
  authentication-server-group  AD
  address-pool  AnyConnect-pool
tunnel-group AnyConnect-profile webvpn-attributes
  group-alias AnyConnect-profile enable
crypto ikev2 policy 1
  group 2 5
  encryption aes-256
crypto ikev2 policy 10
  group 2 5
  encryption aes-192
crypto ikev2 policy 20
  group 2 5
  encryption aes
crypto ikev2 policy 30
  group 2 5
crypto ikev2 policy 40
  group 2 5
  encryption des
crypto ikev2 enable outside client-services port 443
crypto ikev2 remote-access trustpoint ASDM_TrustPoint0
crypto ipsec ikev2 ipsec-proposal AES256
  protocol esp encryption aes-256
  protocol esp integrity sha-1 md5
crypto ipsec ikev2 ipsec-proposal AES192
  protocol esp encryption aes-192
  protocol esp integrity sha-1 md5
crypto ipsec ikev2 ipsec-proposal AES
  protocol esp encryption aes
  protocol esp integrity sha-1 md5
crypto ipsec ikev2 ipsec-proposal 3DES
  protocol esp encryption 3des
  protocol esp integrity sha-1 md5
crypto ipsec ikev2 ipsec-proposal DES
```

```
        protocol esp encryption des
        protocol esp integrity sha-1 md5
      crypto dynamic-map SYSTEM_DEFAULT_CRYPTO_MAP 65535 set
ikev2 ipsec-proposal  AES256 AES192 AES 3DES DES
      crypto map outside_map 65535 ipsec-isakmp dynamic SYSTEM_
DEFAULT_CRYPTO_MAP
      crypto map outside_map interface  outside
      nat (inside,outside) 1 source static Internal-Nets
Internal-Nets destination static NETWORK_OBJ_10.10.28.0_23
NETWORK_OBJ_10.10.28.0_23 no-proxy-arp route-lookup
```

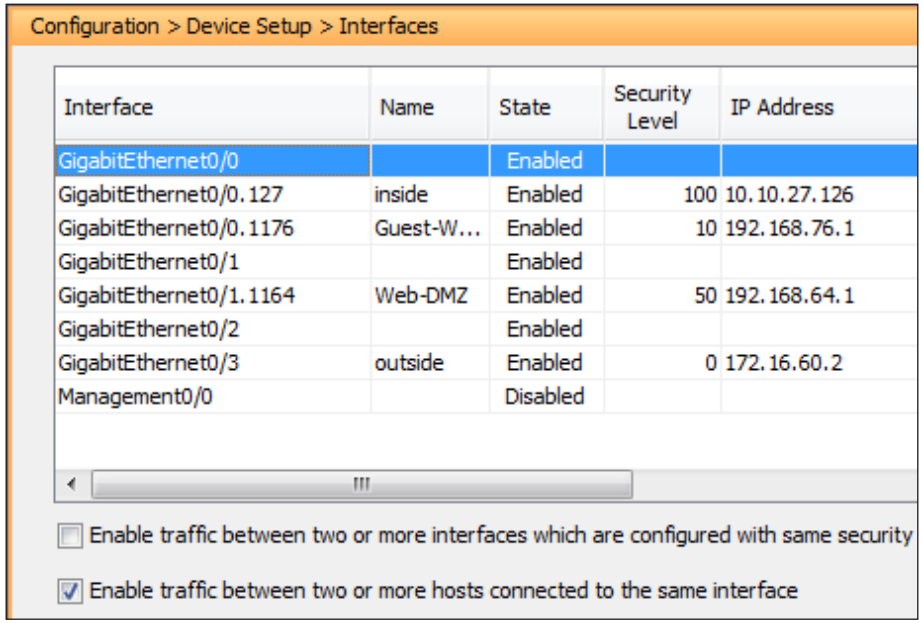
Tech Tip

If you apply this configuration directly to the ASA's CLI, you need to upload the appropriate AnyConnect client packages via ftp, tftp, or some other file-transfer mechanism.

Procedure 2 Allow traffic between VPN clients

Allow intra-interface traffic to allow VPN users (specifically remote workers with IP phones) to communicate with each other.

Step 1: Click **Configuration** > **Device Setup** > **Interfaces**, and select the **Enable traffic between two or more hosts connected to the same interface** check box, and then click **Apply**.



Executing these configuration steps will apply the following CLI configuration:

```
same-security-traffic permit intra-interface
```

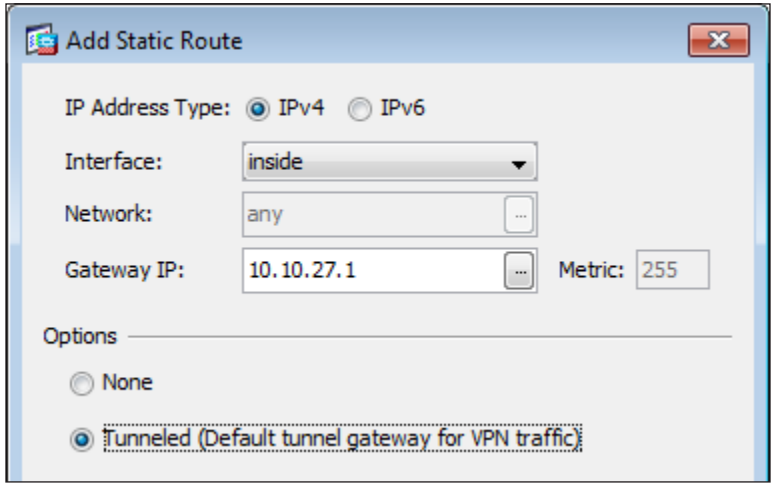
Procedure 3 Configure the tunnel default gateway

Remote-access VPN clients use a full-tunnel connection to carry all of their traffic to the HQ, so that traffic to and from the Internet can be inspected by firewall, IDS, and optional policy controls such as Cisco Web Security Appliance. Traffic to and from the Internet must be router toward a device on the private LAN, so that the ASA's policy engine is able to handle the traffic correctly. Configure the Tunnel Default Gateway route to forward all traffic that came from connected VPN users to the core switch.

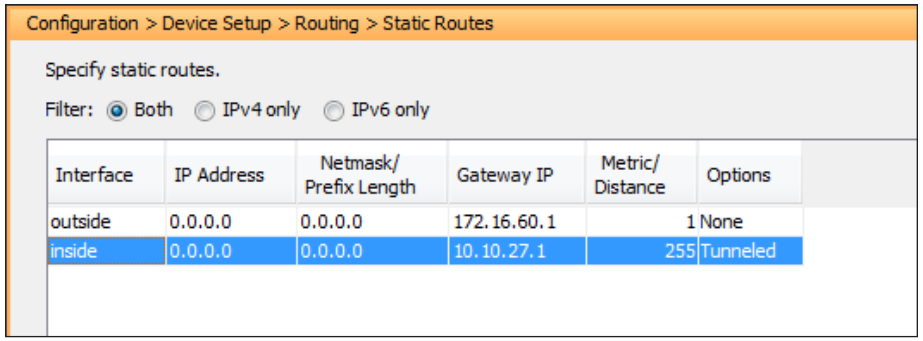
Step 1: Click **Configuration > Device Setup > Routing > Static Routes**, and then click **Add**.

Step 2: Configure the following values:

- Interface: **inside**
- Network: **0.0.0.0/0**, or click the ellipses (...) and click **Any.**
- Gateway IP: 10.10.27.1
- Options: Select **Tunneled (Default tunnel gateway for VPN traffic)**, and click **OK**.



Step 3: Verify the configuration, and then click **Apply**.



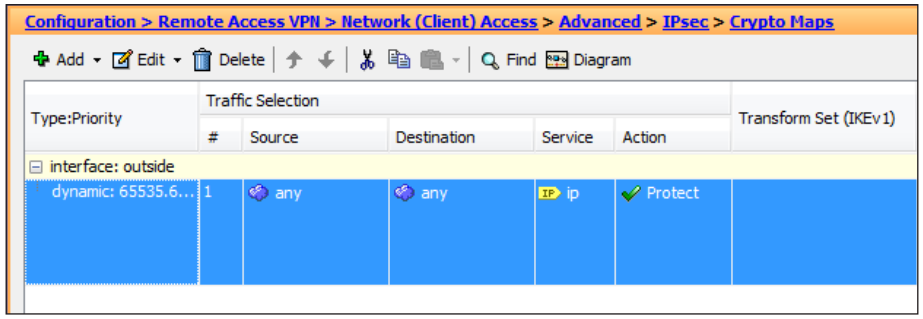
Executing these configuration steps will apply the following CLI configuration:

```
route inside 0.0.0.0 0.0.0.0 10.10.27.1 tunneled
```

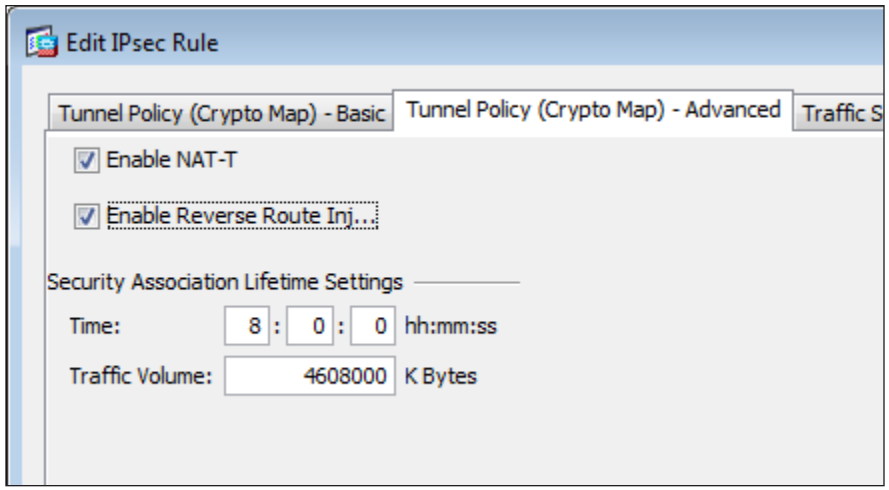
Procedure 4 Configure reverse route injection

This procedure put the initial configuration in place to support a growing network's need for a flexible routing environment. If the network only has one default route (usually via the integrated Internet edge appliance), connectivity to all VPN clients is found by following the route of last resort. As a network grows to the point that additional default routes may be available, which are selected by metric and advertised by dynamic routing, default-route-based route selection to reach VPN clients may not offer a viable option. This procedure ensures that VPN clients and teleworker subnets will be reachable throughout the organization's network by advertising the remote workers' addresses through EIGRP.

Step 1: Click **Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPsec > Crypto Maps**. Select the default dynamic crypto policy on the outside interface, and then click **Edit**.



Step 2: In the **Edit IPsec Rule** dialog box, click the **Tunnel Policy (Crypto Map) – Advanced** tab, select the **Enable Reverse Route Injection** check box, click **OK**, and then click **Apply**.



Executing these configuration steps will apply the following CLI configuration:

```
crypto dynamic-map SYSTEM_DEFAULT_CRYPTO_MAP 65535 set
reverse-route
```

Procedure 5 Connect SSL VPN client

Step 1: For SSL VPN access, open a web browser and browse to the IP address or DNS name of the VPN headend. When the login prompt appears, enter an appropriate username and password that is allowed to access the network with the Cisco AnyConnect client.

Wide-Area Network Module

Business Overview

Depending on their needs, many organizations require remote sites (outside of their headquarters) to be effective. Whether it is a restaurant chain needing to be close to the people it serves, a freight service requiring regional delivery depots, or an education organization with schools distributed about a geography, these and many other types of organizations need a dispersed work force.

One challenge of a dispersed workforce is providing the users at the remote sites access to information and applications housed at the organization's headquarters. Even if the application servers or some of the data is dispersed, they are typically backed up to central locations for efficiency and the data merged for all to use. This means that the organizations require a network to connect together these sites spread over a wide area. Depending on the ability of the remote site to function without connectivity to the central site, the remote site may require varying levels of availability of network equipment and transport.

Another challenge of managing the IT needs of a dispersed organization is providing connectivity that satisfies the application performance when running over a WAN. To maximize worker productivity and effectiveness, a user at a remote site should be able to realize the same application performance and functionality as a user at the headquarters. Lengthy waits or timeouts can cause customer dissatisfaction and result in loss of business.

The WAN's hardware and topology must not impose a restriction against growth and expansion requirements. A WAN design must incorporate sufficient flexibility to enable geographic growth of the WAN, offering scalable connectivity for additional remote sites in a given service area and supporting a hierarchical connectivity model to accommodate the organization's expansion to new regions.

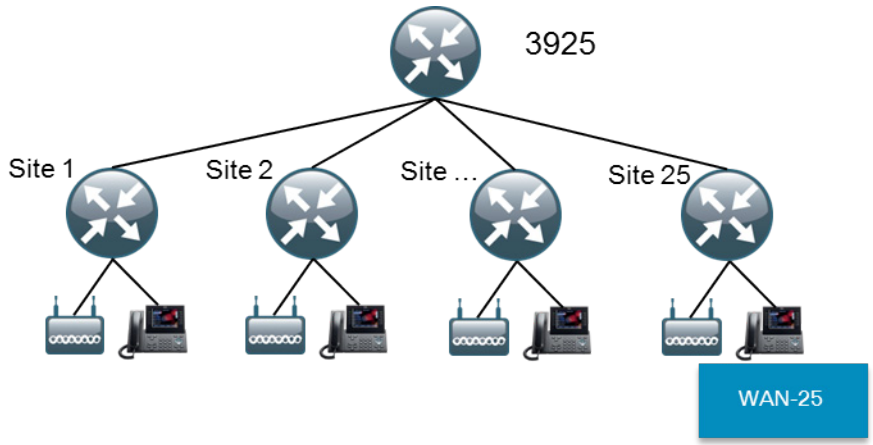
The nature of a WAN is that the farther it must reach and the more complex it is, the more susceptible it is to failure. The challenge to the organization is to balance the cost of bandwidth, equipment, and resiliency with the cost of lost productivity and business should an outage occur.

Technical Overview

The WAN aggregation is the point of connection between the headquarters and the remote sites. The WAN design is based on private line connectivity provided by a service provider. Due to the breadth of WAN service offerings and multitude of possible hardware and software configurations, this deployment guide covers a generic example for an Ethernet-connected Layer 3 Multiprotocol Label Switching (MPLS) WAN service. This guide provides deployment examples that can be used at the headquarters and remote-site WAN interfaces. The WAN interconnects all locations and aggregates traffic for the Internet at the headquarters. The WAN design offers guidance for two size ranges:

- WAN-25 accommodates headquarters WAN connectivity for around 25 remote sites (using a Cisco 3925 ISR G2)

Figure 19 - WAN-25 remote-site aggregation



- WAN-75 supports a larger WAN with up to 75 sites aggregated in one location

The WAN routers selection criteria includes more than the primary function of routing packets between locations; to be flexible enough to provide a long service period, the router may need to support several additional functions:

- Voice media and gateway services for IP telephony
- Application optimization services
- Security functions through the capabilities provided by integrated software features or hardware service modules
- Additional connectivity or resilience options through integrated, hardware-accelerated VPN support

The Cisco 3945 and Cisco 3925 Integrated Services Routers Generation 2 (ISR G2) are the recommended options for the headquarters WAN router to provide the routing capacity to support twenty remote sites, each with T1/E1 connectivity speeds or below.

- The Cisco 3945 and 3925 ISR are flexible, modular platforms that enable high-speed routing and other services—such as voice—for connectivity needs between the headquarters and remote sites.
- The Cisco 3945 and 3925 offer future-proofing and investment protection. These routers support an upgradable motherboard if higher performance is required in the future; they also support the T3/E3 network module for high-speed WAN connectivity.
- The router at the main site can also provide Unified Communications media resources and gateway functions.

The remote-site design supports up to 25 users with computers, IP phones, and wireless. The computers will access desktop applications, email, and other company applications over the WAN; these applications are served from the headquarters' server room, The IP phone system is also supported through the WAN.

The Cisco ISR G2 family routers, 881, 2911, 2921, and 2951 are the platforms that meet the requirements for connecting the remote site via the WAN back to the headquarters:

- The selected platforms provide the processing power necessary to support a T1/E1 of bandwidth and have the ability to grow.
- All four platforms provide integrated services with voice gateway capability for local connectivity to the PSTN.
- Cisco ISR G2 2900-series routers provide wide-area application services SRE for optimization of data, voice, and video over the WAN.

Remote-site router platform selection is based on the greater of the following parameters:

Table 3 - Remote-site WAN router selection parameters

Suggested Platform	Users at Remote Site	WAN Bandwidth
Cisco 881	5	Up to 3 Mbps
Cisco 2911	15	Up to 10 Mbps
Cisco 2921	25	Up to 20 Mbps
Cisco 2951	40	Up to 45 Mbps

Deployment Details

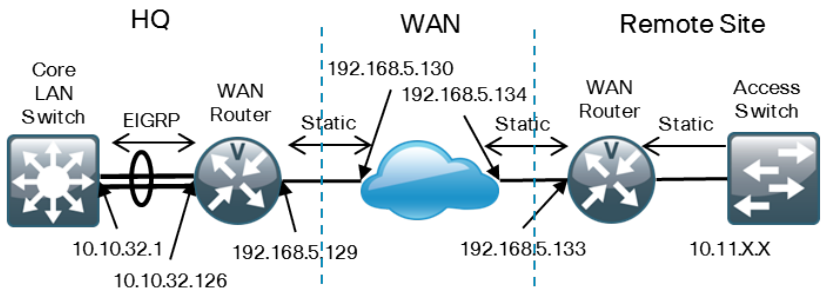
Remote-site configuration consists of several processes:

- Provide headquarters WAN aggregation
- Configure remote-site routing
- Configure remote-site LAN access switch
- Set up headquarters-to-regional site connection

Headquarters WAN Router

This process describes the configuration processes for the headquarters WAN routers.

Figure 20 - Example of remote-site WAN routing topology and configuration values



Reader Tip

Any specific interfaces and IP addresses are examples based on the Cisco lab used to validate this guide. Your interfaces and IP addresses may differ.

Process

Configuring the Headquarters WAN Router

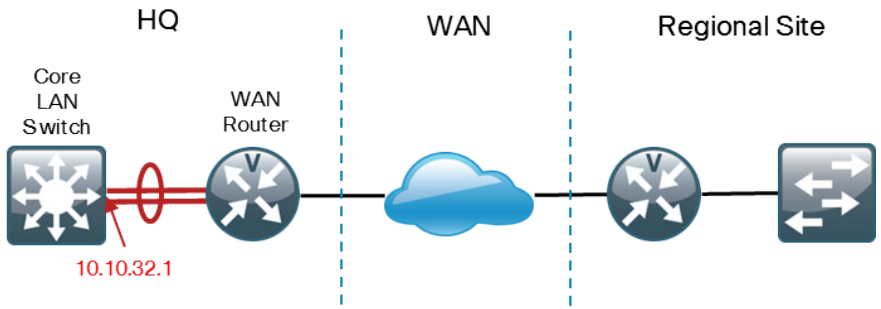
1. Configure headquarters core switch
2. Apply WAN router basic configuration
3. Configure headquarters WAN QoS
4. Configure headquarters router LAN uplink
5. Configure headquarters router WAN link
6. Configure WAN router static routing
7. Configure headquarters WAN router EIGRP

Complete each of the following procedures to configure the headquarters/ regional site WAN.

Procedure 1 Configure headquarters core switch

The headquarters WAN router is connected to the core switches by two Gigabit Ethernet interfaces in an EtherChannel for high availability. Each of the interfaces in the EtherChannel is connected to a different switch or blade in the core stack or modular switch.

Figure 21 - EtherChannel downlink on core switch



Step 1: On the headquarters core switch, create a VLAN.

```
vlan 132
  name core-wan
```

Step 2: Assign interfaces to the EtherChannel port-group.

```
interface range GigabitEthernet1/2/23,GigabitEthernet2/2/23
  description Etherchannel to WAN Router
  switchport
  channel-group 32 mode on
```

Step 3: Define a port-channel interface with a number matching the channel-group on the physical interfaces.

```
interface Port-channel32
  description WAN Router
  switchport
  switchport access vlan 132
  switchport mode access
  spanning-tree portfast edge
  no shutdown
```

Tech Tip

4507 and 3750X core switches only require the **spanning-tree portfast** command.

Step 4: Set up the VLAN's SVI and assign its IP address.

```
interface Vlan132
  ip address 10.10.32.1 255.255.255.128
  ip pim sparse-mode
  no shutdown
```

Step 5: Enable EIGRP peering on the VLAN where the WAN router will be connected.

```
router eigrp 1
  no passive-interface Vlan132
```

Procedure 2 Apply WAN router basic configuration

The headquarters WAN router requires basic global configuration to enable infrastructural requirements such as management access and network time configuration. WAN routers are configured to use a loopback interface to originate some of their management-plane traffic to ensure a consistent source address, in spite of other interfaces' state and the direction that traffic will be sent to the network. WAN routers must be configured to participate in the network's multicast environment so remote sites will have access to content that is distributed by multicast from the headquarters site.

Step 1: Apply configuration described in the Global Configuration Module section earlier in this guide.

Step 2: Define the headquarters WAN router's loopback interface, and apply the IP address.

```
interface Loopback0
  ip address 10.10.32.254 255.255.255.255
  ip pim sparse-mode
```

Step 3: Configure management-plane services to use the loopback interface.

```
ip ssh source-interface Loopback0
snmp-server trap-source Loopback0
ntp source Loopback
```

Step 4: Enable IP Multicast routing.

```
ip multicast-routing
```

Step 5: Define IP Multicast RP and multicast subnet.

```
ip pim rp-address 10.10.15.252 10
ip pim register-source Loopback0
access-list 10 permit 239.1.0.0 0.0.255.255
```

Step 6: Enable IP Multicast routing on the loopback interface.

```
interface Loopback0
  ip pim sparse-mode
```

Procedure 3 Configure headquarters WAN QoS

WAN routers are configured to apply queuing and shaping on traffic to the WAN to ensure that critical and delay-sensitive traffic has the best chance of delivery as it makes the transition from Gigabit connectivity on the LAN to megabit (or less) line speeds available in the WAN.

The policy-map configuration includes a statement of the WAN link's bandwidth, so the interface's output shaper can set bandwidth allocations for various traffic classes. The "shape average" value is determined by the line rate of the WAN circuit, as in the examples in the following table.

Table 4 - QoS shape average values for various WAN line rates

Line speed	Shape-average value
384 Kbps	384k
T1: 1.44 Mbps	1440k
E1: 1.5 Mbps	1500k
10 Mbps	10m

This configuration will be applied on headquarters and regional site WAN routers, as well as remote-site WAN routers.

Step 1: Apply configuration to define the QoS classifiers.

```
class-map match-any DATA
  match ip dscp af21
class-map match-any INTERACTIVE-VIDEO
  match dscp cs4 af41
class-map match-any CRITICAL-DATA
  match dscp cs3 af31
class-map match-any VOICE
 match dscp ef
class-map match-any SCAVENGER
  match ip dscp cs1 af11
class-map match-any NETWORK-CRITICAL
  match ip dscp cs2 cs6
```

Step 2: Define a policy-map describing the bandwidth allocations that will be permitted for the various classes.

```
policy-map WAN
  class VOICE
    priority percent 10
  class INTERACTIVE-VIDEO
    priority percent 23
  class CRITICAL-DATA
    bandwidth percent 15
      random-detect dscp-based
  class DATA
    bandwidth percent 19
      random-detect dscp-based
  class SCAVENGER
    bandwidth percent 5
  class NETWORK-CRITICAL
    bandwidth percent 3
  class class-default
    bandwidth percent 25
      random-detect
```

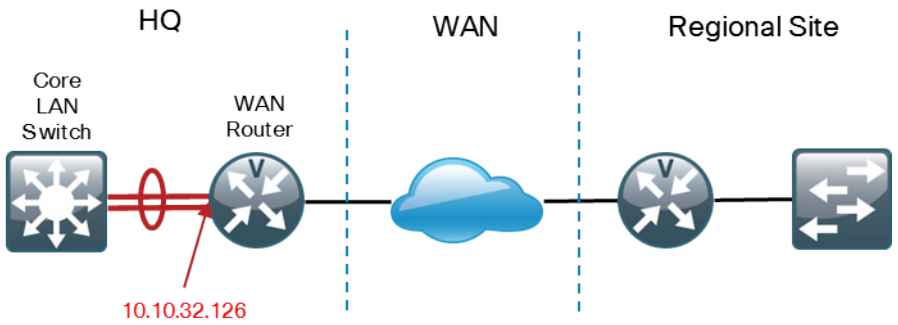
Step 3: Combine the bandwidth-allocation policy-map with the WAN link's line-rate in the policy-map that will be assigned to WAN interfaces.

```
policy-map WAN-QOS-POLICY
  class class-default
    shape average 10m
   service-policy WAN
```

Procedure 4 Configure headquarters router LAN uplink

The headquarters router is connected to the core switches, and both Gigabit Ethernet interfaces use EtherChannel for high availability. Each of the interfaces in the EtherChannel is connected to a different switch or blade in the core stack or modular switch.

Figure 22 - Headquarters WAN router EtherChannel uplink to core



Step 1: Set up the headquarters WAN router's EtherChannel interface for connection to the core, and define the IP address.

```
interface Port-channel1
  ip address 10.10.32.126 255.255.255.128
  ip pim sparse-mode
```

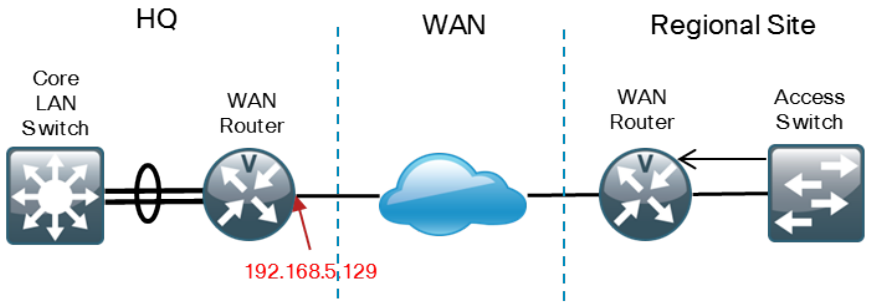
Step 2: Assign physical interfaces to the EtherChannel.

```
interface GigabitEthernet0/1
  no ip address
  channel-group 1
  no shutdown
!
interface GigabitEthernet0/2
  no ip address
  channel-group 1
  no shutdown
```

Procedure 5 Configure headquarters router WAN link

The headquarters WAN router is configured to connect to an Ethernet MPLS WAN connection.

Figure 23 - Headquarters WAN router WAN interface



Step 1: Configure the IP address on the router's Ethernet WAN interface.

```
interface GigabitEthernet0/0
  description MPLS WAN Uplink
  ip address 192.168.5.129 255.255.255.252
  ip pim sparse-mode
  no shutdown
```

Step 2: Apply the WAN QoS queuing and shaping policy from the QoS procedure to the interface.

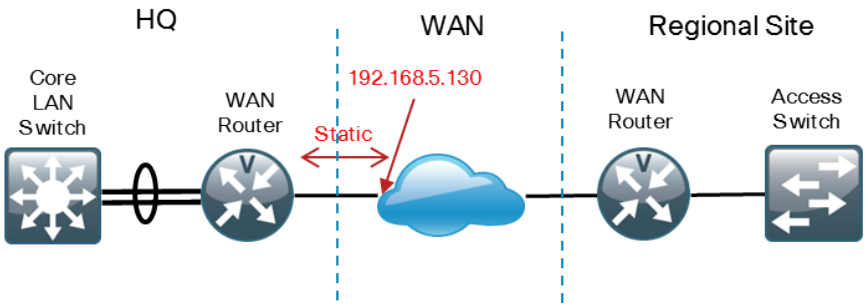
```
service-policy output WAN-QOS-POLICY
```

The QoS policy's "shape" average configuration will depend on the speed of the WAN connection, as defined in the QoS policy-map.

Procedure 6 Configure WAN router static routing

Headquarters routers apply static routing to forward traffic from their respective LANs to sites connected via the WAN. Static routing is the least-complex option if a remote site or headquarters router only has a single option for the next hop for WAN-bound traffic. The static routing configuration points a summarized route for LANS at all of the remote sites to the next-hop device in the WAN, as well as a route for the WAN interfaces of the remote-site routers.

Figure 24 - Headquarters WAN router static routing topology



Step 1: Configure static routes to remote sites' LANs on the headquarters router.

```
ip route 10.11.0.0 255.255.0.0 192.168.5.130
```

Step 2: Configure static routes to the remote-site routers' WAN interfaces.

```
ip route 192.168.5.128 255.255.255.224 192.168.5.130
```

Procedure 7 Configure headquarters WAN router EIGRP

The WAN router establishes an EIGRP adjacency with the core switch to exchange dynamic routing updates.

Step 1: To enable dynamic routing, configure EIGRP with the same autonomous system number as other devices in the LAN that participate in dynamic routing, and set the router instance to use the address on the router's loopback interface as the router ID.

```
router eigrp 1
  eigrp router-id 10.10.32.254
```

Step 2: Using the **network** command, enable EIGRP on all interfaces within the network range specified in this router, and configure the routing process so that routes will not be summarized before being advertised.

```
network 10.10.0.0 0.0.255.255
no auto-summary
```

Step 3: Configure EIGRP so that MPLS WAN interface does not participate in EIGRP.

```
router eigrp 1
  passive-interface GigabitEthernet0/0
```

Step 4: Configure EIGRP to advertise the static routes to the remote sites. The static routes are redistributed into EIGRP with the specified metric. By default, only the bandwidth and delay values are used for metric calculation.

```
router eigrp 1
  redistribute static metric 50000 100 255 1 1500
```

Tech Tip

Advertising the WAN interfaces' subnet is the easiest solution to make remote sites' routers' WAN interfaces reachable from the core network, in order to allow many router-based services to function properly.

Remote-Site WAN Router

This module describes the configuration processes for Remote-Site WAN routers.

Reader Tip

Any specific interfaces and IP addresses are examples based on the Cisco lab used to validate the architecture presented in this guide. Your interfaces and IP addresses will likely differ.

Process

Configuring the Remote-Site WAN Routers

1. Apply WAN router global configuration
2. Apply WAN router loopback interface
3. Configure WAN router QoS policy
4. Configure remote-site router interface
5. Configure remote-site static routing
6. Configure remote-site router LAN links
7. Configure remote-site multicast routing
8. Configure remote-site LAN DHCP pools

Complete each of the following procedures to configure remote-site WAN routers. Remote-sites are allocated eight /24 subnets, to provide for adequate connectivity and address flexibility as the network address requirements change. Routers are configured with the follow VLAN and address allocation scheme.

Table 5 - Remote site 1 VLANs

VLAN number	Purpose	Site 0 IP subnets	Site 1 IP subnets	Site 2 IP subnets	Site n IP subnets
N/A	Infrastructure	10.11.0.0/21	10.11.8.0/21	10.11.16.0/21	10.11.n*8.0/21
64	Wired Data	10.11.4.0/24	10.11.12.0/24	10.11.20.0/24	10.11.n*8+4.0/24
65	Wireless Data	10.11.2.0/24	10.11.10.0/24	10.11.18.0/24	10.11.n*8+2.0/24
69	Wired Voice	10.11.5.0/24	10.11.13.0/24	10.11.21.0/24	10.11.n*8+5.0/24
70	Wireless Voice	10.11.3.0/24	10.11.11.0/24	10.11.19.0/24	10.11.n*8+3.0/24

Procedure 1 Apply WAN router global configuration

WAN routers requires basic global configuration to enable infrastructural requirements such as management access and network time configuration.

Step 1: Apply the configuration described in the "Global Configuration Module" section earlier in this guide.

Procedure 2 Apply WAN router loopback interface

Branch WAN routers can use a loopback interface as a reliable IP address for router services, such as web-cache redirection, router telephony resources, and management addresses.

Step 1: Define the router's loopback interface.

```
interface Loopback0
  ip address 10.11.0.1 255.255.255.255
```

Step 2: Configure management services to use the loopback interface as their source address.

```
ip ssh source-interface Loopback0
ip pim register-source Loopback0
snmp-server trap-source Loopback0
ntp source Loopback0
```

Procedure 3 Configure WAN router QoS policy

Step 1: Perform the "Configure headquarters WAN QoS policy" procedure described earlier because it is identical for remote sites. Define the shape-average value for each site's WAN line rate so that the interface's output shaper can set bandwidth allocations for various traffic classes. The shape-average value is determined by the line rate of the WAN circuit, as in the following examples:

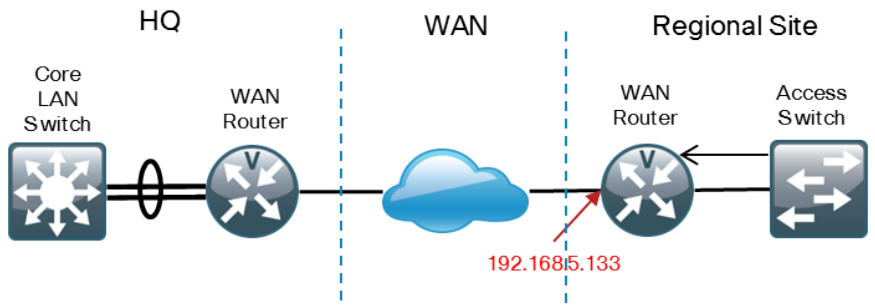
Table 6 - Shape-average values

Line speed	Shape-average value
384 Kbps	384k
T1: 1.44 Mbps	1440k
E1: 1.5 Mbps	1500k
10 Mbps	10m

Procedure 4 Configure remote-site router interface

You must configure an IP address on the Ethernet interface that connects to the service provider's MPLS private WAN.

Figure 25 - IP address on remote site's router for the connection to the WAN



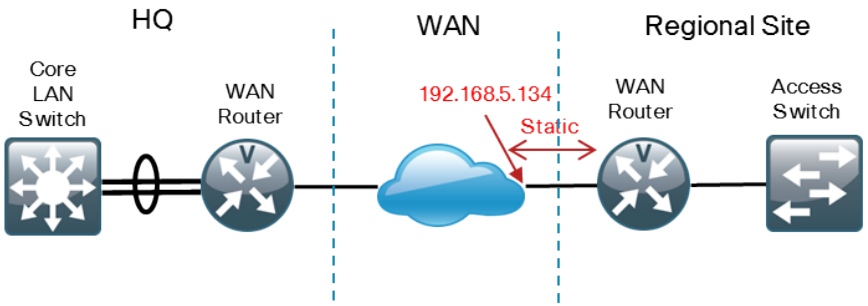
Step 1: Configure the router's Ethernet WAN interface's IP address, and apply the WAN QoS policy.

```
interface GigabitEthernet0/0
  description MPLS WAN Uplink
  ip address 192.168.5.133 255.255.255.252
  service-policy output WAN-QOS-POLICY
  no shutdown
```

Procedure 5 Configure remote-site static routing

Remote sites use static routing to an MPLS WAN to forward all traffic to the headquarters or regional site's aggregation router.

Figure 26 - Static default route from remote site to MPLS WAN



Step 1: Configure a static default route to forward all of the remote sites' LAN traffic to the WAN, and subsequently to the headquarters' router.

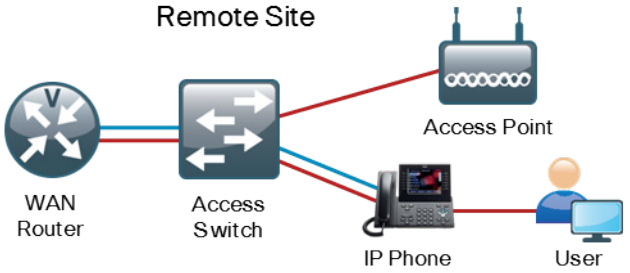
```
ip route 0.0.0.0 0.0.0.0 192.168.5.134
```

Procedure 6 Configure remote-site router LAN links

The remote-site router Ethernet configuration is similar to the headquarters, except for the following:

- There are more subinterfaces because the router is providing Layer 3 switching at the remote site for data and voice VLANs over a VLAN trunk interface.
- There is an option for remote sites that are connected to the access layer via a single link if a single-chassis access switch is used (as opposed to a stack), instead of a dual-link-connected EtherChannel.
- There is an option for small remote sites that use a Cisco 888 router that connects to the access switch with an Ethernet port in their integrated Ethernet switch.

Figure 27 - Uplink from LAN switch to remote-site router



Option 1. Configure an Etherchannel link to the LAN switch

This option connects remote site ISR G2 routers to an access switch stack with a multi-link Etherchannel for added resilience.

Step 1: Configure the remote-site router's connection to the remote-site Ethernet switch.

```
interface Port-channel1
 no ip address
 no shutdown
!
interface GigabitEthernet 0/1
 channel-group 1
 no shutdown
!
interface GigabitEthernet 0/2
 channel-group 1
 no shutdown
```

Step 2: Configure the Layer 3 subinterfaces' IP addresses that will provide routing for the subnets at the remote site, and match them to the 802.1q tag for the subinterface.

```
interface Port-channel1.64
 description Wired Data
 encapsulation dot1Q 64
 ip address 10.11.4.1 255.255.255.0
!
interface Port-channel1.69
 description Wired Voice
 encapsulation dot1Q 69
 ip address 10.11.5.1 255.255.255.0
```

Option 2. Configure a single Ethernet link to the LAN switch

This option connects remote site ISR G2 routers to a single-member access switch with a single Ethernet connection.

Step 1: Configure the remote-site router's connection to the remote-site Ethernet switch.

```
interface GigabitEthernet0/2
  no ip address
  no shutdown
```

Step 2: Configure the Layer 3 subinterfaces' IP addresses that will provide routing for the subnets at the remote site, and match them to the 802.1q tag for the subinterface.

```
interface GigabitEthernet0/2.64
  description Wired Data
  encapsulation dot1Q 64
  ip address 10.11.4.1 255.255.255.0
!
interface GigabitEthernet0/2.69
  description Wired Voice
  encapsulation dot1Q 69
  ip address 10.11.5.1 255.255.255.0
```

Option 3. Connect a Cisco 881 to the LAN switch

This option connects the remote site Cisco 881 router to a single-member access switch with a single Ethernet connection. This option differs significantly from the previous two options because the Cisco 881's LAN connectivity is provided by an embedded Ethernet switch.

Step 1: Configure the remote-site router's connection to the remote-site Ethernet switch.

```
interface FastEthernet0
 switchport trunk allowed vlan 1,2,64,69,1002-1005
 switchport mode trunk
 no ip address
 no shutdown
```

Step 2: Configure the Layer 3 subinterfaces' IP addresses that will provide routing for the subnets at the remote site and match them to the 802.1q tag for the VLANs on the trunk.

```
interface Vlan64
 description Wired Data
 ip address 10.11.4.1 255.255.255.0
!
interface Vlan69
 description Wired Voice
 ip address 10.11.5.1 255.255.255.0
```

Procedure 7 Configure remote-site multicast routing

Perform the "Configure headquarters WAN multicast routing" procedure described earlier in this guide because the procedure is identical for remote sites. Apply multicast configuration to all interfaces, including the routers' loopback interface that will participate in multicast routing.

```
ip pim sparse-mode
```

Procedure 8 Configure remote-site LAN DHCP pools

Remote sites use local DHCP service on WAN routers to assign basic network configuration for IP phones, wireless access-points, users' laptop and desktop computers, and other endpoint devices.

Step 1: Configure a DHCP scope for data endpoints, excluding DHCP assignment for the first ten addresses in the subnet.

```
ip dhcp excluded-address 10.11.4.1 10.11.4.10
ip dhcp pool wired-data
   network 10.11.4.0 255.255.255.0
   default-router 10.11.4.1
   domain-name cisco.local
   dns-server 10.10.48.10
```

Step 2: Configure a DHCP scope for voice endpoints, excluding DHCP assignment for the first ten addresses in the subnet. Voice endpoints require an option field to tell them where to find their initial configuration. Different vendors use different option fields, so the number vary based on the voice product you choose (for example, Cisco uses DHCP option 150).

```
ip dhcp excluded-address 10.11.5.1 10.11.5.10
ip dhcp pool wired-voice
   network 10.11.5.0 255.255.255.0
   default-router 10.11.5.1
   domain-name cisco.local
   dns-server 10.10.48.10
```

Process

Configuring the Remote-Site LAN Access Switch

1. Set global and platform-specific settings
2. Configure the access switch
3. Configure the access port
4. Configure the access switch uplink

Remote-site configuration focuses on the Cisco 2960-S, 3560-X, and 3750-X switches, excluding the 4507R+E chassis-based switch. Remote sites' LAN Access switch configuration is fairly similar to the headquarters LAN access switches' configuration, so a detailed description of the features is not provided in this section. If you have questions about the feature implementation details, see the "Configuring the Headquarters WAN Router" section earlier in this guide.

Procedure 1 Set global and platform-specific settings

The remote-site LAN access switch requires basic global configuration to enable infrastructural requirements such as management access and network time configuration.

Step 1: Apply configuration described in the "Global Configuration Module" section earlier in this guide.

Step 2: When configured in a stack, Catalyst 2960-S and 3750-X switch platforms require an initial configuration prior to configuring the features and services of the switch. If the remote site does not use a stack of 2960-S or 3750-X switches of three or more members, you can skip this step. Configure a switch that does not carry uplinks to the WAN router as the stack master.

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

Step 3: If the remote site does not use a 2960-S stack or a 3750-X stack, you can skip this step. Use the **stack-mac persistent timer 0** command to ensure that the original master MAC address remains the stack MAC address after a failure.

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

Step 4: To make consistent deployment of QoS easier, you define two macros for each platform that you use in later procedures to apply the platform specific QoS configuration.

```
macro name AccessEdgeQoS
auto qos voip cisco-phone
@
!
macro name EgressQoS
mls qos trust dscp
queue-set 2
srr-queue bandwidth share 1 30 35 5
priority-queue out
@
```

Procedure 2 Configure the access switch

Step 1: Configure device resiliency features and EtherChannel load-balancing behavior.

```
vtp mode transparent
spanning-tree mode rapid-pvst
udld enable
port-channel load-balance src-dst-ip
```

Step 2: Configure data and voice VLANs on the switch so connectivity to clients, IP phones, and the in-band management interfaces can be configured. Both the data and the voice VLAN will be available on all user-facing interfaces.

- The Wired Data VLAN (64) provides access to the network for all attached devices other than IP phones, and is used in the remote sites for management access to the switch.
- The Wired Voice VLAN (69) provides access to the network for IP phones.

All remote sites use the same VLANs.

```
vlan 64,69
```

Step 3: Configure the switch with an IP address so that it can be managed via in-band connectivity.

```
interface vlan 64
  ip address 10.11.4.5 255.255.255.0
  no shutdown
  ip default-gateway 10.11.4.1
```

Step 4: Configure DHCP snooping and ARP inspection.

```
ip dhcp snooping vlan 64,69
  no ip dhcp snooping information option
  ip dhcp snooping
  ip arp inspection vlan 64,69
```

Procedure 3 Configure the access port

To save time and make configuration easier when the same configuration will be applied to multiple interfaces on the switch, use the **interface range** command. This command allows you to issue a command once and have it apply to many interfaces at the same time. For example, the following command allows you to enter commands on all 23 interfaces (Gig 0/1 to Gig 0/23) simultaneously.

```
interface range Gigabitethernet 0/1-23
```

Step 1: Configure switch interfaces to support clients and IP phones.

The host interface configurations support PCs, phones, or wireless access points. Inline power is available on switches that support 802.3AF/AT for capable devices.

```
interface range [interface type] [port number]-[port number]
switchport access vlan 64
switchport mode access
switchport voice vlan 69
switchport host
macro apply AccessEdgeQoS
```

Step 2: Configure port security on the interface.

```
switchport port-security maximum 11
switchport port-security
switchport port-security aging time 2
switchport port-security aging type inactivity
switchport port-security violation restrict
```

Step 3: Apply DHCP snooping and ARP inspection on the interface.

```
ip arp inspection limit rate 100
ip dhcp snooping limit rate 100
```

Step 4: Configure IP Source Guard on the interface.

```
ip verify source
```

Step 5: Configure BPDU guard on the interface.

```
spanning-tree bpduguard enable
```

Step 6: (Optional): Configure QoS for trusted access devices.

In some cases you may want to trust the QoS markings from an access port device, like a video endpoint or wireless access point. To trust QoS from a device on an interface, enter the following commands.

```
no auto qos voip
auto qos trust dscp
```

Procedure 4 Configure the access switch uplink

Remote-site Access switches can be configured to connect with a single link, or ideally, using a multi-link EtherChannel connection to provide greater fault tolerance. An 802.1Q trunk is used for the connection to the upstream router, which allows it to provide the Layer 3 services to all the VLANs defined on the access layer switch. The VLANs allowed on the trunk are pruned to only the VLANs that are active on the access switch. DHCP snooping and ARP inspection are set to trust.

Option 1. Configure Interfaces as members of EtherChannel for multi-link EtherChannel uplink

Step 1: Configure physical uplinks to the remote-site WAN router.

Configure two or more physical interfaces to be members of the EtherChannel. The physical interfaces that are members of a Layer 2 EtherChannel are configured prior to configuring the logical port-channel interface. This allows for minimal configuration because most of the commands entered to a port-channel interface are copied to its members interfaces and do not require manual replication.

```
interface range [interface type] [port 1], [interface type]
[port 2]
switchport
macro apply EgressQoS
channel-group 1 mode on
no shutdown
```

Tech Tip

The Catalyst 2960-S does not require the **switchport** command.

Step 2: Configure the uplink VLAN trunk.

When you use EtherChannel, the interface type is port-channel and the number must match channel-group configured in Step 1.

```
interface Port-channel1
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 64,69
  switchport mode trunk
  ip arp inspection trust
  ip dhcp snooping trust
  logging event link-status
  no shutdown
```

Tech Tip

The Catalyst 2960-S does not require the **switchport trunk encapsulation dot1q** command.

Option 2. Configure an interface for single-link connection

Step 1: Configure physical uplinks to the remote-site WAN router.

```
interface [interface type] [port 1]
  switchport
  macro apply EgressQoS
  no shutdown
```

Tech Tip

The Catalyst 2960-S does not require the **switchport** command.

Step 2: Configure an interface for single-link connection.

```
interface [interface type] [port 1]
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 64,69
  switchport mode trunk
ip arp inspection trust
ip dhcp snooping trust
logging event link-status
```

Tech Tip

The Catalyst 2960-S does not require the **switchport trunk encapsulation dot1q** command.

Wireless Module

Business Overview

The effectiveness and efficiency of today's employee can be improved with the ability to stay connected regardless of location. As an integrated part of the wired networking port design that provides connectivity when a user is at their desk or another prewired location, wireless allows connectivity in transit to meetings and turns cafeterias or other meeting places into ad-hoc conference rooms. Wireless networks enable users to stay connected and the flow of information moving regardless of any physical building limitations.

Remote site and headquarters users can connect to voice and data services via the same methods and authentication database, creating a seamless business environment for the enterprise user.

Benefits include:

- **Location-independent network access**—Improves employee productivity.
- **Additional network flexibility**—Hard-to-wire locations can be reached without costly construction.
- **Easy to manage and operate**—Centralized control of the distributed wireless environment.
- **Plug and play deployment**—LAN switches preconfigured to recognize new access points connected to any access port.
- **Highly resilient deployment model**—Provide access to vital resources.

Technical Overview

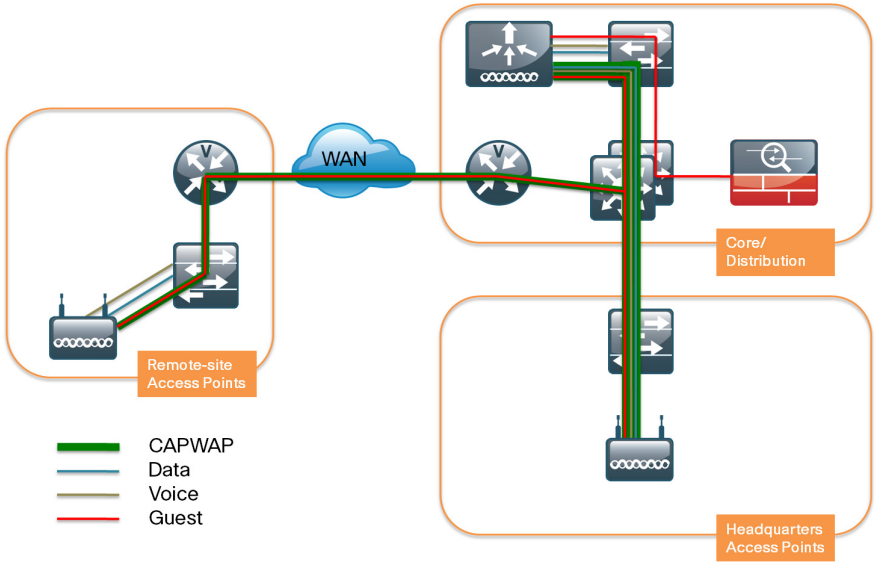
As the work environment becomes more mobile, the needs of companies are evolving as well—and Cisco technology and products are evolving to meet those needs by focusing on expanding wireless capabilities. Cisco recommends using a wireless mobility network for voice and data services to provide data, video, and voice connectivity for employees, voice connectivity for wireless IP phones, and wireless guest access for visitors to connect to the Internet.

With ease of deployment as one of the core goals, this wireless network design is secure and expandable and covers the headquarters and remote sites connected via a WAN. It does not cover the RF design that is unique in every environment.

In the past, the simplest approach was to use standalone APs, but each needed to be managed individually, and they lacked the ability to expand the network functionality across the entire network.

At the center of this new design is a WLC appliance that can be scaled to support the required number of APs to match the required coverage. For this design, Cisco recommends using a Cisco 5500 Series Wireless Controller that provides support for up to 500 APs each. For simplicity, the design uses two units, each having the same AP coverage that as a single unit can handle every AP deployed. Should one controller fail, the remaining controller can support every access point in the design. This resilient design is known as the N+N design, where the 'N' is a controller that supports a specific number of access points. In our design, we specifically used the Cisco 5508 WLC, which has eight Small Form-Factor Pluggable (SFP)-based distribution ports that provide EtherChannel connectivity to the server-farm switches directly off the core, which can be either copper or fiber, depending on distance and preference.

Figure 28 - Wireless LAN topology and VLAN switching



The APs used at the headquarters are Cisco 1140, 1260 and 3500 Series Lightweight Access Points with 802.11a/b/g/n support. Power is provided by standard 802.3af PoE from the access-layer switches, which allows the APs to be deployed without installing or modifying existing building electrical outlets (which is often the case because access points are typically mounted on the ceiling.)

APs at remote sites typically operate in lightweight mode. If connectivity between the remote site and headquarters is lost, they revert to standalone mode, which allows clients to remain connected to the LAN.

The deployment of wireless mobility requires a RADIUS server for authentication and DNS entry for the APs to locate the WLC.

At the headquarters, there will be a campus-wide data wireless LAN (WLAN) and a separate voice WLAN that will be terminated at the WLC where they will be put on their separate broadcast domains.

Each remote site will also carry the same data and voice WLANs that will be locally switched within the remote site to avoid traversing the WAN when accessing local resources. A single guest WLAN is deployed for the headquarters and all the remote sites, which is tunneled back to the headquarters WLC and onto a specific VLAN that connects to the Cisco Adaptive Security Appliance (ASA) providing secure access to the Internet while preventing access to the enterprise network. The guest WLAN has no wireless security and uses open authentication. Access to the Internet is controlled by using web authentication that uses an expiring guest account created locally on the WLC by the user holding the Lobby Ambassador account.

Deployment Details

Wireless LAN deployment consists of several processes:

- Configuring WLAN connectivity to the core
- Initializing the wireless controllers

Process

Configuring Wireless LAN Connectivity to the Core

1. Prepare core switch for WLC connection

Each WLC is connected by at least one link to different line cards on a chassis-based core switch, or different members of a multi-chassis core switch, to provide resilience. EtherChannel configuration offers load-balancing and resilience between the WLC and adjacent switches.

Procedure 1 Prepare core switch for WLC connection

The VLANs used in the following configuration are for headquarters wireless data (116), headquarters wireless voice (120), and wireless guest (1176). Networks that need more than one WLC due to resilience or scalability requirements will need to execute the steps below to assign port-channels and add physical port-channels for each wireless controller.

Table 7 - Switch ports and port channels for WLC downlinks

WLC name	Port-channel number	Physical switch port numbers
WLC-5508-1	11	GigabitEthernet 1/0/11 GigabitEthernet 2/0/11
WLC-5508-2	12	GigabitEthernet 1/0/12 GigabitEthernet 2/0/12

Step 1: Add Wireless VLANs to the core switch.

```
vlan 116
 name wireless-data
vlan 120
 name wireless-voice
vlan 1176
 name wireless-guest
```

Step 2: Define SVI Layer 3 configuration for wireless data and wireless voice VLANs. Add **ip helper-address** configuration to forward DHCP requests to the DHCP server.

Tech Tip

The wireless-guest VLAN's only Layer 3 interface is the default gateway on the Internet edge firewall, where the guest VLAN goes for Internet access. There is no SVI on the core switch to prevent routing the guest VLAN directly to the LAN.

```
interface Vlan116
  description Wireless Data
  ip address 10.10.16.1 255.255.252.0
  ip helper-address 10.10.48.10
  ip pim sparse-mode
  no shutdown
!
interface Vlan120
  description Wireless Voice
  ip address 10.10.20.1 255.255.252.0
  ip helper-address 10.10.48.10
  ip pim sparse-mode
  no shutdown
```

Step 3: Assign physical ports to port channel as a group, set spanning-tree configuration, and apply QoS macro.

```
interface range GigabitEthernet1/0/11,GigabitEthernet2/0/11
 description Etherchannel to WLC-5508-1
 channel-group 11 mode on
 spanning-tree link-type point-to-point
 macro apply EgressQoS
```

Step 4: Configure port-channel and add wireless VLANs to port-channel connecting to the core switch.

```
interface Port-channel11
 description EtherChannel to WLC-5508-1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 999
 switchport trunk allowed vlan 115,116,120,1176
 switchport mode trunk
```

Step 5: If you plan to use more than one WLC to provide WLC resiliency and scalability, repeat steps 3 and 4 for additional physical ports and port-channels.

Process

Initializing the Wireless Controllers

1. Run WLC setup script
2. Configure time zone
3. Disable RADIUS management access
4. Configure SNMP
5. Configure WLC resilience

Basic configuration of the WLC is applied through a CLI-driven dialog, accessed through the WLC's console port. Management addresses will be assigned according to the matrix in the following table.

Table 8 - WLC Management Addresses

WLC name	Management IP Address
WLC-5508-1	10.10.50.11
WLC-5508-2	10.10.50.12

Procedure 1 Run WLC setup script

Connect a terminal to the WLC console port to access the WLC's text-driven setup dialog.

Step 1: After powering up the WLC, a setup script appears.

```
Welcome to the Cisco Wizard Configuration Tool
Use the '-' character to backup
Would you like to terminate autoinstall? [yes]:
AUTO-INSTALL: starting now...
rc = 0
System Name [Cisco_7e:11:c4] (31 characters max):
AUTO-INSTALL: no interfaces registered.

AUTO-INSTALL: process terminated -- no configuration loaded
```

Step 2: Enter a system name.

```
System Name [Cisco_7e:8e:43] (31 characters max): WLC-5508-1
```

Step 3: Enter an administrator username and password.

```
Enter Administrative User Name (24 characters max): admin
Enter Administrative Password (24 characters max): *****
Re-enter Administrative Password : *****
```

Step 4: Use DHCP for the service port interface address.

```
Service Interface IP address Configuration [none] [DHCP]: DHCP
```

Step 5: Enable link aggregation.

```
Enable Link Aggregation (LAG) [yes][NO]: yes
```

Step 6: Enter the IP address and subnet mask for the management interface.

```
Management Interface IP Address: 10.10.15.11
Management Interface Netmask: 255.255.255.0
Management interface Default Router: 10.10.15.1
Management Interface VLAN Identifier (0 = untagged): 115
```

Step 7: Enter the default DHCP server for clients.

```
Management Interface DHCP Server IP Address: 10.10.48.10
```

Step 8: Enter the virtual interface. The WLC uses the virtual interface for mobility DHCP relay and inter-controller communication.

```
Virtual Gateway IP Address: 192.168.255.1
```

Step 9: Enter a name that will be used as the default mobility and RF group.

```
Mobility/RF Group Name: SBA
```

Step 10: Enter an initial SSID of WLAN-data or your choice of SSID name that you want to use as your data WLAN's SSID.

```
Network Name (SSID): WLAN-data
```

Step 11: Accept the default response no to avoid configuring the DHCP bridging mode.

```
Configure DHCP Bridging Mode [yes][NO]: no
```

Step 12: Enter no to make clients use DHCP IP addresses.

```
Allow Static IP Addresses [YES][no]: no
```

Step 13: Accept the default **YES** to configure RADIUS.

```
Configure a RADIUS Server now? [YES][no]: YES
Enter the RADIUS Server's Address: 10.10.48.10
Enter the RADIUS Server's Port [1812]:
Enter the RADIUS Server's Secret: c1sco123
```

Tech Tip

A basic procedure for configuring a RADIUS authentication server is provided in this document in Appendix B.

Step 14: Enter the correct country code for the country in which you are deploying. If you don't know the country code, enter **help** to get a list of valid country codes.

```
Enter Country Code list (enter 'help' for a list of countries)
[US]: US
```

Step 15: Enter **yes** to enable all wireless networks. 802.11a is typically used for wireless IP phones and 802.11b/g/n is typically used for data.

```
Enable 802.11b network [YES][no]: yes
Enable 802.11a network [YES][no]: yes
Enable 802.11g network [YES][no]: yes
```

Step 16: Enable the WLC's radio resource management (RRM) auto RF feature by entering **yes**.

```
Enable Auto-RF [YES][no]: yes
```

Step 17: Synchronize the WLC clock to the organizations NTP server.

```
Configure a NTP server now? [YES][no]:YES
Enter the NTP server's IP address: 10.10.48.17
Enter a polling interval between 3600 and 604800 secs: 86400
```

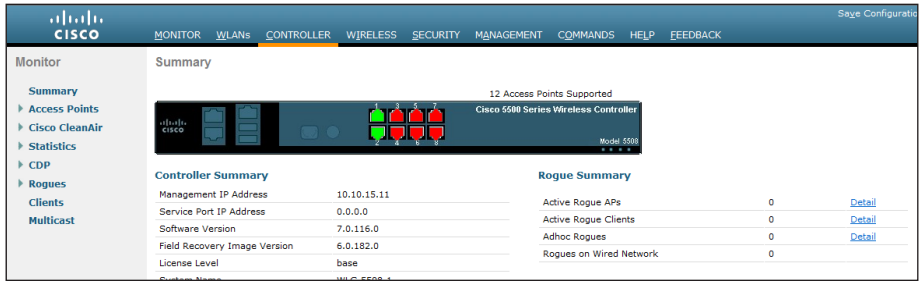
Step 18: Save the configuration. If you respond with **no** in this step, the system restarts without saving the configuration and you must complete this procedure again.

```
Configuration correct? If yes, system will save it and reset.
[yes][NO]: YES
Configuration saved!
Resetting system with new configuration
```

Step 19: Once the WLC has reset, use a compatible web browser to log in to the Cisco Wireless LAN Controller Administration page using the credentials defined in Step 3 (Example: https://10.10.15.11/). You may also use a DNS name if you have added a host entry for the management IP address.

Step 20: After logging into the web interface, we are able to verify the basic health of the WLC on the **Monitor > Summary** page.

This page shows the distribution ports that are up (in green) and any APs that have established communications.



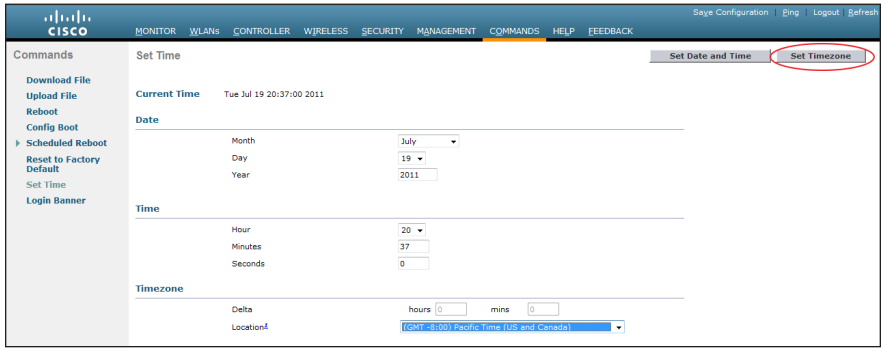
Step 21: Repeat this procedure for the secondary WLC.

Procedure 2 Configure time zone

Step 1: On the primary WLC, navigate to **Commands** > **Set Time.**

Step 2: In the **Location** list, select the timezone that corresponds to the location of the WLC.

Step 3: Click **Set Timezone**.

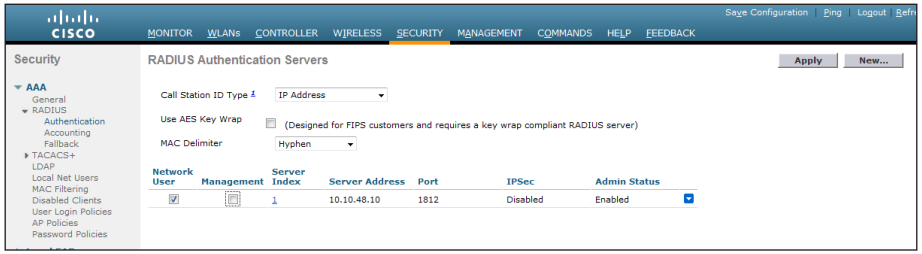


Step 4: Repeat this procedure for the secondary WLC.

Procedure 3 Disable RADIUS management access

By configuring RADIUS in the Initial Configuration Dialog, all users are allowed access to the WLC's management interface. The RADIUS configuration must be adjusted so as to prevent management access by all users.

Step 1: On the primary WLC, click **Security** > **AAA** > **RADIUS** > **Authentication**. Clear the check mark in the **Management** column.



Step 2: Click **Apply.**

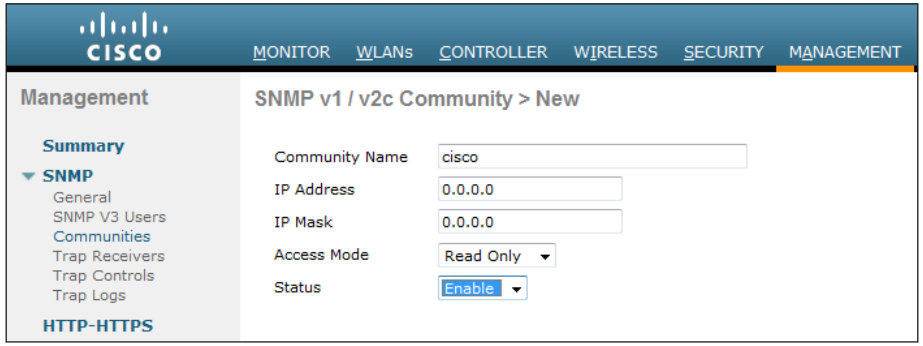
Step 3: Repeat this procedure for the secondary WLC.

Procedure 4 Configure SNMP

Step 1: On the primary WLC, click **Management** > **SNMP** > **Communities**, and then click **New**.

Step 2: Fill in the fields in the **SNMP v1/v2c Community** > **New** window as described:

- Enter the **Community Name**. (Example: **cisco**)
- Enter the **IP Address.** (Example: 0.0.0.0)
- Enter the **IP Mask**. (Example: 0.0.0.0)
- In the **Status** list, choose **Enable**.



Step 3: Click **Apply.**

Step 4: In **Management** > **SNMP** > **Communities**, click **New**.

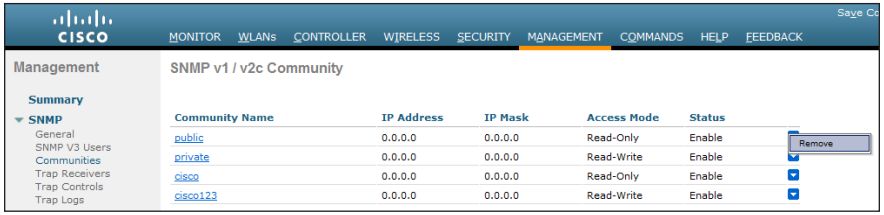
Step 5: Fill in the fields in the **SNMP v1/v2c Community** > **New** window as described:

- Enter the **Community Name**. (Example: **cisco123**)
- Enter the **IP Address.** (Example: 0.0.0.0)
- Enter the **IP Mask**. (Example: 0.0.0.0)
- In the **Access Mode** list, choose **Read/Write**.
- In the **Status** list, choose **Enable**.

Step 6: Click **Apply.**

Step 7: Navigate to **Management** > **SNMP** > **Communities**.

Step 8: Point to the blue drop-down menu icon for the **public** community, and then click **Remove**.



Step 9: In the **Are you sure you want to delete?** message box, click **OK**.

Step 10: Repeat Step 8 and Step 9 for the **private** community, so that only the **cisco** and **cisco123** communities remain.

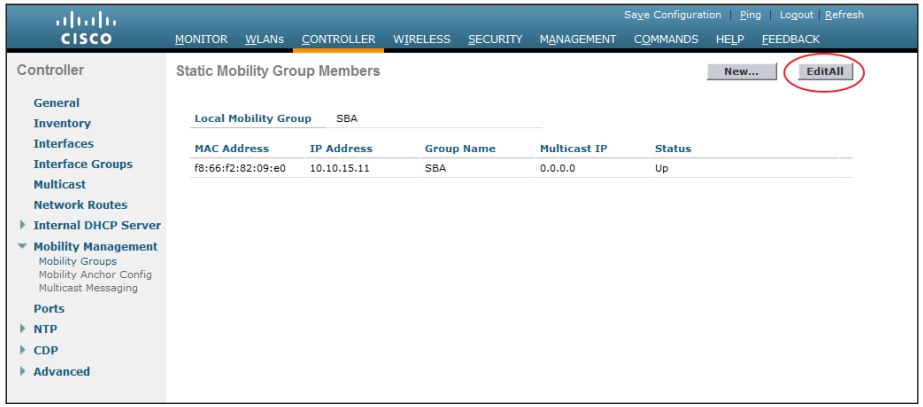
Step 11: Repeat this procedure for the secondary WLC.

Procedure 5 Configure WLC resilience

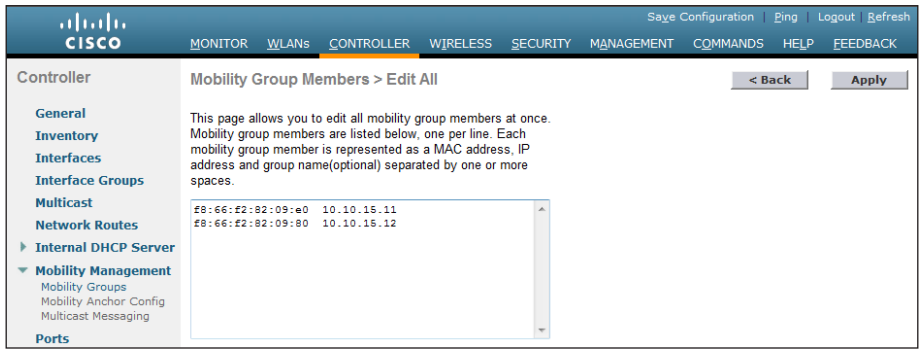
Our network design can use two controllers to offer resilience and scalability by leveraging the N+N controller deployment model. This model allows the network to continue offering WLAN connectivity after the failure of a WLC. During normal operation, the access-point load is distributed across all resilient controllers in the network. Each controller is no more than 50% loaded to the access-point capacity for which it is licensed and that it can handle. In this configuration, should a controller fail, the remaining controllers can register all the network access points.

To provide resilience, the WLCs must be configured as members of a mobility group.

Step 1: On both WLCs, click **Controller** > **Mobility Management** > **Mobility Groups** and then click **EditAll**.



Step 2: Copy and paste each controller's MAC address and IP Address to the other WLC's **Edit All** entry field.



Step 3: Click **Apply**.

Step 4: Perform this entire procedure on both controllers.

Step 5: Refresh the display by clicking **Controller** > **Mobility Management** > **Mobility Groups** until all of the WLCs in the mobility group have initialized communication between each other, which is indicated by the value **Up** in the **Status** column. This may take a few minutes.

Process

Configuring WLCs for Voice and Data Access

1. Create data and voice interfaces
2. Create voice and data WLANs

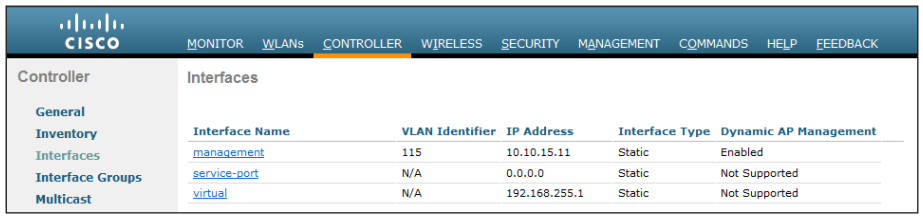
Separate Wireless Voice and Wireless Data networks are used to maintain consistency with the wired policy. Applying QoS to traffic based on Layer 3 characteristics can be easier to enforce. Configuration details will be applied as described in the following table.

Table 9 - WLC Configuration Details

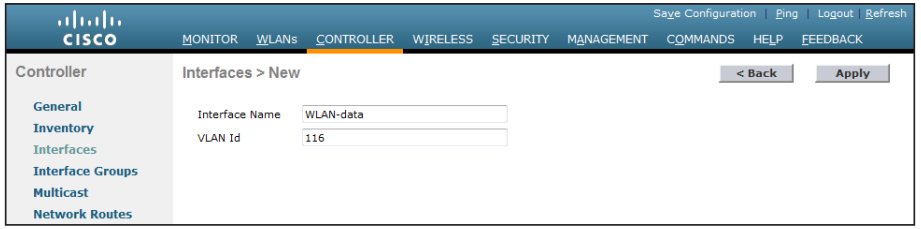
WLC name	Data VLAN	WLAN-data IP address	Voice VLAN	WLAN-voice IP address
WLC-5508-1	116	10.10.16.11	120	10.10.20.11
WLC-5508-2	116	10.10.16.12	120	10.10.20.12

Procedure 1 Create data and voice interfaces

Step 1: In **Controller** > **Interfaces** click **New**.

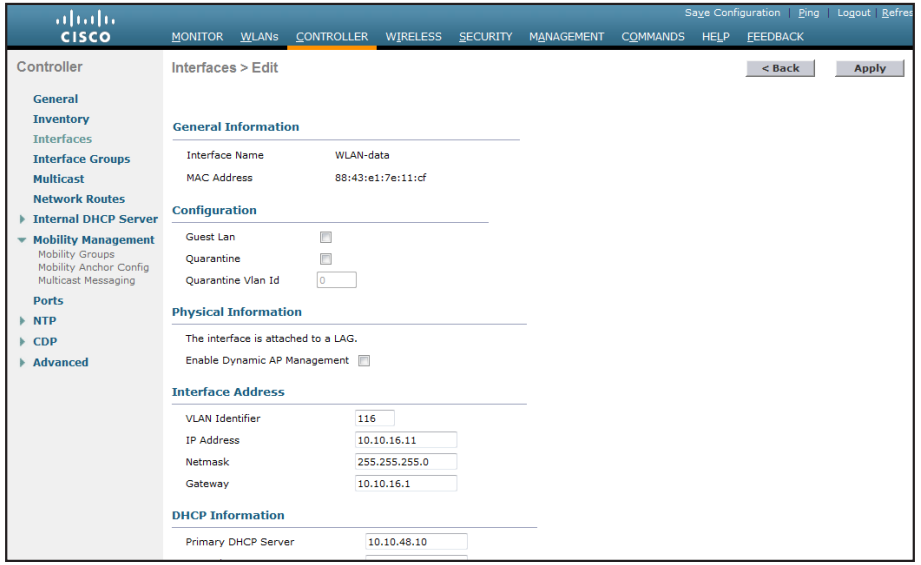


Step 2: Add the data interface name of **WLAN-data** (without spaces) and VLAN ID of **116**, **and then click Apply.**

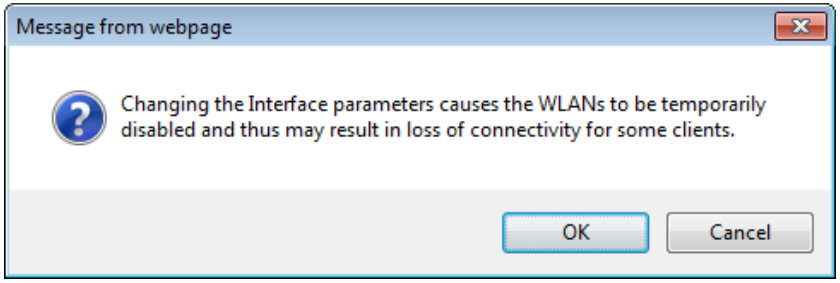


Step 3: Configure the following attributes, **and then click Apply**:

- IP Address: **10.10.16.11**
- Network Mask: **255.255.252.0**
- Default-Gateway: **10.10.16.1**
- DHCP server: **10.10.48.10**



Step 4: Click **OK** to acknowledge the warning that WLANs will be temporarily disabled as a result of changes you are making.



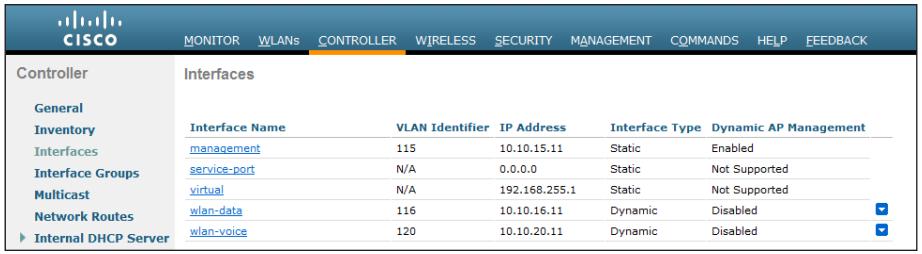
Step 5: On the primary controller, repeat Steps 1 through 4 with the values in the following table to configure the **wlan-voice** interface.

Attribute	Value
Interface Name	WLAN-voice
VLAN Id	120
IP Address	10.10.20.11
Network Mask	255.255.252.0
Default Gateway	10.10.20.1
DHCP Server	10.10.48.10

Tech Tip

To prevent DHCP from assigning addresses to wireless clients that conflict with the WLC's addresses, exclude the addresses you assign to the WLC interfaces from DHCP scopes.

Step 6: Verify the interface configuration.



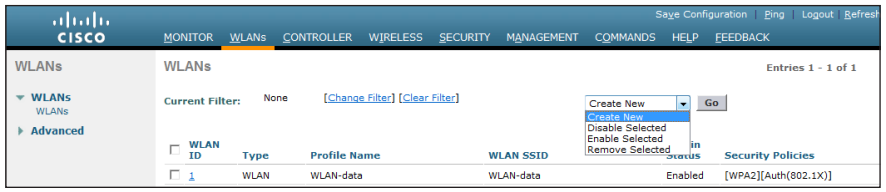
Step 7: Repeat Steps 6 and 7 on other WLC in the mobility group, using the following configuration values:

Attribute	Data WLAN values	Voice WLAN values
Interface Name	WLAN-data	WLAN-voice
VLAN Id	116	120
IP Address	10.10.16.12	10.10.20.12
Network Mask	255.255.252.0	255.255.252.0
Default Gateway	10.10.16.1	10.10.20.1
DHCP Server	10.10.48.10	10.10.48.10

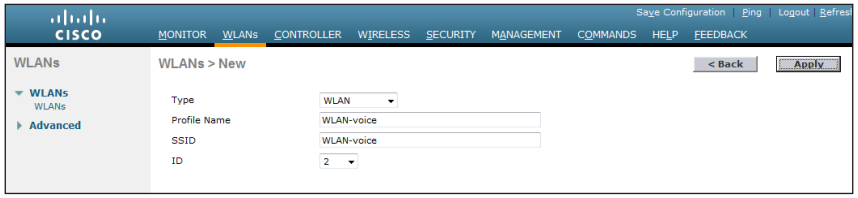
Procedure 2 Create voice and data WLANs

In this section, you authenticate data and voice against the previously configured RADIUS server. QoS is the real difference because voice must have greater access to transmit and receive packets than wireless data traffic.

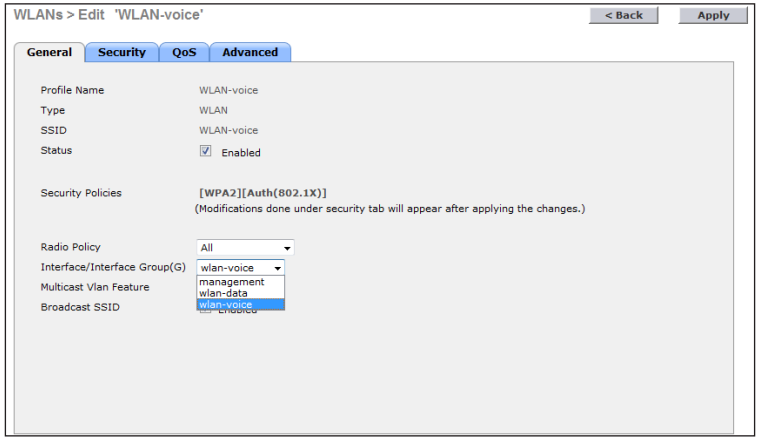
Step 1: In **WLANs > WLANs**, choose **Create New** from the drop-down list and then click **Go**.



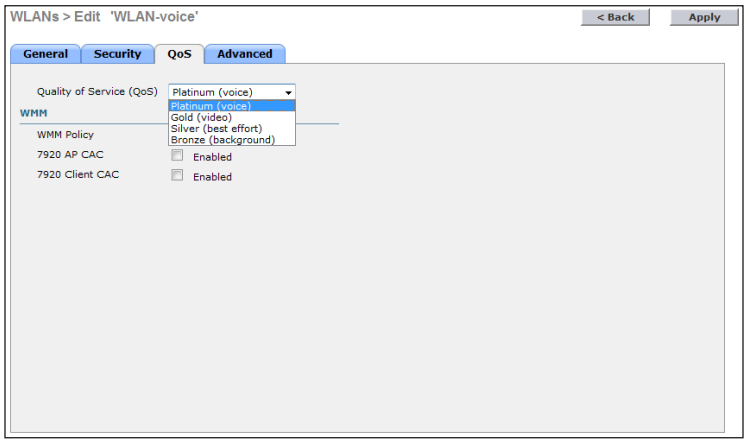
Step 2: Add a profile name of **WLAN-voice** and the Voice SSID of **WLAN-voice**, leave the ID provided in the drop-down list as it appears, and then click **Apply**.



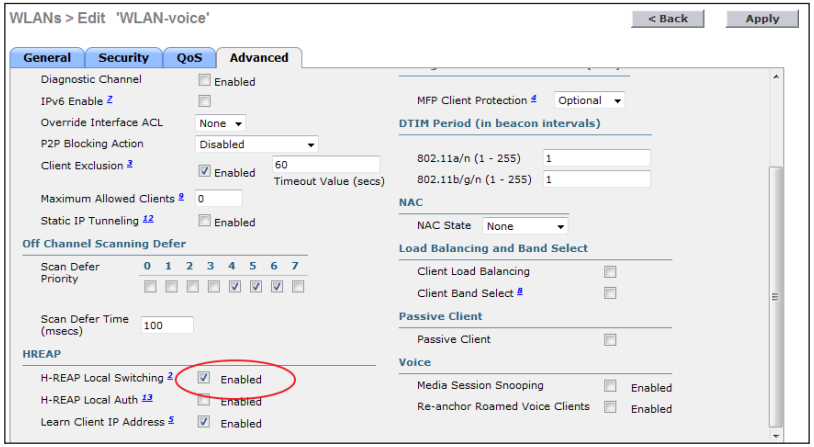
Step 3: On the **General** tab, select the **Status Enabled** check box, and in the **Interface** drop-down list, select the **WLAN-voice** interface you created previously.



Step 4: On the **QoS** tab, choose **Platinum (voice)** in the **Quality of Service (QoS)** list.

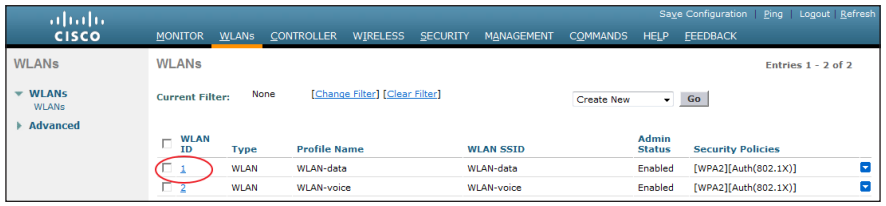


Step 5: On the **Advanced** tab, scroll to the bottom of the tab, and select the **H-REAP Local Switching Enabled** check box and then click **Apply**.

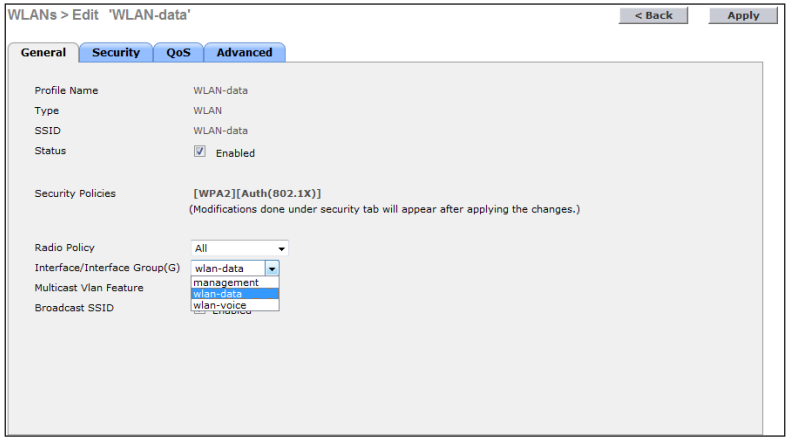


Step 6: Click **OK** to acknowledge the warning that Platinum QoS will degrade data network performance.

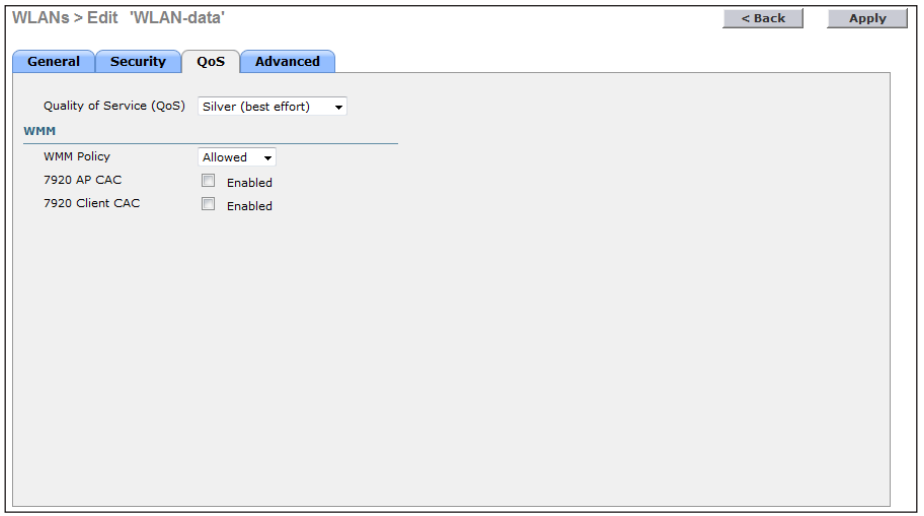
Step 7: In **WLANs** > **WLANs**, click **1** next to **WLAN-data.**



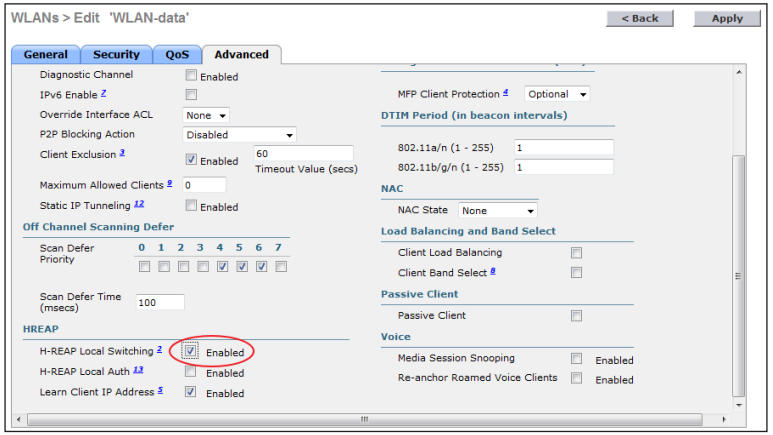
Step 8: On the **General** tab, select the **Status Enabled** check box, and in the **Interface** drop-down list, select the VLAN **wlan-data** you created previously.



Step 9: On the **QoS** tab, verify that the **Silver (best effort)** is selected.



Step 10: On the **Advanced** tab, select the **H-REAP Local Switching Enabled** check box and then click **Apply**.



Step 11: Review the WLAN configuration.

Step 12: Repeat this procedure on other WLC in the mobility group.

Process

Connecting APs to the Headquarters LAN

1. Prepare DNS to support wireless APs

You need to prepare the headquarters LAN and network infrastructure to support wireless APs.

APs request their IP address, subnet mask, gateway, and DNS server addresses from DHCP, and then the AP uses DNS to resolve cisco-capwap-controller and establish a connection with the WLC to configure the AP and enable the radios (they are disabled by default).

Procedure 1 Prepare DNS to support wireless APs

Configure the LAN's DNS servers (in this case, 10.10.48.10) defined in the network's DHCP service to resolve the cisco-capwap-controller host name to the management IP address of the WLC (in this case, 10.10.50.11). The cisco-capwap-controller DNS record provides bootstrap information for access points that run software version 6.0 and higher.

Tech Tip

If the network may include APs that run software older than version 6.0, add a DNS record to resolve the host name cisco-lwapp-controller to the WLC's management IP address of the WLC.

Step 1: At the headquarters, the access ports, which APs connect to, use a standard access switchport configuration, with one exception: the default trust must be changed from CoS to DSCP by using the following interface command.

```
mls qos trust dscp
```

Remote-Site Wireless

Each remote site has a data and voice WLAN, which matches the WLANs that we just configured for the LAN, but with one fundamental difference: you use Hybrid Remote Edge Access Point (H-REAP) to locally switch wireless packets at the remote site. At the headquarters, the wireless user traffic is transported over Control and Provisioning of Wireless Access Points (CAPWAP) using the wired data VLAN to the WLC. From there it is switched out over the link aggregation (LAG) ports, which form an 802.1Q trunk, into the resilient core as illustrated at the beginning of this module. If wireless traffic at the remote sites also behaved this way, the traffic between two devices within the remote site would then be transported via CAPWAP over the WAN to the company's WLC(s) where it would be trunked into the core, to be routed back across the WAN to its destination. Routing traffic this way can be problematic for Unified Communications because a wireless IP phone making a call out of the remote-site gateway would traverse the WAN twice, when in reality, it did not need to leave the remote site at all. To resolve this, the voice and data WLAN is locally switched via a trunking interface on the AP and the guest WLAN is still centrally switched. This switching pattern allows only the management, control, and guest traffic to be transported via CAPWAP to the WLC at the headquarters.

The remote-site configuration is discussed later in this guide, but during the initial creation of the WLANs, you need to enable both the voice and data WLANs to locally switch packets for this purpose alone.

Process

Configuring Remote-Site Wireless Access

1. Prepare DNS to support Wireless APs
2. Configure Remote-Site Router for WLAN
3. Add remote-site WLAN DHCP pools
4. Configure Remote-Site Switch for WLAN
5. Configure Hybrid Remote Edge AP

On the headquarters' wireless controllers, you configured three WLANs, two of which are enabled for local switching via H-REAP. APs at the headquarters apply the default mode of operation (local mode), forwarding all wireless LAN traffic via CAPWAP to the controller and switching the wireless traffic to the wired network. At the remote site, you change the APs' behavior to H-REAP mode, so that the APs switch the remote sites' traffic directly to the LAN at the remote site, instead of forwarding it to the headquarters over a CAPWAP tunnel before switching it to the LAN. You must configure remote-site routers to provide DHCP scopes and routing connectivity for the additional VLANs, and you must configure remote-site switches for connectivity for APs.

Routers and switches are configured with the following VLAN and address allocation scheme:

Table 10 - Remote Site 1 VLANs

VLAN number	Purpose	Site 0 IP subnets	Site 1 IP subnets	Site 2 IP subnets	Site n IP subnets
N/A	Infrastructure	10.11.0.0/24	10.11.8.0/24	10.11.16.0/24	10.11.n*8.0/24
64	Wired Data	10.11.4.0/24	10.11.12.0/24	10.11.20.0/24	10.11.n*8+4.0/24
65	Wireless Data	10.11.2.0/24	10.11.10.0/24	10.11.18.0/24	10.11.n*8+2.0/24
69	Wired Voice	10.11.5.0/24	10.11.13.0/24	10.11.21.0/24	10.11.n*8+5.0/24
70	Wireless Voice	10.11.3.0/24	10.11.11.0/24	10.11.19.0/24	10.11.n*8+3.0/24

Procedure 1 Prepare DNS to support Wireless APs

Similar to the headquarters LAN, if the remote sites use their own DNS, you must add an A record so that the remote sites' name servers resolve the WLAN controllers' addresses. If remote sites use the headquarters' DNS, you can skip this procedure.

Configure the LAN's DNS servers (in this case, 10.10.48.10) defined in the network's DHCP service to resolve the cisco-capwap-controller host name to the management IP address of the WLC (in this case, 10.10.15.11). The cisco-capwap-controller DNS record provides bootstrap information for access points that run software version 6.0 and higher.

Tech Tip

If the network includes APs that run software older than version 6.0, add a DNS record to resolve the hostname cisco-lwapp-controller to the WLC's management IP address.

Procedure 2 Configure Remote-Site Router for WLAN

Remote-site routers require additional configuration to support wireless VLANs. The procedure varies by the type of connection from the access switch to the router's ports:

- Multi-link EtherChannel trunk to a Cisco ISR G2 2951,2921, or 2911
- Single-link Ethernet trunk to a Cisco ISR G2 2951, 2921, or 2911
- Single-link Ethernet trunk to a switchport on a Cisco ISR G2 881

Option 1. Add VLANs to an Etherchannel link from the WAN router

This option adds wireless VLANs to a remote site ISR G2 router's multi-link Etherchannel trunk to an access switch stack.

Step 1: Add subinterfaces to the WAN router's port-channel.

```
interface Port-channel1.65
 description Wireless Data
 encapsulation dot1Q 65
 ip address 10.11.2.1 255.255.255.0
 ip pim sparse-mode
!
interface Port-channel1.70
 description Wireless Voice
 encapsulation dot1Q 70
 ip address 10.11.3.1 255.255.255.0
 ip pim sparse-mode
```

Option 2. Configure a single Ethernet link to the LAN switch

This option adds wireless VLANs to a remote site ISR G2 router's single-link Ethernet trunk to a single-member access switch.

Step 1: Add subinterfaces to the WAN router's physical interface.

```
interface GigabitEthernet0/2.65
  description Wireless Data
  encapsulation dot1Q 65
  ip address 10.11.2.1 255.255.255.0
  ip pim sparse-mode
!
interface GigabitEthernet0/2.70
  description Wireless Voice
  encapsulation dot1Q 70
  ip address 10.11.3.1 255.255.255.0
  ip pim sparse-mode
```

Option 3. Connect a Cisco 881 to the LAN switch

This option adds wireless VLANs to a remote site Cisco 881 router's single-link Ethernet trunk to a single-member access switch.

Step 1: Add the wireless VLANs to the router's VLAN switch database:

```
vlan 65,70
```

Step 2: Add the VLANs tp the switchport that connects to the access switch:

```
interface FastEthernet0
 switchport trunk allowed vlan add 65,70
```

Step 3: Configure the Layer 3 subinterfaces' IP addresses that will provide routing for the wireless subnets at the remote site and match them to the 802.1q tag for the VLANs on the trunk.

```
interface Vlan65
 description Wireless Data
 ip address 10.11.2.1 255.255.255.0
!
interface Vlan70
 description Wireless Voice
 ip address 10.11.3.1 255.255.255.0
```

Procedure 3 Add remote-site WLAN DHCP pools

Remote sites provide IP addresses for wireless endpoints with a local DHCP service in the WAN router.

Step 1: Add DHCP scopes for wireless data and wireless voice.

```
ip dhcp excluded-address 10.11.2.1 10.11.2.10
ip dhcp pool wireless-data
   network 10.11.2.0 255.255.255.0
   default-router 10.11.2.1
   domain-name cisco.local
   dns-server 10.10.48.10
!
ip dhcp excluded-address 10.11.3.1 10.11.3.10
ip dhcp pool wireless-voice
   network 10.11.3.0 255.255.255.0
   default-router 10.11.3.1
   domain-name cisco.local
   dns-server 10.10.48.10
```

Procedure 4 Configure Remote-Site Switch for WLAN

Access points require configuration changes to the remote-site switches to offer the appropriate trunk behavior to accommodate H-REAP wireless switching.

Step 1: Add the wireless data and wireless voice VLANs to the remote-site access switch's VLAN database.

```
vlan 65,70
```

Step 2: Add the wireless data and wireless voice VLANs to the remote-site access switch's uplink trunk to the WAN router. If the uplink trunk is an EtherChannel, use the following configuration.

```
interface Port-channel1
  switchport trunk allowed vlan add 65,70
```

If the uplink trunk is a single link, use the following configuration.

```
interface [interface type] [port 1]
  switchport trunk allowed vlan add 65,70
```

Step 3: Reset the remote-site access port where the wireless APs will be connected to default configuration.

```
default interface GigabitEthernet0/23
```

Step 4: Configure the access switch interface where the AP will be connected to allow a VLAN trunk for branch-site VLANs that is required by the AP.

```
interface GigabitEthernet0/23
  description HREAP Access Point Connection
  no auto qos voip
  no ip verify source
  auto qos trust dscp
  switchport trunk encapsulation dot1q
  switchport trunk native vlan 64
  switchport trunk allowed vlan 64-65,70
  switchport mode trunk
  switchport port-security maximum 255
  spanning-tree portfast trunk
```

Step 5: Configure DAI.

```
ip arp inspection trust
```

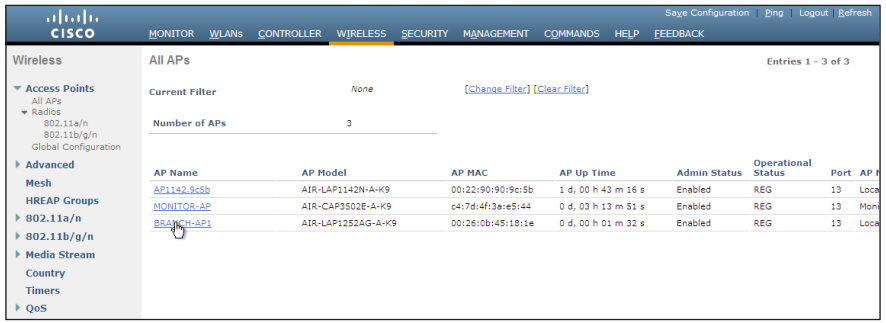
Step 6: Configure DHCP snooping to trust for multiple clients.

```
ip dhcp snooping trust
```

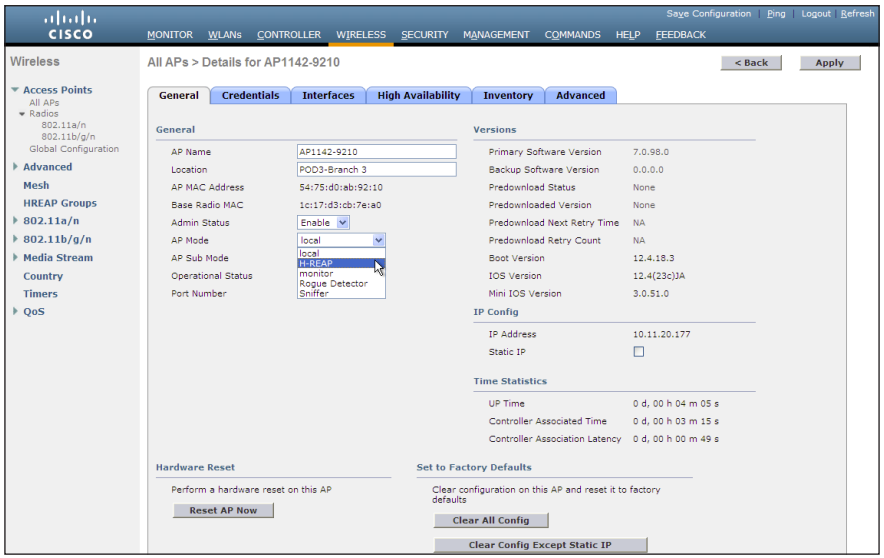
Procedure 5 Configure Hybrid Remote Edge AP

Step 1: Connect APs to switches at the remote sites. Log in to the WLAN controller's web interface and go to **WIRELESS** > **Access Points**.

Step 2: Select a remote-site AP.



Step 3: Change the value in the **AP Mode** list to **H-REAP**, click **Apply**, and then click **Back**.

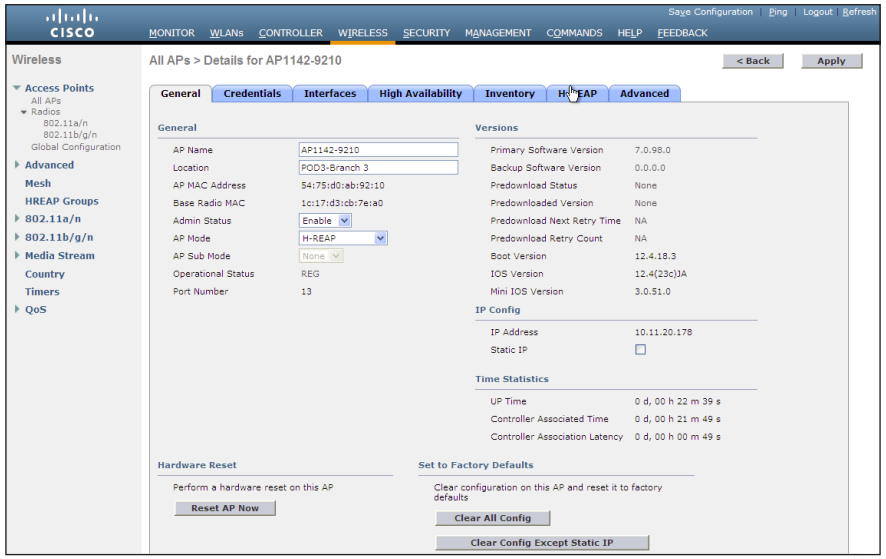


The access point reboots, comes back, and then connects to the controller after approximately three minutes.

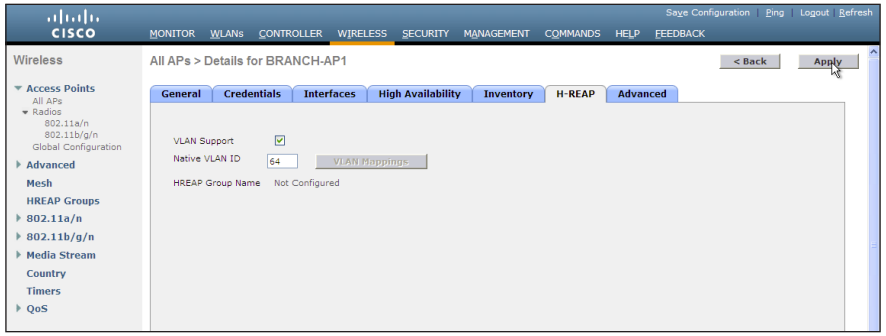
Tech Tip

If you have multiple WLCs in a mobility-group, APs may reconnect to a different WLC in the mobility group.

Step 4: Select the same remote-site AP, click the **H-REAP** tab.



Step 5: Select the **VLAN Support** check box, type **64** in **Native VLAN ID**, and then click **Apply**.

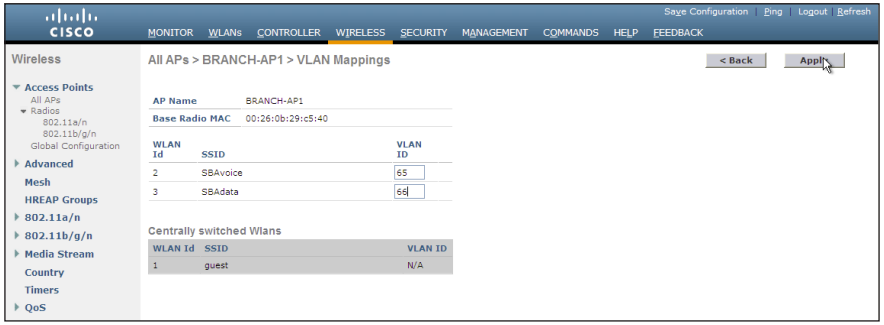


Step 6: Click **VLAN Mappings,** which is now active.

Step 7: In **WLAN Ids**, type **70** in **VLAN ID** for the **WLAN-voice** SSID, type **65** in **VLAN ID** for the **WLAN-data** SSID, and then click **Apply**.

Reader Tip

Notice that the guest WLAN is gray and unable to map, but the Voice and Data WLANs can be assigned to the two Wired Voice and Data VLANs at the remote site.



Process

Configuring Guest Access

1. Create the Guest Interface
2. Create Guest DHCP Scope
3. Create Guest WLAN
4. Create Guest-Admin Account
5. Create Guest Accounts

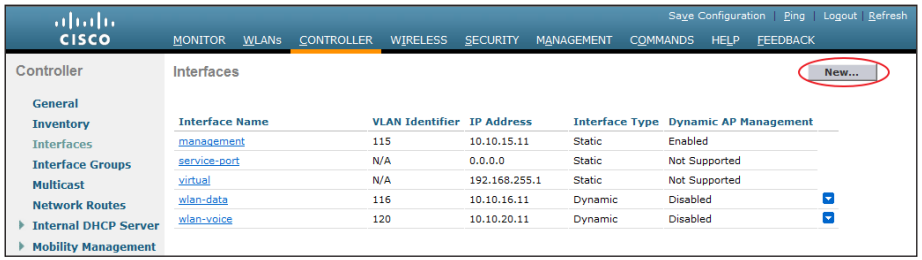
In this section, you deploy a guest wireless network that allows visitors, with a guest username and password, to access the Internet at the headquarters and remote sites.

On the core and server-room switches, you used VLAN 1176 to switch guest traffic to the ASA. The VLAN interface on the core switch does not have an IP address because this subnet's default gateway will be the ASA. This prevents the wireless guest network's access to the rest of the network. The WLC provides DHCP services and guest authentication for the guest WLAN. The guest account on the WLC expires after a predetermined length of time (the default is 24 hours), after which a guests are required to provide a new authentication using a new username and password. You complete the Cisco ASA's guest-network firewall configuration in the Security section of this guide to allow access to the Internet.

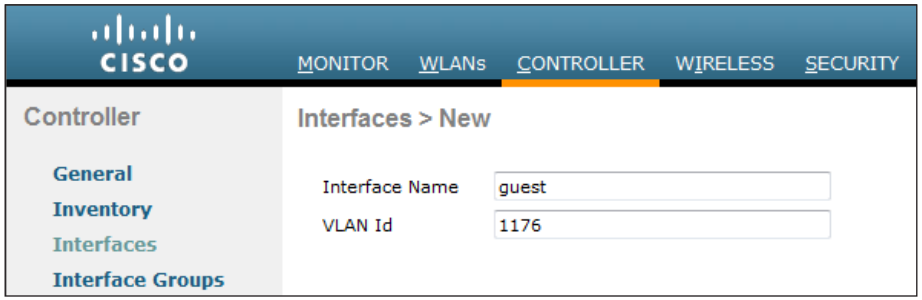
Procedure 1 Create the Guest Interface

Configure an interface for guest WLAN connectivity.

Step 1: In **Controller** > **Interfaces**, click **New**.



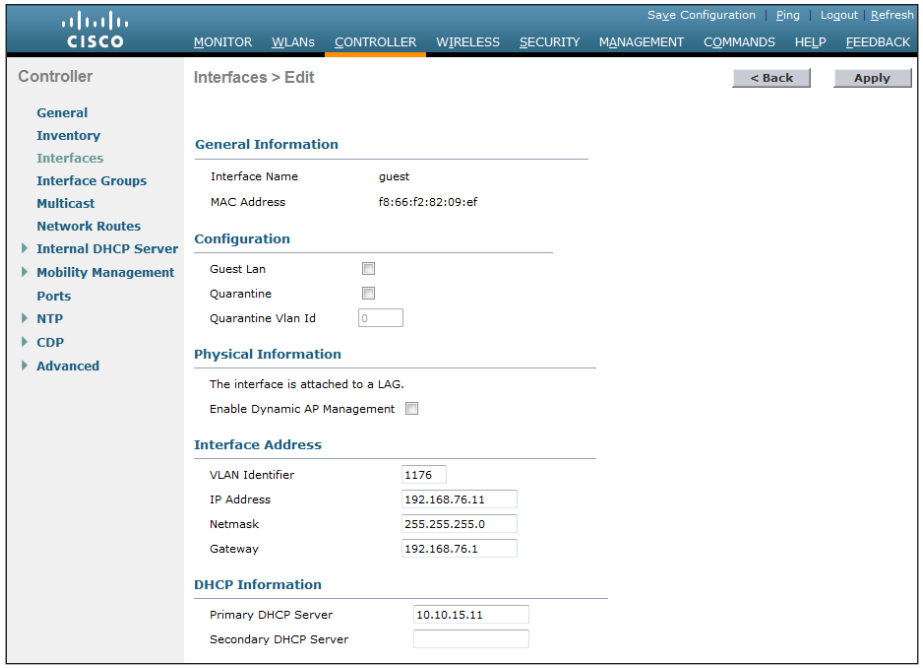
Step 2: In **Interface Name**, type **guest**, in **VLAN Id** type **1176**, and then click **Apply**.



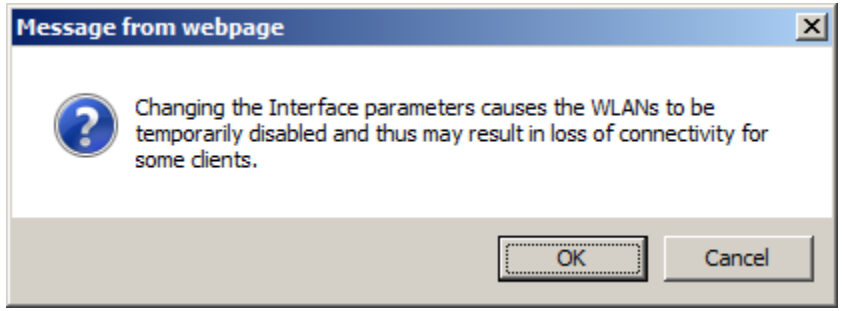
Step 3: In the **Interfaces>Edit** window, enter the following:

- IP Address—192.168.76.11
- Netmask—255.255.255.0
- Gateway—192.168.76.1
- Primary DHCP Server—10.10.15.11

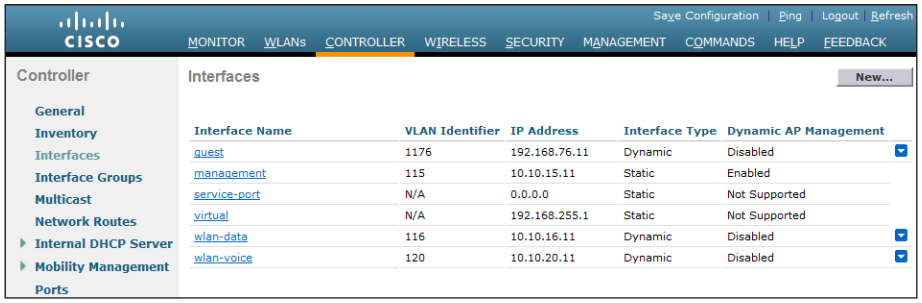
Step 4: Click **Apply**.



Step 5: Click **OK** to acknowledge the warning that WLANs will be temporarily disabled as a result of changes you are making.



Step 6: Review the Interface configuration.

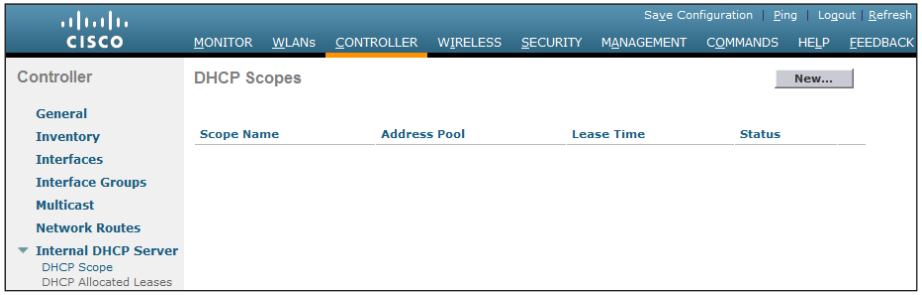


Step 7: Repeat this procedure on other WLCs in the mobility group.

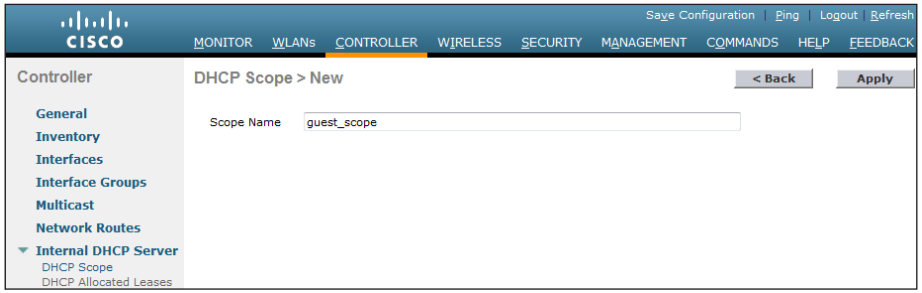
Procedure 2 Create Guest DHCP Scope

Configure a DHCP scope on the WLC's internal DHCP server.

Step 1: In **Controller > Internal DHCP Server > DHCP Scope**, click **New**.



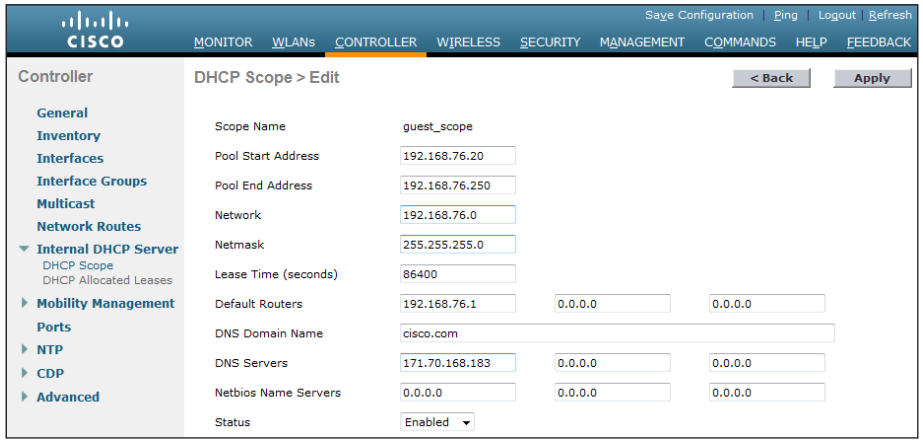
Step 2: In **Scope Name**, type **guest_scope** and then click **Apply**.



Step 3: On the **DHCP Scopes** page, click **guest_scope.**

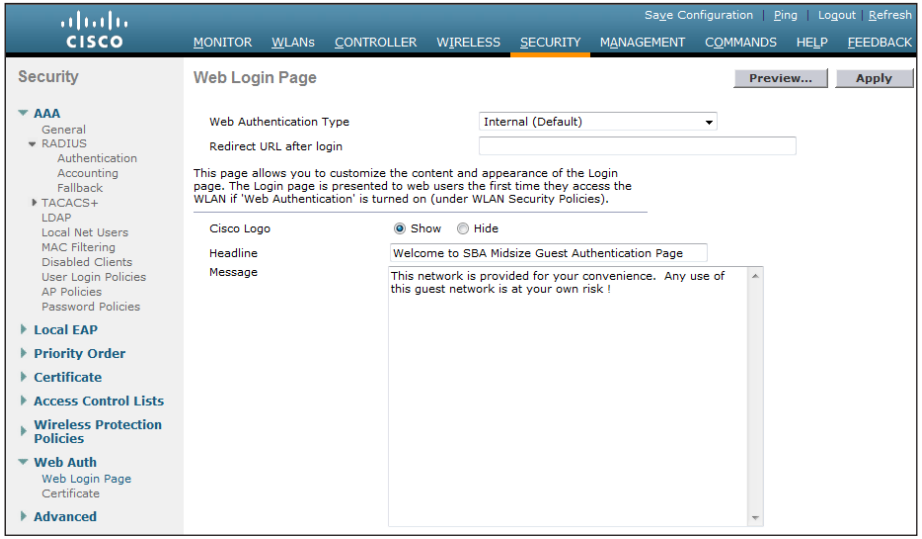
Step 4: Configure the following scope parameters, and then click **Apply**.

- Pool Start Address: 192.168.76.20
- Pool End Address: 192.168.76.250
- Network: 192.168.76.0
- Netmask: 255.255.255.0
- Lease Time (seconds): **86400** (This is the default 1 Day)
- Default Routers: 192.168.76.1(leave last two at 0.0.0.0)
- DNS Domain Name: **cisco.com** (Our external Service Provider)
- DNS Servers: 171.70.168.183 (Our Service Providers DNS Server)
- Status: **Enabled**

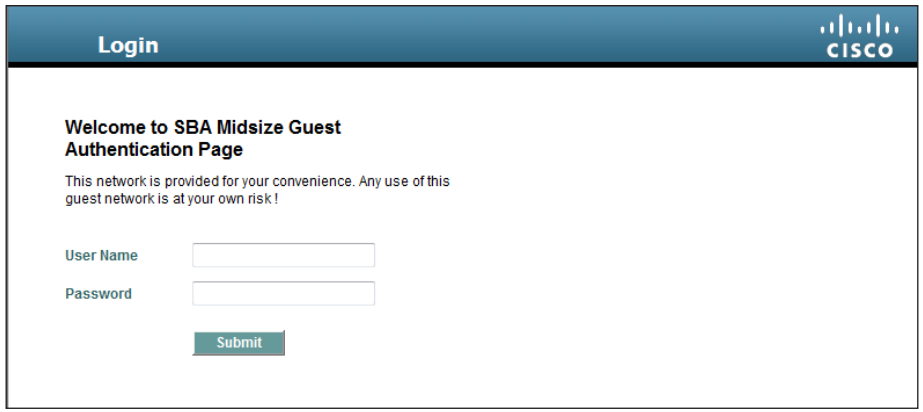


Step 5: Verify that the Guest_Scope in the scope summary is enabled and showing a **Lease Time** of **1 d** (one day).

Step 6: In **Security > Web Auth,** click **Web Login Page,** enter the appropriate information specific to your organization to advise users of the conditions of guest WLAN use, enter a redirection URL (for example, your company's web address or a guest portal page), and then click **Apply**.



Step 7: Confirm the page you have created by clicking **Preview**.



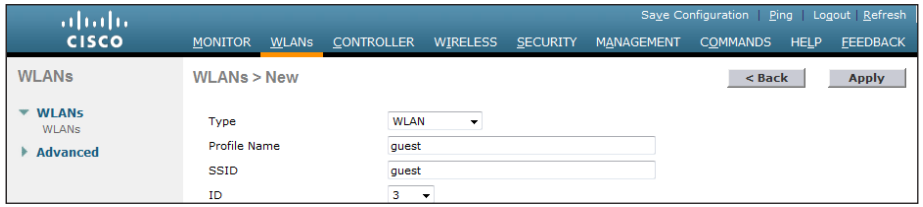
Step 8: Close the Preview window and repeat this procedure on other WLCs in the mobility group.

Procedure 3 Create Guest WLAN

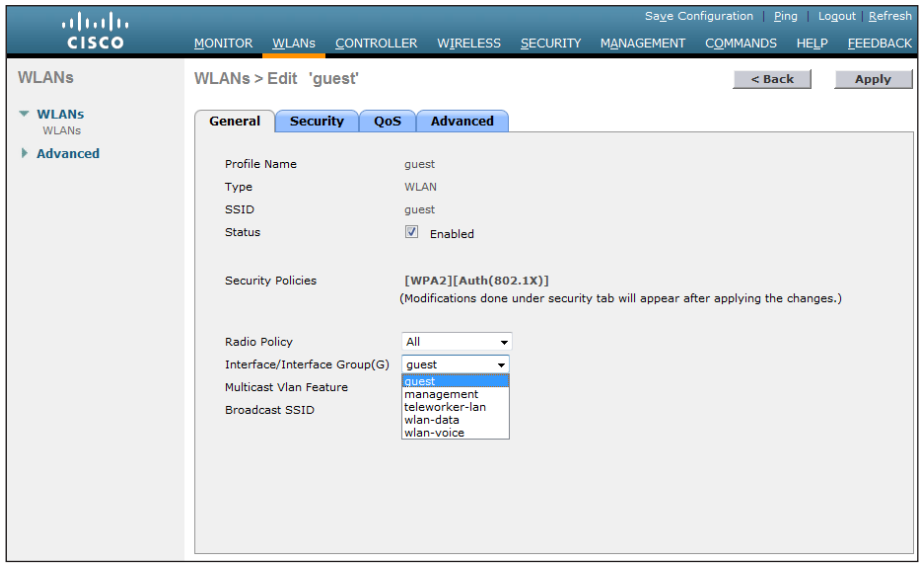
During the installation script, a temporary SSID of guest is created. You need to modify this SSID for your guest authentication.

Step 1: In **WLANs > WLANs**, select **Create New** from the list and then click **Go**.

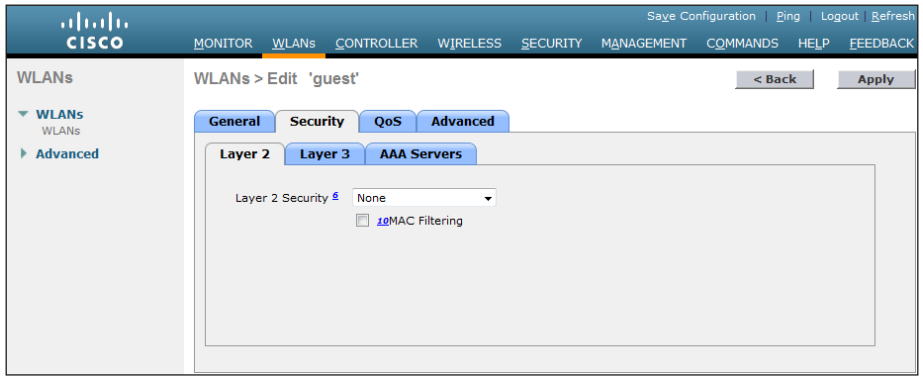
Step 2: On the New page, type **guest in Profile Name, guest in SSID**, keep the ID value in the list, and then click **Apply**.



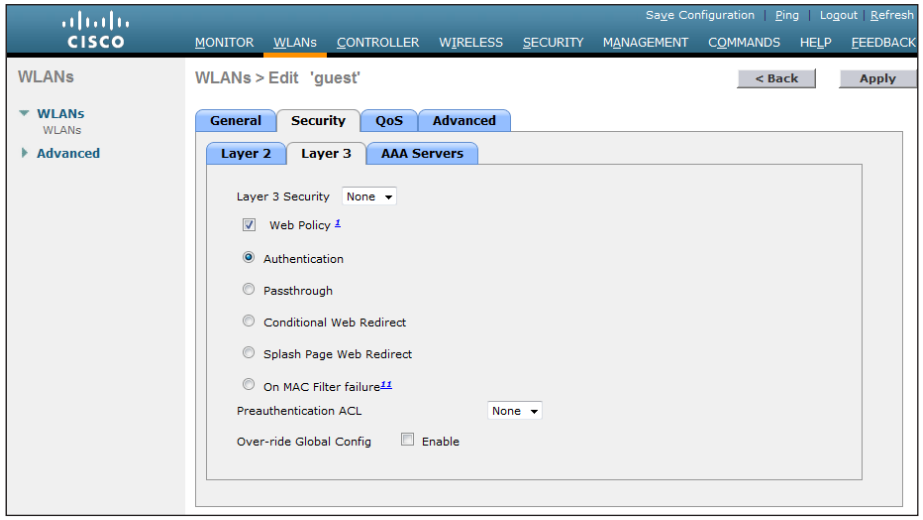
Step 3: On the **General** tab, select the **Status Enabled** check box and in the **Interface** list, select the **guest** interface you created previously.



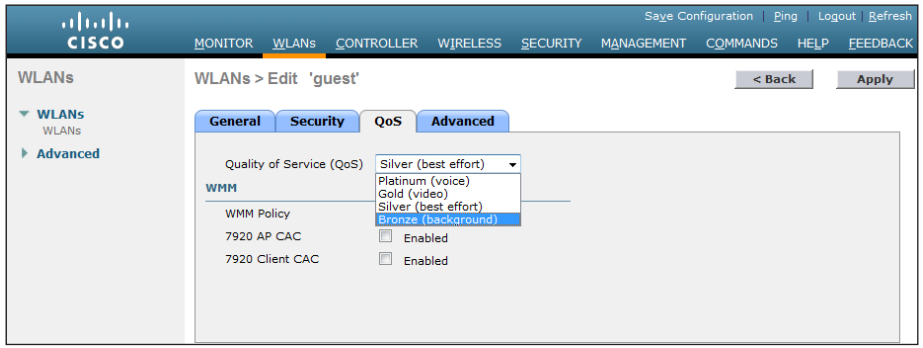
Step 4: Click the **Security** tab, click the **Layer 2** tab, and in the **Layer 2 Security** list, select **None**.



Step 5: Click the **Layer 3** tab, and in the **Layer 3 Security** list, select **None** , select the **Web Policy** check box, and then confirm that the **Authentication** option is selected.



Step 6: Click the **QoS** tab, and in the **Quality of Service (QoS)** list, select **Bronze (background)**.

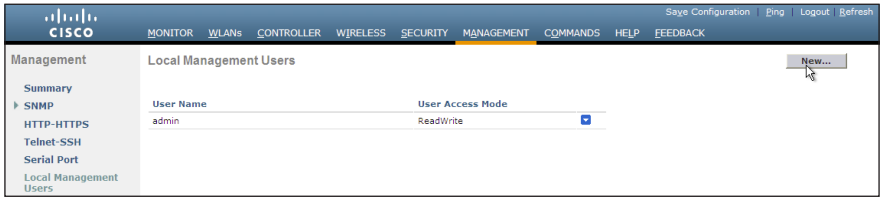


Step 7: Click **Apply** to finish.

Procedure 4 Create Guest-Admin Account

You can create guest user accounts with a separate lobby administrator account on the WLC. By doing this, you can allow guest user accounts to be created without contacting the network administration team.

Step 1: In **Management** > **Local Management Users**, click **New**.



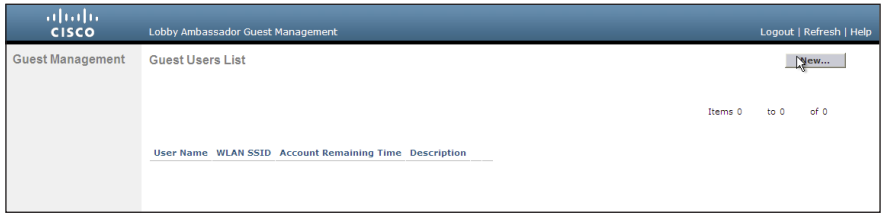
Step 2: Create the username **Guest-Admin**, enter the password **C1sco123** in both password fields, and change the **User Access Mode** to **LobbyAdmin**. Upon completion you should see your new user on the **Local Management Users** page.

Procedure 5 Create Guest Accounts

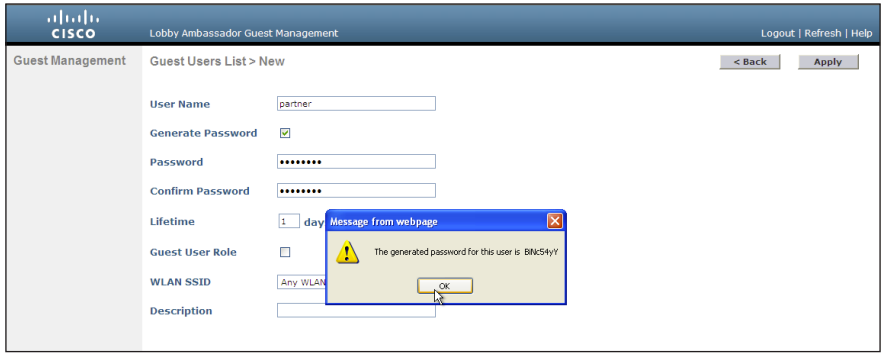
Now you can use the lobby administrator account to create usernames and passwords for partners, customers, and anyone else who is not normally granted access to your network.

Step 1: Using a web browser, open the WLC's web interface (for example, https://10.10.50.11/), and then log in using your LobbyAdmin account with the username **Guest-Admin** and password **C1sco123**.

Step 2: From the Lobby Ambassador Guest Management page, click **New**.



Step 3: Create a new username and password or allow the system to create a password automatically by selecting the **Generate Password** check box.



With a wireless client, you can now test connectivity to the Guest WLAN. Without any security enabled, you should receive an IP address, and after opening a web browser, be redirected to a web page to enter a username and password for Internet access, which will be available to a guest user for 24 hours.

Notes

Application Optimization Module

Business Overview

As an organization expands its presence to include new remote sites, additional network investment is required to allow remote-site users access to the same business applications and services available at the headquarters.

WAN connections are normally provisioned by a service provider, who charges a recurring cost for the bandwidth provided. Regardless of the WAN technology in use, service providers' charges increase as the provisioned bandwidth increases, so it is in the best interest of the organization to use this resource efficiently.

Maintaining consistent application response time for remote-site users can be a challenge with the delay introduced by WAN connections when applications are hosted at headquarters. Duplicating services locally at each remote site can be cost-prohibitive, requiring hardware, software, and additional staff to manage. Replicating data throughout an organization's sites increases security risks, because storing data in more sites increases the risk that the data will be compromised.

Technical Overview

Cisco application optimization technologies provide a way for organizations to improve user productivity, without buying additional bandwidth or hardware for remote sites. The performance improvements allow critical equipment and processes to remain centralized at the headquarters location, further reducing operating costs and improving data security.

Cisco application optimization technologies also help to protect your data by allowing centralization of application resources at the headquarters location. Proper data protection procedures can then be applied consistently across all of the organization's data by removing the need for separate backup and archival functions at the remote sites. The design allows remote-site users to experience similar performance levels for centralized application access as that of users working from the headquarters location.

By using the existing bandwidth more effectively, the organization can often add staff or new applications at a remote site without requiring additional bandwidth.

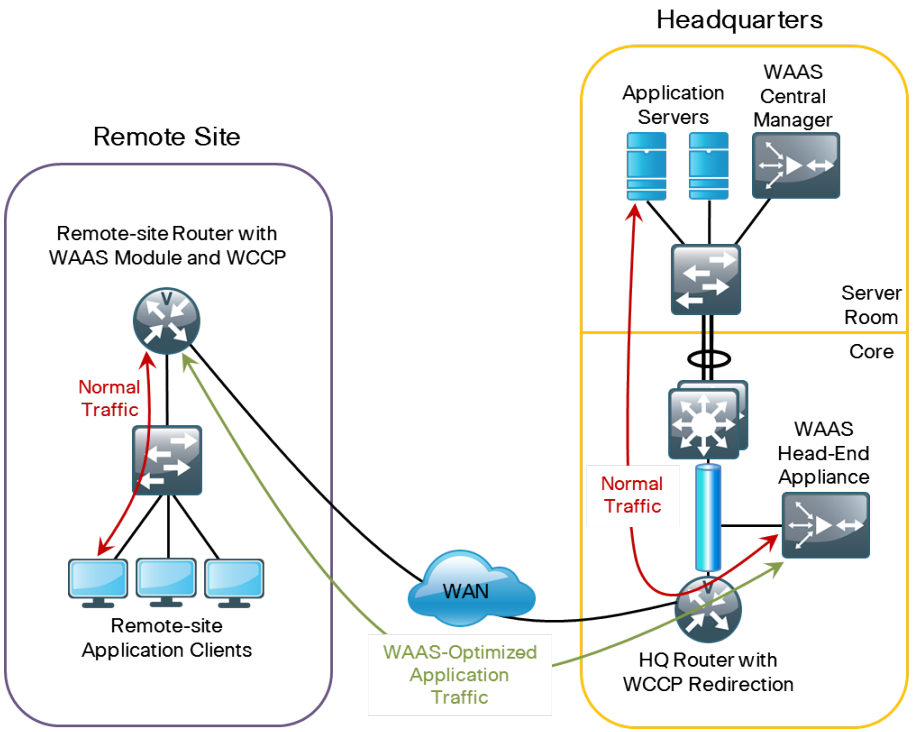
Cisco Wide Area Application Services (WAAS) is a comprehensive system designed to accelerate and optimize data over a WAN network.

Cisco WAAS Wide-Area Virtualization Engine (WAVE) appliances and router-integrated network modules (Cisco WAAS on Service-Ready Engine (SRE) provide right-sized options for deployment with the SBA).

WAAS uses multiple technologies to minimize the transmission of traffic between headquarters and remote sites, which reduces the consumption of WAN bandwidth as follows:

- Cisco WAAS Transport Flow Optimization (TFO) terminates a TCP session locally, optimizing flows that traverse the WAN and shielding end-user applications from WAN characteristics.
- Persistent Lempel-Ziv (LZ) compression saves 10-20 percent of the WAN bandwidth required for typical traffic profiles.
- Cisco WAAS provides additional bandwidth savings using Data Redundancy Elimination (DRE), which identifies redundant patterns in network data and eliminates the need to resend this data over the WAN. Depending on the application, DRE can reduce the traffic between the remote site and headquarters by 40–80 percent.
- Additional application-specific acceleration capabilities are also included in WAAS—capabilities approved by vendors of commonly used applications such as Microsoft Outlook and Windows file and printing services.

Figure 29 - Application Optimization: Cisco WAAS Components and Traffic Flow



The combination of the technologies included in Cisco WAAS may provide enough savings to allow additional applications such as voice and video to be deployed over an existing WAN, without incurring the cost of additional carrier bandwidth.

For this deployment, the headquarters location uses the WAVE-594 appliance to provide application optimization services as a central connection point for the remote sites. A separate Central Manager WAVE-294 appliance is used as a management, monitoring, and reporting point for the WAAS solution. If a physical appliance is not desired for the Central Manager, a virtualized vWAAS appliance can be deployed on an appropriate virtualized server infrastructure.

Additional details about the WAE sizing is provided in Table 11 The fan-out numbers correspond to the total number of remote-peer WAE devices.

Table 11 - WAN-Aggregation WAE Options

Device	Maximum optimized TCP connections	Maximum recommended WAN Link [Mbps]	Max core fan-out [Peers]
WAVE-594-8GB	750	50	50
WAVE-594-12GB	1300	100	100
WAVE-694-16GB	2500	200	150
WAVE-694-24GB	6000	200	300

Remote Sites

The remote sites use SRE, which integrates directly into the Cisco ISR G2 routers. There are two interfaces: one internal interface (router connect only) and one external interface.

The primary parameter of interest for performance sizing is the bandwidth of the WAN link. After the bandwidth requirement has been met, the next item to consider is the maximum number of concurrent, optimized TCP connections. Recommendations for WAE sizing are provided in Table 12 The optimized throughput numbers correspond to the apparent bandwidth available after successful optimization by Cisco WAAS.

Table 12 - WAN Remote-Site WAE Options

Device	Maximum simultaneous active users	Maximum recommended WAN link [Mbps]
SRE-700-S	20	20
SRE-700-M	50	20
SRE-900-S	20	50
SRE-900-M	50	50

WAE appliances use the Web Cache Communication Protocol (WCCP), a protocol developed by Cisco, to transparently intercept and redirect traffic from a network device to a WCCP appliance such as a WAE running Cisco WAAS. WCCP is enabled on the headquarters and remote-site WAN routers. The WCCP redirect uses service groups 61 and 62 to match traffic for redirection. These service groups must be used in pairs, where:

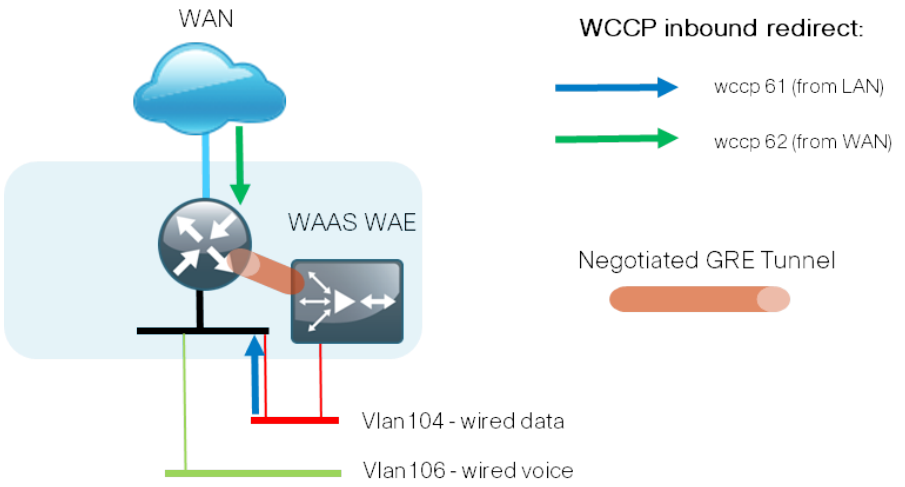
- Service group 61 uses the source address to redirect traffic
- Service group 62 uses the destination address to redirect traffic

This design uses WCCP 61 inbound on LAN-facing interfaces to match unoptimized data sourced from the data center that is destined for clients at the WAN remote sites. WCCP 62 is used inbound on WAN-facing interfaces, matching optimized data sourced from the WAN remote sites.

WCCP uses a GRE tunnel negotiated between the WAAS appliance or module and the originating router to return optimized traffic to the network. This method is preferred because it allows the WAE appliances to be located one or more routed hops away from the WCCP router. There are several benefits associated with this method, which are covered in more detail in the following sections.

The WAE devices should connect to the data VLAN of the access switch in all flat Layer 2 designs, as shown.

Figure 30 - WAN remote site, WAAS topology (access layer connection)



Deployment Details

The following process describes configuring and deploying a basic WAAS environment.

Process

Configuring the Cisco WAAS Central Manager

1. Configure Server Room Switch Access Port
2. Configure the WAAS Central Manager

The design deploys the Cisco WAAS Central Manager appliance in the server room, so the appliance is connected to the server-room switch.

Tech Tip

The Cisco WAAS Central Manager appliance does not require a resilient EtherChannel connection, because loss of connectivity to the appliance will not affect network function, and the appliance does not need the greater bandwidth offer by an EtherChannel connection.

Procedure 1 Configure Server Room Switch Access Port

This procedure assumes that you have already configured the server room switch. Only the steps required to complete the connection of the WAE appliance to the switch are included. You must create a VLAN and SVI for this and other devices with similar connectivity requirements. This VLAN is referred to as the WAN service network.

Step 1: Configure a switchport on the server-room switch as an access port to allow traffic to VLAN 150.

```
interface GigabitEthernet1/0/2
 description WAAS-CM
 switchport access vlan 150
 switchport mode access
 srr-queue bandwidth share 1 30 35 5
 queue-set 2
 priority-queue out
 mls qos trust dscp
 macro description EgressQoS
 spanning-tree portfast
```

Procedure 2 Configure the WAAS Central Manager

A Cisco WAVE-294 device or a vWAAS appliance is used for the Central Manager function at the primary location to provide graphical management, configuration, and reporting for the WAAS network. This device is connected to the server-room switch because it is not directly in the forwarding path of the WAN optimization but provides management and monitoring services. Initial configuration of the Central Manager requires terminal access to the console port for basic configuration options and IP address assignment. For all WAE devices, the factory default username is **admin** and the factory default password is **default**.

You can start the initial setup utility from the command line by entering the setup command.

Step 1: Connect the Cisco WAAS Appliance to the server-room switch, or install Cisco vWAAS on a virtualized server host.

Step 2: Run setup.

```
Parameter                 Default Value
1. Device Mode            Application Accelerator
2. Interception Method    WCCP
3. Time Zone              UTC 0 0
4. Management Interface   GigabitEthernet 1/0
5. Autosense              Enabled
6. DHCP                   Enabled
ESC Quit ? Help ———————— WAAS Default Configuration ————————
Press 'y' to select above defaults, 'n' to configure all, <1-
6> to change specific default [y]: n
```

Step 3: Configure it as Central Manager.

```
1. Application Accelerator
2. Central Manager
Select device mode [1]: 2
```

Step 4: Configure the time zone.

```
Enter Time Zone <Time Zone Hours(-23 to 23) Minutes(0-59)>
[UTC 0 0]: PST -8 0
```

Step 5: Configure the management interface, IP address, and default gateway.

```
No. Interface Name       IP Address    Network Mask
1.         GigabitEthernet 1/0                dhcp
2.         GigabitEthernet 2/0                dhcp
Select Management Interface [1]: 1
Enable Autosense for Management Interface? (y/n)[y]: y
Enable DHCP for Management Interface? (y/n)[y]: n
Enter Management Interface IP Address
<a.b.c.d or a.b.c.d/X(optional mask bits)> [Not configured]:
10.10.50.100/24
Enter Default Gateway IP Address [Not configured]: 10.10.50.1
```

Step 6: Configure the DNS server, host, and NTP settings.

```
Enter Domain Name Server IP Address [Not configured]:
10.10.48.10
Enter Domain Name(s) (Not configured): cisco.local
Enter Host Name (None): WAAS-CM
Enter NTP Server IP Address [None]: 10.10.48.17
```

Step 7: Select the appropriate license.

```
The product supports the following licenses:
1. Enterprise
Enter the license(s) you purchased [1]: 1
```

Step 8: Verify configuration settings and initiate reload.

```
Parameter                 Configured Value
1. Device Mode            Central Manager
2. Time Zone              PST -8 0
3. Management Interface   GigabitEthernet 1/0
4. Autosense              Enabled
5. DHCP                   Disabled
6. IP Address             10.10.50.100
7. IP Network Mask        255.255.255.0
8. IP Default Gateway     10.10.50.1
9. DNS IP Address         10.10.48.10
10. Domain Name(s)        cisco.local
11. Host Name             WAAS-CM
12. NTP Server Address    10.10.48.17
13. License               Enterprise
ESC Quit ? Help ! CLI ——— WAAS Final Configuration ————————
Press 'y' to select configuration, 'd' to toggle defaults
display, <1-13> to change specific parameter [y]: y
Apply WAAS Configuration: Device Mode changed in SETUP; New
configuration takes effect after a reload. If applicable,
registration with CM, CM IP address, WAAS WCCP configuration etc,
are applied after the reboot. Initiate system reload?
<y/n> [n] y
Are you sure? <y/n> [n]: y
```

Step 9: After the reboot, log in to the WAAS Central Manager and enable SSH. To enable SSH, you need to generate the RSA key and enable the sshd service.

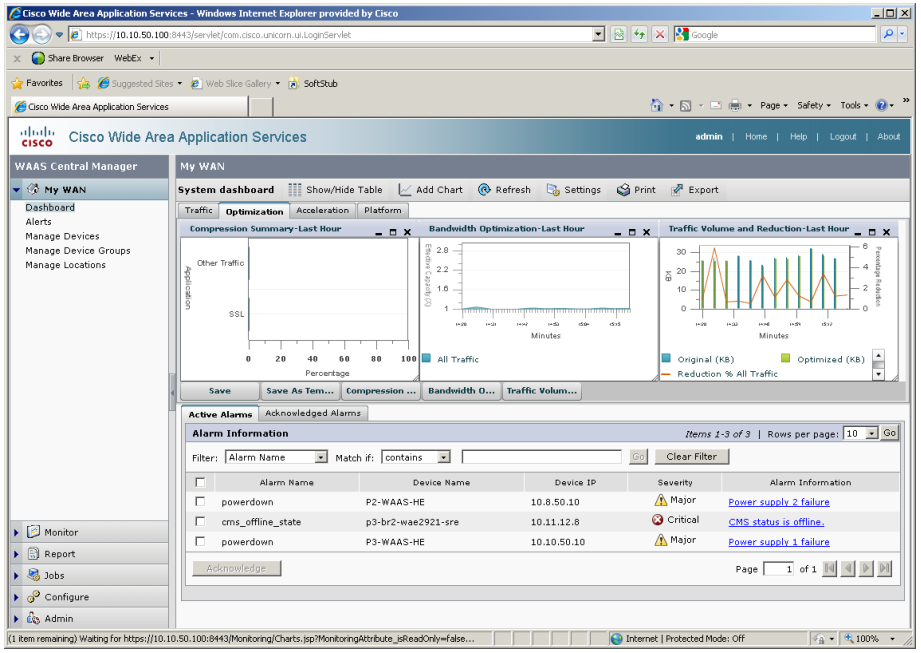
```
ssh-key-generate key-length 2048
sshd version 2
sshd enable
```

Step 10: Save the configuration after making changes through the console, and then reboot.

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

Step 11: Access the WAAS Central Manager through the web interface. After the reload completes, you can access the Central Manager device from a web browser at the IP address assigned during Step 4 of the setup utility (or at the associated hostname if it has been configured in DNS). To access the Central Manager, specify secure HTTP and the port number 8443 (for example, https://10.10.50.100:8443).

Step 12: Log in using the username **admin** and password **default** and then click **My WAN > Manage Devices** to display a screen showing the Central Manager initially as the only managed device.



Process

Configuring the WAAS Headend Appliances

1. Configure WAAS Downlinks on Core Switch
2. Configure the WAE Appliance Devices

Cisco WAAS Headend devices are connected directly to the core switch in the WAN Service VLAN (132).

Procedure 1 Configure WAAS Downlinks on Core Switch

Cisco WAAS Headend devices are connected directly to the core switch. Cisco WAAS devices (other than the Central Manager) require a resilient connection but do not require a routing protocol. This type of connection uses an access EtherChannel link to connect to the WAN Service VLAN (132).

Step 1: Assign interfaces to the EtherChannel port-group.

```
interface range GigabitEthernet1/2/22,GigabitEthernet2/2/22
  description Etherchannel to WAAS-HE Gi1/0
  switchport
  channel-group 31 mode on
```

Step 2: Define a port-channel interface with a number matching the channel-group on the physical interfaces.

```
interface Port-channel31
  description WAN Router
  switchport
  switchport access vlan 132
  switchport mode access
  spanning-tree portfast edge
  no shutdown
```

Tech Tip

4507 and 3750X core switches only require the **spanning-tree portfast** command.

Procedure 2 Configure the WAE Appliance Devices

A WAE-694 appliance provides the headend termination for WAAS traffic to and from the remote-sites across the WAN. These devices are connected to the core switch, leveraging GRE-negotiated return to communicate with the WCCP routers.

The same setup utility used in the initial configuration of the WAAS Central Manager is used for the setup of the WAE appliance devices. These devices only require basic setup through their console port to assign initial settings; initial setup of the WAE application defines basic configuration options and IP address assignment. For all WAE devices, the factory default username is **admin** and the factory default password is **default**.

After you complete initial setup, all management of the WAAS network can be performed through the graphical interface of the WAAS Central Manager system.

The setup utility configuration steps for the application accelerator WAEs are similar to the setup of the Central Manager, but the steps begin to differ after you choose application-accelerator as the device mode in Step 2. After you select the mode, the setup script changes to allow you to register the WAE with the existing Central Manager and define the traffic interception method as WCCP.

Step 1: Run setup. You can start the initial setup utility from the command line by entering the setup command.

```
Parameter                 Default Value
1. Device Mode            Application Accelerator
2. Interception Method    WCCP
3. Time Zone              UTC 0 0
4. Management Interface   GigabitEthernet 1/0
5. Autosense              Enabled
6. DHCP                   Enabled
ESC Quit ? Help ———————— WAAS Default Configuration ————————
Press 'y' to select above defaults, 'n' to configure all, <1-
6> to change specific default [y]: n
```

Step 2: Configure it as an application accelerator.

```
1. Application Accelerator
2. Central Manager
Select device mode [1]: 1
```

Step 3: Configure the interception method.

```
1. WCCP
2. Other
Select Interception Method [1]: 1
```

Step 4: Configure the time zone.

```
Enter Time Zone <Time Zone Hours(-23 to 23) Minutes(0-59)>
[UTC 0 0]: PST -8 0
```

Step 5: Configure the management interface, IP address, and default gateway.

```
No.         Interface Name       IP Address    Network Mask
1. GigabitEthernet 1/0           dhcp
2. GigabitEthernet 2/0           dhcp
Select Management Interface [1]: 1
Enable Autosense for Management Interface? (y/n)[y]: y
Enable DHCP for Management Interface? (y/n)[y]: n
Enter Management Interface IP Address
<a.b.c.d or a.b.c.d/X(optional mask bits)> [Not configured]:
10.10.32.10/25
Enter Default Gateway IP Address [Not configured]: 10.10.32.1
Enter Central Manager IP Address (WARNING: An invalid entry
will cause SETUP to take a long time when applying WAAS
configuration) [None]: 10.10.50.100
```

Step 6: Configure the DNS server, host, and NTP settings.

```
Enter Domain Name Server IP Address [Not configured]:
10.10.48.1
Enter Domain Name(s) (Not configured): cisco.local
Enter Host Name (None): WAAS-HE
Enter NTP Server IP Address [None]: 10.10.48.17
```

Step 7: Configure the WCCP router list (values here can be arbitrary; the configuration will be modified in later steps).

```
Enter WCCP Router (max 4) IP Address list (ip1 ip2 ...) []:
10.10.32.126
```

Step 8: Select the appropriate license.

```
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]: 2
```

Step 9: Verify the configuration settings.

```
Parameter                 Configured Value
2. Interception Method    WCCP
3. Time Zone              PST -8 0
4. Management Interface   GigabitEthernet 1/0
5. Autosense              Enabled
6. DHCP                   Disabled
7. IP Address             10.10.50.10
8. IP Network Mask        255.255.255.0
9. IP Default Gateway     10.10.50.1
10. CM IP Address         10.10.50.100
11. DNS IP Address        10.10.48.10
12. Domain Name(s)        cisco.local
13. Host Name             bn-wae7341-1
14. NTP Server Address    10.10.48.17
15. WCCP Router List      10.10.50.1
16. License               Enterprise
ESC Quit ? Help ! CLI ——— WAAS Final Configuration ———
Press 'y' to select configuration, <F2> to see all
configuration, 'd' to toggle defaults display, <1-16> to
change specific parameter [y]: y
Applying WAAS configuration on WAE ...
May take a few seconds to complete ...
```

The setup dialog displays a failure message because the WAE setup script does not enable the port-channel. An intermediate step is required to change the interface configuration, and then you complete registration with the Cisco WAAS Central Manager manually in Step 11.

Step 10: Configure the port-channel connection for WAE to connect to the core switch.

```
interface GigabitEthernet 1/0
  no ip address
exit
!
primary-interface PortChannel 1
!
interface PortChannel 1
ip address 10.10.32.10 255.255.255.128
exit
!
interface GigabitEthernet 1/0
description sr-3750 G1/0/44
channel-group 1
exit
interface GigabitEthernet 2/0
description sr-3750 G2/0/44
channel-group 1
exit
```

Step 11: Complete registration with WAAS Central Manager. After the port-channel has been configured, the WAE can reach the WAAS Central Manager. Run the **cms enable** command to force a manual registration.

```
cms enable
Registering WAAS Application Engine...
Sending device registration request to Central Manager with
address 10.10.50.100
Please wait, initializing CMS tables
Successfully initialized CMS tables
Registration complete.
Please preserve running configuration using 'copy running-
config startup-config'.
Otherwise management service will not be started on reload and
node will be shown 'offline' in WAAS Central Manager UI.
management services enabled
```

To complete the Cisco WAAS configuration, you must change several additional settings on the WAE devices must be changed from the default configuration. These settings are configured in Steps 13 through 15.

Step 12: Configure GRE negotiated return. All WAE devices use GRE-negotiated return with their respective WCCP routers.

```
egress-method negotiated-return intercept-method wccp
```

Step 13: Configure the WCCP router list. The setup script generated a router list based on the information provided. To view the device configuration, enter the following command.

```
WAAS-HE# show running-config | include wccp router-list
wccp router-list 8 10.10.50.10
```

Router list 8 is specifically used with WCCP configured on a default gateway router. This design uses GRE-negotiated return to the WAN routers core uplink Ethernet address, so we need to create a new router list and delete router list 8.

All WAE configurations in this design use router list 1.

```
no wccp router-list 8 10.10.50.10
wccp router-list 1 10.10.32.126
```

This design uses authentication between the routers and WAE. You make this change on the WAEs, not on the routers.

```
wccp tcp-promiscuous router-list-num 1 password c1sco123
```

Step 14: Enable SSH and disable telnet. To enable SSH, you need to generate the RSA key and enable the sshd service.

```
ssh-key-generate key-length 2048
sshd version 2
sshd enable
no telnet enable
```

Step 15: Save the configuration after making changes through the console, and then reload the WAE.

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

Process

Configuring the Cisco WAAS Remote-Site Appliances

1. Configure Switches for WAE Connection
2. Configure the WAE SRE Devices

This process must be applied at every remote site that uses a WAE device to optimize traffic across the WAN. The WAE devices at the remote site are connected to the access switch, instead of using the internal interface between the router and the WAE module. This offers simplified configuration and reduces address assignment complexity at the remote site.

Procedure 1 Configure Switches for WAE Connection

This guide assumes that the remote-site access switch has already been configured. Only the procedures required to complete the connection of the switch to the WAE appliances are included.

This design locates the WAE devices on the data (primary) VLAN.

Step 1: Connect the WAE's external Ethernet port to an Ethernet port on the remote site's access switch, and return the switchport configuration to the default.

```
default interface GigabitEthernet1/0/3
```

Step 2: Define the switchport in the remote-site access switch as an access port for the data VLAN, and apply port-security and QoS configuration.

```
interface GigabitEthernet1/0/3
  description ** WAAS Connection **
  switchport access vlan 64
  switchport mode access
  ip arp inspection trust
  srr-queue bandwidth share 1 30 35 5
  queue-set 2
  priority-queue out
  mls qos trust dscp
  spanning-tree portfast
  spanning-tree bpduguard enable
  no shutdown
```

Procedure 2 Configure the WAE SRE Devices

The remote-site Cisco WAAS equipment in this design is one of the SRE variants, depending on the performance requirements.

The SRE module can be inserted directly into a corresponding module slot in the remote-site router and are configured somewhat differently from the appliances.

Although the remote-site router can potentially communicate directly with the SRE using the router backplane, this design leverages the external interfaces on the modules, which allows for a consistent design implementation regardless of the chosen WAE device. You must enable the integrated-service-engine interface and assign an arbitrary (locally significant only) IP address in order to access the WAAS SRE through a console session from the host router.

Step 1: Configure console access and SRE IP addresses on the host router. To permit console access to SRE modules, you must enter the following commands on the host router.

```
interface SM1/0
ip address 1.1.1.1 255.255.255.252
service-module external ip address 10.11.4.8 255.255.255.0
service-module ip default-gateway 10.11.4.1
no shutdown
```

Step 2: Connect to the WAE console using a session from the host router. After the IP address is assigned, and the interface is enabled, it is possible to open a session on the WAE and run the setup script. For all WAE devices, the factory default username is **admin** and the factory default password is **default**.

```
Br1-2921# service-module sm 1/0 session
```

Step 3: Run setup. You can start the initial setup utility from the command line by entering the setup command.

```
Parameter                 Default Value
Device Mode               Application Accelerator
1. Interception Method    WCCP
2. Time Zone              UTC 0 0
3. Management Interface   GigabitEthernet 1/0       (internal)
Autosense                 Disabled
DHCP                      Disabled
ESC Quit ? Help ———————— WAAS Default Configuration ————————
Press 'y' to select above defaults, 'n' to configure all, <1-
3> to change specific default [y]: n
```

Step 4: Configure the interception method.

```
1. WCCP
2. Other
Select Interception Method [1]: 1
```

Step 5: Configure the time zone.

```
Enter Time Zone <Time Zone Hours(-23 to 23) Minutes(0-59)>
[UTC 0 0]: PST -8 0
```

Step 6: Configure the management interface, IP address, and default gateway. This design uses the external interface as the management interface.

```
No. Interface Name       IP Address    Network Mask
1.  GigabitEthernet 1/0  unassigned    unassigned     (internal)
2.  GigabitEthernet 2/0  dhcp                         (external)
Select Management Interface [1]: 2
Enable Autosense for Management Interface? (y/n)[y]: y
Enable DHCP for Management Interface? (y/n)[y]: n
```

Tech Tip

You may receive the following warning. You may disregard this warning; the IP address configuration was provided previously.

```
*** You have chosen to disable DHCP! Any network
configuration learnt from DHCPserver will be
unlearnt! SETUP will indicate failure as the
management interface cannot be brought up - Please
make sure WAE Management Interface IPaddress and
Default Gateway are configured from the Router;
Press ENTER to continue:
```

```
Enter Central Manager IP Address (WARNING: An invalid entry
will cause SETUP to take a long time when applying WAAS
configuration) [None]: 10.10.50.100
```

Step 7: Configure the DNS server, host, and NTP settings.

```
Enter Domain Name Server IP Address [Not configured]:
10.10.48.10
Enter Domain Name(s) (Not configured): cisco.local
Enter Host Name (None): Br1-WAE-SRE
Enter NTP Server IP Address [None]: 10.10.48.17
```

Step 8: Configure the WCCP router list.

```
Enter WCCP Router (max 4) IP Address list (ip1 ip2 ...) []:
10.11.4.1
```

Step 9: Select the appropriate license.

```
The product supports the following licenses:
1. Transport
2. Enterprise
3. Enterprise & Video
Enter the license(s) you purchased [2]: 2
```

Step 10: Verify the configuration settings.

```
Parameter                 Configured Value
1. Interception Method    WCCP
2. Time Zone              PST -8 0
3. Management Interface   GigabitEthernet 2/0 (external)
4. Autosense              Enabled
5. DHCP                   Disabled
   IP Address             10.11.4.8
   IP Network Mask        255.255.255.0
   IP Default Gateway     10.11.4.1
6. CM IP Address          10.10.50.100
7. DNS IP Address         10.10.48.10
8. Domain Name(s)         cisco.local
9. Host Name              p3-br1-wae-sre
10. NTP Server Address    10.10.48.17
11. WCCP Router List      10.11.4.1
12. License               Enterprise
ESC Quit ? Help ! CLI ———— WAAS Final Configuration ————
Press 'y' to select configuration, <F2> to see all
configuration, 'd' to toggle defaults display, <1-12> to
change specific parameter [y]: y
Router WCCP configuration
First WCCP router IP in the WCCP router list seems to be an
external address; WCCP configuration on external routers is
not allowed through SETUP. Please press ENTER to apply WAAS
configuration on WAE ...
Applying WAAS configuration on WAE ...
May take a few seconds to complete ...
WAAS configuration applied successfully!!
Saved configuration to memory.
Press ENTER to continue ...
```

Tech Tip

You will be prompted with a recommended router WCCP configuration template. This router configuration is not correct, because the SBA WAAS implementation uses GRE return. The correct steps are described in depth in a later procedure, so you do not need to retain this information.

When this configuration is complete, enter the escape sequence, CTRL-Shift-6-x, to return the session to the command line.

Step 11: Configure GRE negotiated return. All WAE devices use GRE-negotiated return with their respective WCCP routers.

```
egress-method negotiated-return intercept-method wccp
```

Step 12: Configure WCCP router list. The set up script generated a router list based on the information provided. To view the device configuration, enter the following command.

```
Br1-WAE-SRE# show running-config | include wccp router-list
wccp router-list 8 10.11.4.1
```

Router list 8 is specifically for use with WCCP configured on a default gateway router. This design uses GRE-negotiated return and router loopback addresses (as defined in the WAN section of this document), so we need to create a new router list and delete router list 8.

All WAE configurations in this design use router list 1.

```
no wccp router-list 8 10.11.4.1
wccp router-list 1 10.11.0.1
```

This design uses authentication between the routers and the WAEs.

```
wccp tcp-promiscuous router-list-num 1 password c1sco123
```

Step 13: Enable SSH and disable telnet,. To enable SSH, you need to generate the RSA key and enable the sshd service.

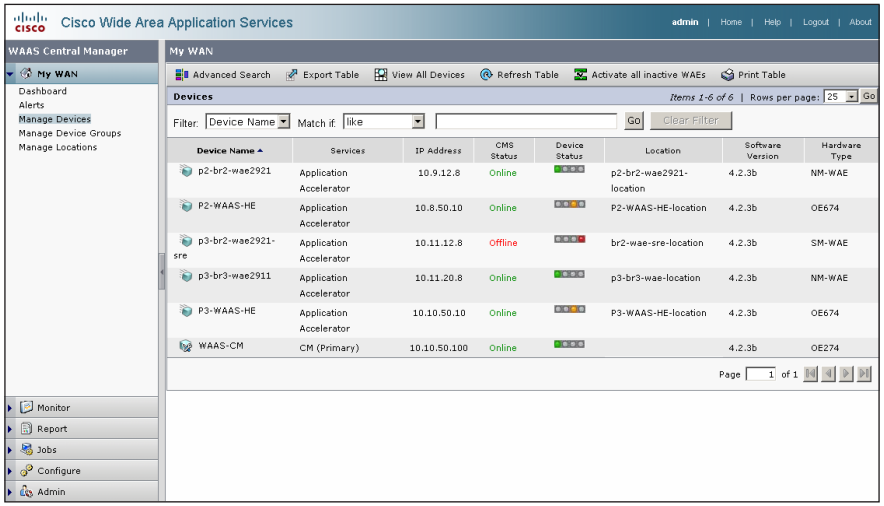
```
ssh-key-generate key-length 2048
sshd version 2
sshd enable
no telnet enable
```

Step 14: Save the configuration.

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

Each WAE registers with the Cisco WAAS Central Manager as they become active on the network. You can verify this registration by using the **show cms info** command on the respective WAE or via the web interface to the WCM.

Figure 31 - Verify Cisco WAAS Registration in Central Manager



Process

Configuring WCCP on the WAN Routers

1. Configure WCCP

This process describes configuring WCCP Version 2 on the WAN-Aggregation and WAN remote-site routers. This design uses WCCP to divert network traffic destined for the WAN to the Cisco WAAS system for optimization. This method provides for a clean deployment with minimal additional cabling and requires that you configure both the WAN-aggregation and remote-site routers for WCCP.

Procedure 1 Configure WCCP

Step 1: Configure global WCCP parameters and enable services 61 and 62. Services 61 and 62 must be enabled for WCCP redirect for Cisco WAAS. These services should be using WCCP Version 2. As a best practice, exempt certain critical traffic types from WCCP redirect by using a redirect list.

To prevent unauthorized WAE devices from joining the Cisco WAAS cluster, you should configure a group-list and password.

```
ip wccp version 2
ip wccp 61 redirect-list WAAS-REDIRECT-LIST group-list BN-WAE
password ***password***
ip wccp 62 redirect-list WAAS-REDIRECT-LIST group-list BN-WAE
password ***password***
ip access-list standard BN-WAE
permit 10.11.4.8
!
ip access-list extended WAAS-REDIRECT-LIST
remark WAAS WCCP Mgmt Redirect List
deny       tcp any any eq 22
deny       tcp any eq 22 any
deny       tcp any any eq 123
deny       tcp any eq 123 any
permit     tcp any any
```

Step 2: Configure WCCP redirect on the LAN interfaces. Specific interfaces must be identified where traffic to and from the WAN are intercepted. Traffic from the LAN is intercepted with service 61 inbound on all LAN interfaces. It is not necessary to configure WCCP interception on voice interfaces and voice VLANs.

If LAN interfaces are configured in an EtherChannel port-group (as on the headquarters router), define WCCP redirection on the port-channel interface.

```
interface Port-channel1
  ip wccp 61 redirect in
```

If LAN interfaces are VLAN trunks, define WCCP redirection on the data VLAN subinterface.

```
interface GigabitEthernet0/2.64
  description Wired Data
  ip wccp 61 redirect in
```

Step 3: Traffic from the WAN is intercepted with service 62 inbound on all WAN interfaces.

```
interface GigabitEthernet0/0
  description MPLS WAN Uplink
  ip wccp 62 redirect in
```

Application Optimization Summary

Cisco WAAS provides multiple traffic optimization technologies to accelerate applications over the WAN. In this Deployment Guide section we covered the basic configuration needed to add Cisco WAAS capabilities to a network built using the SBA. Cisco WAAS also has specific templates and customizable settings for many applications not covered in this guide. For more information, please consult your Cisco representative, authorized Channel Partner, or www.cisco.com.

Cisco WAAS Configuration Checklist

This table specifies the different parameters and data that you need to set up and configure the Cisco WAAS network. For your convenience, you can enter your values in the table and refer to it when configuring the Cisco WAAS network. The values you enter will differ from those in this example, which are provided for demonstration purposes only.

Table 13 - Cisco WAAS network system parameters checklist

Parameter	Cisco WAAS Central Manager values	Main office Cisco WAE values	Branch office Cisco WAE values*
Interface Speed	Default	Default	Default
IP Address	10.10.50.100	10.10.32.10	10.11.4.8
Subnet Mask	255.255.255.0	255.255.255.0	255.255.255.0
Default Gateway	10.10.50.1	10.1.32.1	10.11.4.1
DNS Server 1	10.10.48.10	10.10.48.10	10.10.48.10
DNS Server 2	[optional]	[optional]	[optional]
DNS Domain	cisco.local	cisco.local	cisco.local
Cisco WAAS Device (Hostname)	waas-cm	waas-he	p3-br1-wae-sre
IP Addresses of Routers Intercepting Traffic with WCCP		10.10.32.126	10.11.0.1
NTP Server	10.10.48.17	10.10.48.17	10.10.48.17
Time Zone	PST	PST	PST

* You will need one column for each branch office.

Notes

Server Load Balancing Module

Business Overview

The network is playing an increasingly important role in the success of an organization. Key services such as e-commerce, email, and web applications must be available without interruption around the clock. However, the availability of these applications is often threatened by network overloads as well as server and application failures. Furthermore, resource use is often out of balance, resulting in some systems being overloaded with requests while others remain idle. Application performance and availability directly affect employee productivity and the bottom line of an organization.

It is common for midsize organizations to run an application on a single server. As the use of the service grows or becomes more critical to the organization, the need to run the application on multiple servers can arise. This creates an issue because most applications do not handle distribution across multiple systems well natively. One possibility is to rewrite the application to make it network-optimized. However, this requires application developers to have a deep understanding of how different applications respond to things such as bandwidth constraints, delay, jitter, and other network variances. In addition, developers need to accurately predict each end-user's foreseeable access method. This is simply not feasible for every business application, especially applications that have been written and customized over many years.

Technical Overview

The idea of improving application performance began in the data center. The Internet boom ushered in the era of the server load balancers. The primary role of server load balancers is to balance application load across servers to improve the response to client requests, but they have evolved to taking on additional functionality such as application proxies and Layer 4 through 7 application switching.

Cisco ACE is the next-generation application delivery controller that provides server load balancing (SLB), SSL offload, and application acceleration capabilities. There are four key benefits provided by Cisco ACE:

- Scalability—The engine 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.
- High availability—The engine provides high availability by automatically detecting the failure of a server and repartitioning client traffic among remaining servers within seconds, providing users with continuous service.
- Application acceleration—The engine improves application performance and reduces response time by minimizing latency and data transfers for any HTTP-based application, for internal or external users.
- Server offload—The engine can offload TCP and SSL processing, allowing more users to be served without increasing the number of servers.

You always deploy Cisco ACE hardware in pairs for high availability: one primary and one secondary. If the primary engine fails, the secondary engine takes control. Depending on how you configure session-state redundancy, 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 engine rapidly detects 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.

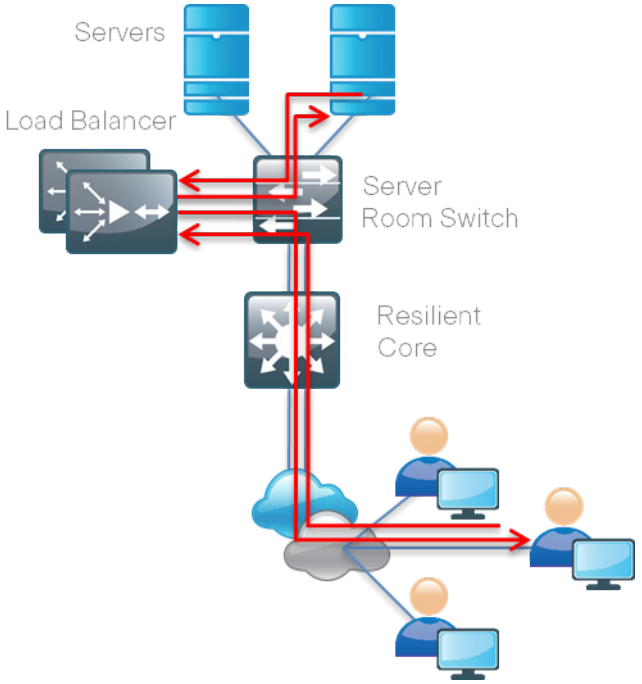
You can use Cisco ACE for a number of more advanced services that are not covered in the basic configuration, but are worth mentioning. Cisco ACE:

- Can 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 servers, allowing the application to scale very efficiently.
- Maximizes cache coherency by keeping requests for the same pages on the same servers.
- May be used to push requests for cacheable content, such as image files, to caches that can serve them more cost-effectively than servers.
- Can offload SSL processing with specialized hardware that is more efficient and requires fewer SSL certificates than the servers.
- Reduces the amount of data sent from the web application server to the browser by using hardware compression and only sending parts of the page that have changed since the last request.
- Further improves the end-user application experience by reducing latency and the number of round trips required for application access by eliminating unnecessary browser cache validation requests. The engine also provides automatic embedded object version management at the server, resulting in significantly improved response times for users.

There are several ways to integrate Cisco ACE into the server room. Logically, the engine is deployed in front of the web application cluster. Requests to the cluster are directed to a virtual IP address (VIP) configured on the engine. The engine 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 and is what Cisco uses in the SBA design (). Cisco ACE is connected to the server room switch with interfaces in the same VLAN as the servers that are being load balanced. It is not directly in the data path and only receives traffic directed at the VIP for load balancing. Access to the real IP addresses in the server room is not affected.

Figure 32 - Cisco ACE load-balancer topology



Deployment Details

In this deployment example, you first configure the Cisco ACE appliance with the required parameters to be recognized on the network. Then, you define the policies for directing the traffic. Although the first part of the configuration is typically performed at the CLI when you boot the appliance, you can configure both parts via the Cisco ACE GUI.

Process

Configuring Cisco ACE

1. Apply Initial and Global Configuration
2. Configure a Load-Balancing Policy

This guide uses the CLI commands for both network and application policy configuration.

Procedure 1 Apply Initial and Global Configuration

Step 1: Connect a console cable to the Cisco ACE appliance to perform initial configuration of the admin user, and then exit from the initial configuration dialog box at the prompt.

```
switch login: admin
Password: admin
Admin user is allowed to log in only from console until the
default password is changed.
www user is allowed to log in only after the default password
is changed.
Enter the new password for user "admin":
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 Cisco ACE.

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

Step 3: Ethernet VLAN trunks to the network's switching resources connect the Cisco ACE appliances. Configure two Gigabit Ethernet ports on each appliance to trunk to the server room switch.

```
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 148
  no shutdown
```

You must configure the switch ports that connect to the security appliances so that they are members of the same secure VLANs and they forward secure traffic to switches that offer connectivity to servers and other devices in the server room.

You need to configure the Cisco ACE appliances for active-standby high availability.

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 heartbeats, configuration sync packets, and state replication packets). Apply the following configuration to the first appliance.

```
ft interface vlan 12
  ip address 10.255.255.1 255.255.255.0
  peer ip address 10.255.255.2 255.255.255.0
  no shutdown
ft peer 1
  heartbeat interval 300
  heartbeat count 10
  ft-interface vlan 12
ft group 1
  peer 1
  peer priority 110
  associate-context Admin
  inservice
```

You need to configure the FT to be repeated on the second appliance, with the values for IP and peer IP addresses swapped.

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

```
interface vlan 148
  ip address 10.10.48.119 255.255.255.0
  peer ip address 10.10.48.120 255.255.255.0
  access-group input ALL
  nat-pool 1 10.10.48.99 10.10.48.99 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 10.10.48.1
```

At this point, the engine should be reachable on the network. Now you can configure a load-balancing policy. If you are configuring a second appliance for high availability, repeat Step 5, swapping the values for the IP and peer IP addresses.

Procedure 2 Configure a Load-Balancing Policy

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

```
rserver host webserver1
  ip address 10.10.48.111
  inservice
rserver host webserver2
  ip address 10.10.48.112
  inservice
```

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

```
probe http http-probe
  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-any http-vip
  2 match virtual-address 10.10.48.100 tcp eq www
policy-map type loadbalance first-match http-vip-l7slb
  class class-default
    serverfarm webfarm
policy-map multi-match int148
  class http-vip
    loadbalance vip inservice
    loadbalance policy http-vip-l7slb
    loadbalance vip icmp-reply active
    nat dynamic 1 vlan 148
interface vlan 148
  service-policy input int148
```

At this point, the application is accessible via the VIP (10.10.48.100) and the requests are distributed between the two web servers.

Summary

IT organizations face significant challenges associated with the delivery of applications and critical business data with adequate service levels to a globally distributed workforce. Application-delivery technologies help IT organizations improve availability, performance, and security.

Notes

Appendix A: Midsize Organizations Deployment Product List

Functional area	Product	Part numbers	Software version
100-600 Network Core	Cisco Catalyst 3750-X Stackable 12 & 24 Port SFP and IP Services Image	WS-C3750X-12S-E WS-C3750X-24S-E	15.0(1)SE1
600-1000 Network Core	Cisco Catalyst 4507RE 7-Slot Chassis, fan, no ps, Red Sup Capable Cisco Catalyst 4500 E-Series 24-Port GE (SFP) Dual supervisors and dual power supplies	WS-C4507R+E Catalyst 4500 E-Series WS-X45-SUP7-E WS-X4712-SFP+E WS-X4648-RJ45-E WS-X4624-SFP-E	15.0(2)SG1 CAT4500E SUP7e Universal Crypto Image
1000-2500 Network Core	Cisco Catalyst 6500VSS; Two each of every component	WS-C6504-E VS-S720-10G WS-X6716-10GE WS-X6748-SFP	12.2(33)SXI7

Functional area	Product	Part numbers	Software version
Headquarter access for PC, phones, APs, other devices	Cisco Catalyst 4507R+E Dual supervisors (or single supervisor for lower cost) Dual power supplies	WS-C4507R+E WS-X45-SUP7L-E Catalyst 4500 E-Series Supervisor LE, 520Gbps WS-X4648-RJ45V+E	15.0(2)XO
	Cisco Catalyst 3750-X Stackable 24 &48 Ethernet 10/100/1000 ports with PoE+ and IP Base. Uplink Module is optional.* *Optional 3750-X 4xSFP Uplink Module	WS-C3750X-24P-S WS-C3750X-48PF-S C3KX-NM-1G	15.0(1)SE1
	Cisco Catalyst 3560-X Standalone 24 & 48 Ethernet 10/100/1000 ports with PoE+ and IP Base. Uplink Module is optional.* *Optional 3560-X 4xSFP Uplink Module	WS-C3560X-24P-S WS-C3560X-48PF-S C3KX-NM-1G	15.0(1)SE1
	Cisco Catalyst 2960-S Stackable** 24 & 48 Ethernet 10/100/1000 ports with PoE+,LAN Base, 4 SFP ports. Stacking Module is optional.** **Optional 2960-S FlexStack Stack Module	WS-C2960S-24PS-L WS-C2960S-48FPS-L C2960S-STACK	15.0(1)SE1
Server Room Switch	Cisco Catalyst 3750-X Stackable 24 &48 Ethernet 10/100/1000 ports with IP Base. Uplink Module is optional.* *Optional 3560-X or 3750-X 4xSFP Uplink Module	WS-C3750X-24T-S WS-C3750X-48T-S C3KX-NM-1G	15.0(1)SE1
	Cisco Catalyst 3560-X Standalone 24 & 48 Ethernet 10/100/1000 ports with IP Base. Uplink Module is optional.* *Optional 3560-X or 3750-X 4xSFP Uplink Module	WS-C3560X-24T-S WS-C3560X-48T-S C3KX-NM-1G	15.0(1)SE1
Internet DMZ Switch	Cisco Catalyst 3750-X Stackable 24 &48 Ethernet 10/100/1000 ports with IP Base.	WS-C3750X-24T-S WS-C3750X-48T-S	15.0(1)SE1
	Cisco Catalyst 3560-X Standalone 24 & 48 Ethernet 10/100/1000 ports with IP Base.	WS-C3560X-24T-S WS-C3560X-48T-S	15.0(1)SE1

Functional area	Product	Part numbers	Software version
Headquarters WAN router	Cisco 3945 or 3925 Integrated Services Router G2	C3945-VSEC/K9 C3925-VSEC/K9	15.1(4)M2
Remote-site router	Cisco 2951 Integrated Services Router Cisco 2921 Integrated Services Router Cisco 2911 Integrated Services Router Cisco 881 Integrated Services Router	C2951-VSEC/K9 C2921-VSEC/K9 C2911-VSEC/K9 C881SRST-K9	15.1(4)M2
Remote-site router modules	Cisco Wide Area Acceleration Module	SRE-700-S SRE-900-M	4.4.1.12
Remote-site Switch	Cisco Catalyst 3750-X Stackable 24 &48 Ethernet 10/100/1000 ports with PoE+ and IP Base. Uplink Module is optional.* Cisco Catalyst 3560-X Standalone 24 & 48 Ethernet 10/100/1000 ports with PoE+ and IP Base. Uplink Module is optional.* Cisco Catalyst 2960-S Stackable** 24 & 48 Ethernet 10/100/1000 ports with PoE+,LAN Base, 4 SFP ports. **Optional 2960-S FlexStack Stack Module	WS-C3750X-24P-S WS-C3750X-48PF-S WS-C3560X-24P-S WS-C3560X-48PF-S WS-C2960S-24PS-L WS-C2960S-48FPS-L C2960S-STACK	15.0(1)SE1
Internet Edge Firewall	Cisco Adaptive Security Appliance ASA 5540 with the SSM-40 IPS Module ASA 5520 with the SSM-20 IPS Module ASA 5510 with the SSM-10 IPS Module	 ASA5540-AIP40-K9 ASA5520-AIP20-K9 ASA5510-AIP10-K9	8.4.2.ED 7.0(5a)E4
Server Room Firewall	Cisco Adaptive Security Appliance ASA 5540 with the SSM-40 IPS Module	ASA5540-AIP40-K9	8.4.2.ED 7.0(5a)E4

Functional area	Product	Part numbers	Software version
Headquarters— Intrusion Prevention System	Cisco Intrusion Prevention System 4200 Series	IPS-4240-K9 (300 Mbps) IPS-4255-K9 (600 Mbps) IPS-4260-K9 (2 Gbps)	7.0(5a)E4
Application Acceleration Headquarters CM Headquarters endpoint	Cisco WAVE 694 Cisco WAVE 594 Cisco WAVE 294	WAVE-694-K9 WAVE-594-K9 WAVE-294-K9	4.4.1.12
Wireless Access Points	Cisco Aironet access points 1140 Fixed with Internal Antennas 1260 with Internal Antennas 3500 with Internal Antennas 3500 with External Antennas	 AIR-LAP1142N (Country-specific) AIR-LAP1262N (Country-specific) AIR-CAP3502I (Country-specific) AIR-CAP3502E (Country-specific)	7.0.116.0
Wireless LAN Controller	Cisco WLC 5508	AIR-CT5508-12-K9	7.1.91.0
Server Load Balancing	Cisco Application Control Engine	ACE-4710-1F-K9	A5.1

Appendix B: RADIUS Authentication with Windows Server 2008

The following procedure describes the steps required to enable RADIUS authentication for the Wireless LAN Controller deployment in this guide on an existing Windows Server 2008 Enterprise Edition installation.

Process

Installing Active Directory Certificate Services and Network Policy Services

1. Install services
2. Set up certificate auto enrollment
3. Verifying on the wireless LAN controller
4. Testing the DATA WLAN

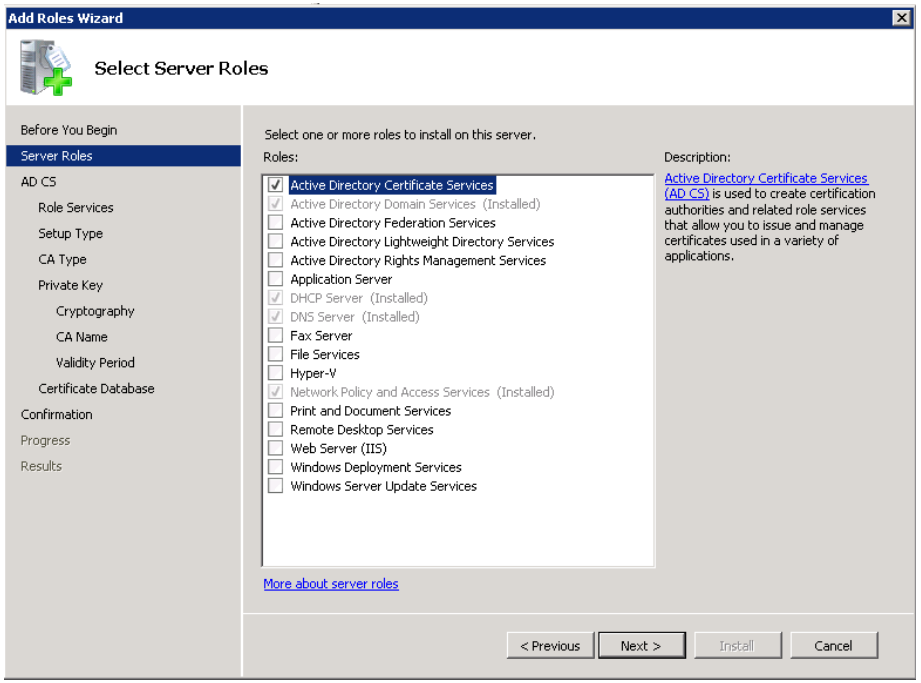
Procedure 1 Install services

Step 1: Join the server to your existing domain, and then restart.

Step 2: After the server restarts, open Server Manager.

Step 3: Navigate to **Roles >Add Roles.**

Step 4: On the **Server Roles** page, select **Active Directory Certificate Services** and **Network Policy and Access Services**.



Step 5: Follow the instructions in the wizard.

When configuring the Network Policy and Access Services role, select **Network Policy Server** and leave the default Certification Authority role service selected for AD CS.

For the setup type for Active Directory CS, choose **Enterprise**.

For the CA Type, choose Root CA.

Tech Tip

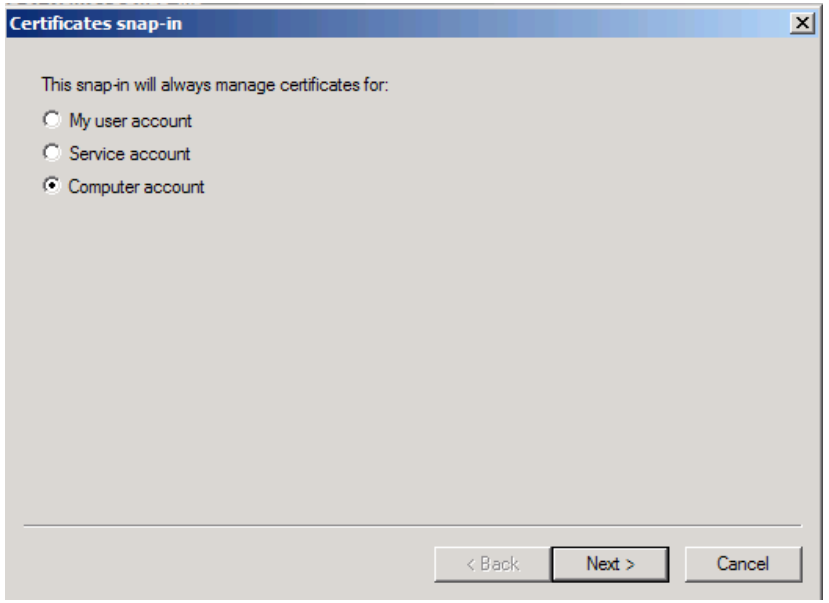
We're assuming that this is the first Certification Authority in your environment, so if it's not, you either don't need to install this role, or you can configure this server as a Subordinate CA instead.

Run through the rest of the wizard, making any changes you want. Otherwise, just leave the default values as appropriate–note that there is a warning at the end of the wizard, stating that the name of this server cannot be changed after installing the AD CS role.

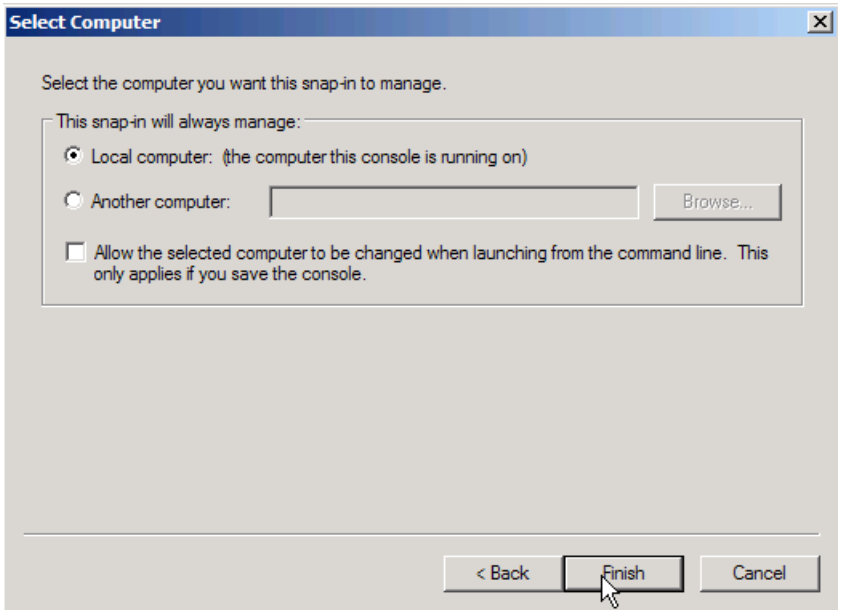
Now that you have a Root CA and an NPS server on your domain, you can configure it.

Step 6: Open an MMC console, and then click **File -> Add/Remove Snap-in**.

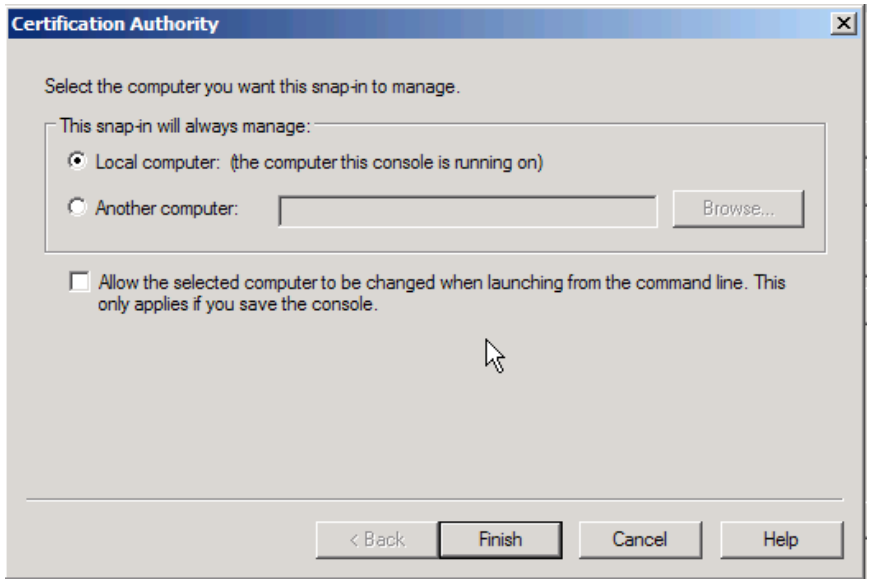
Step 7: In **Certificates snap-in**, select **Computer account** for the local computer.



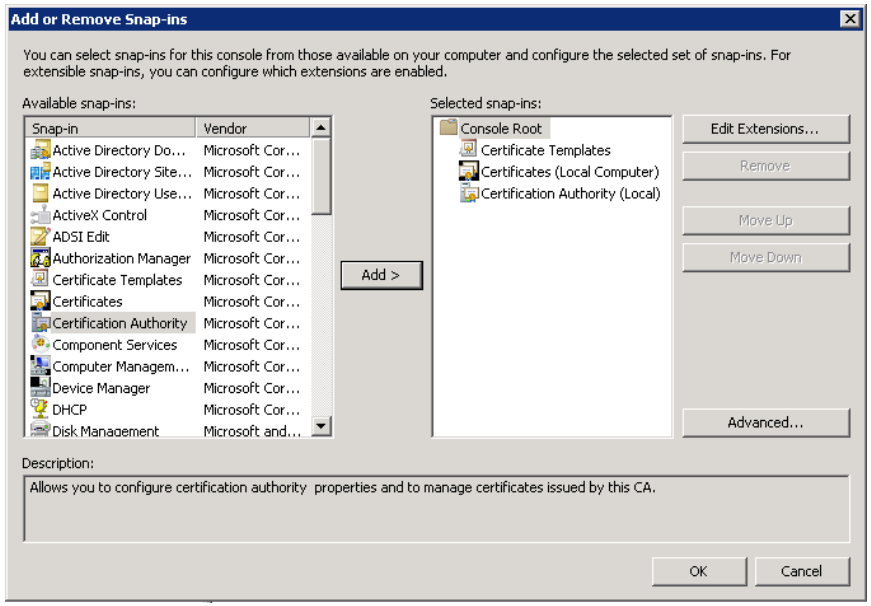
Step 8: In **Select Computer**, select **Local computer**, and then click **Finish**.



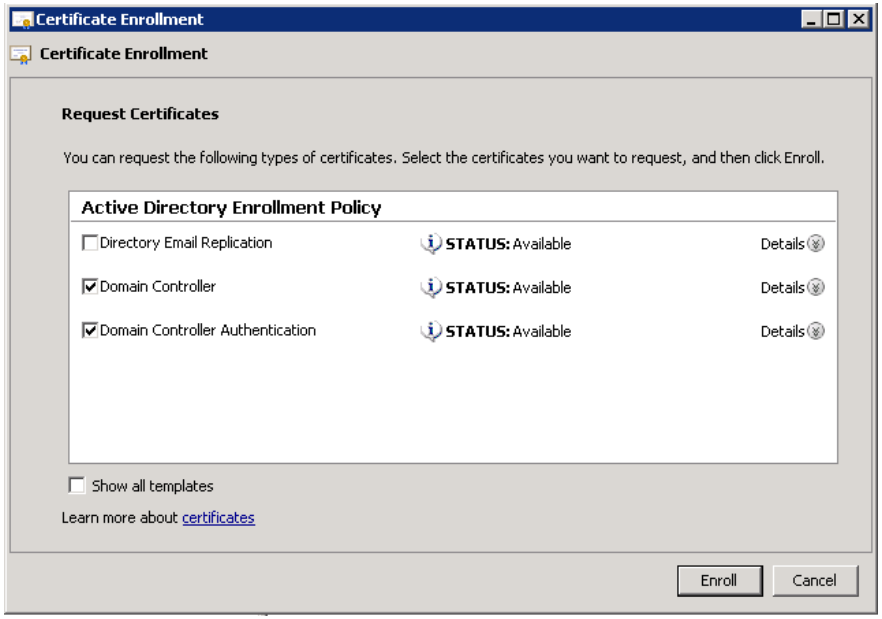
Step 9: Add the Certification Authority Snap-in.



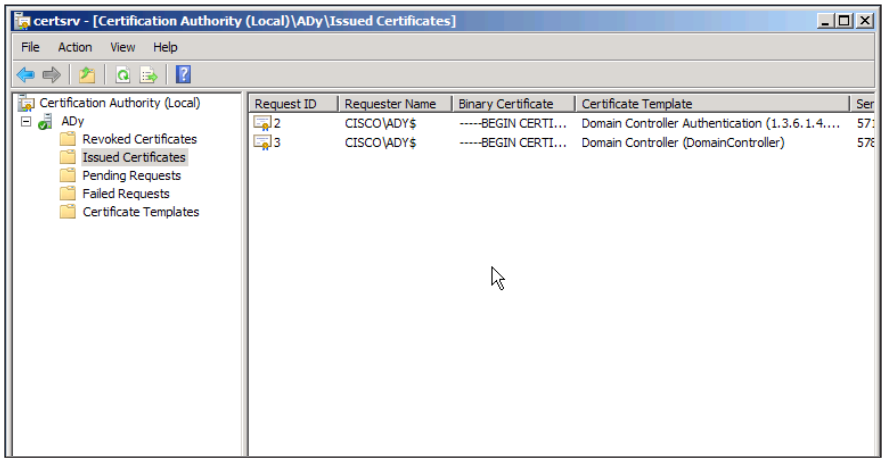
Step 10: Add the Certificate Templates Snap-in, and then click **OK**.



Step 11: Expand **Certificates (Local Computers) -> Personal**, right-click **Certificates**, and then click **Request new certificate**.

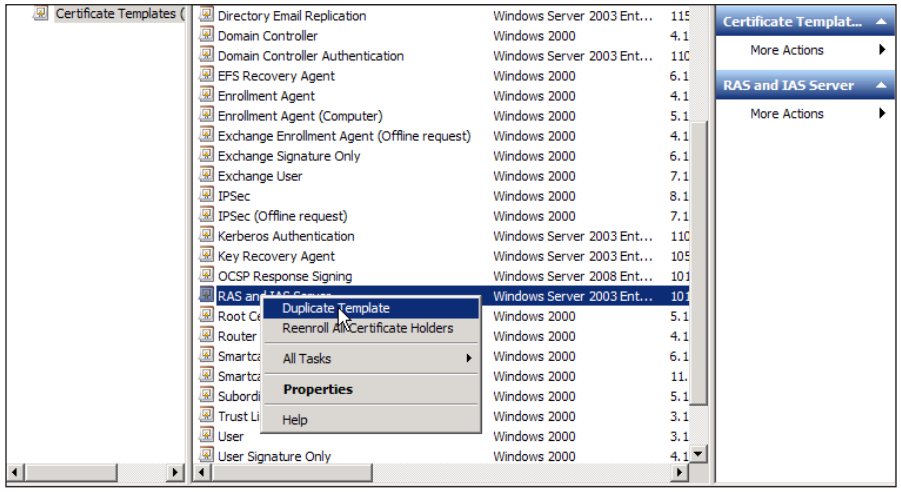


Step 12: Follow the wizard, choosing **Computer** for the certificate type and then click **Enroll**. Verify that the Certificate templates folder appear under **Certificate Authority / Issued Certificates**.

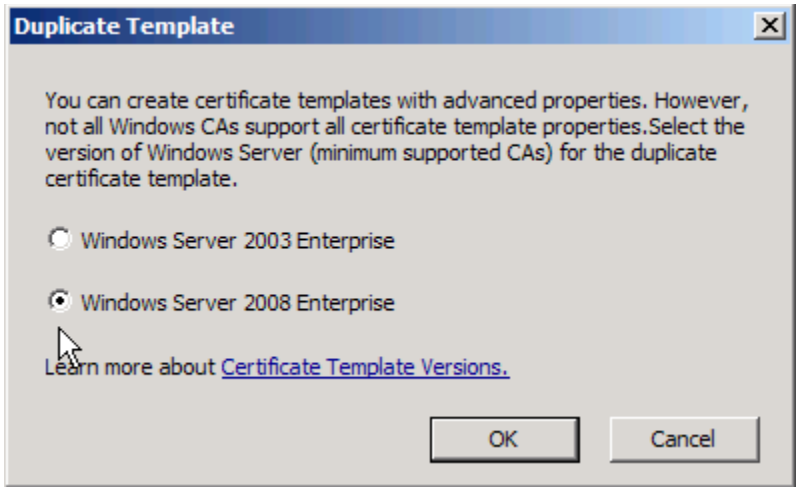


Step 13: Click the Certificate Templates folder and in the right pane locate the RAS and IAS Server Template.

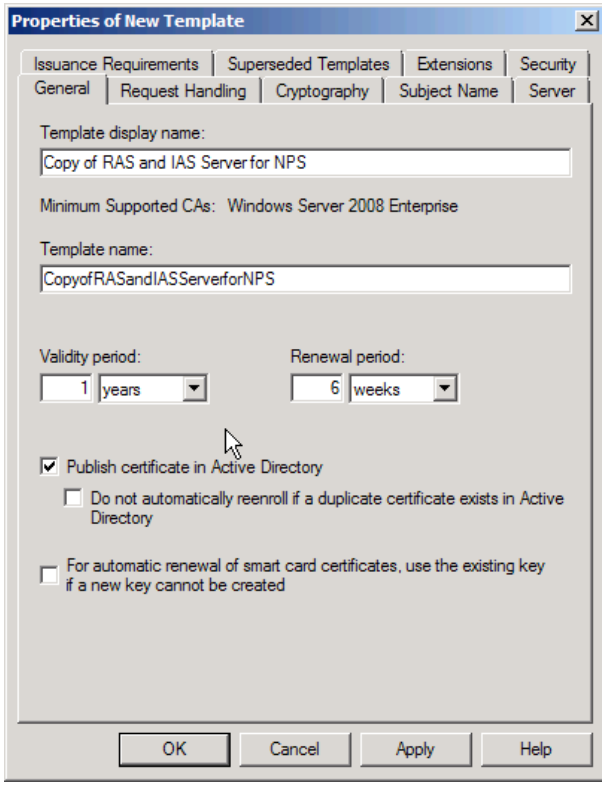
Step 14: Right-click **RAS and IAS Server**, and then click **Duplicate Template**.



Step 15: Select **Windows Server 2008 Enterprise**, and then click **OK**.

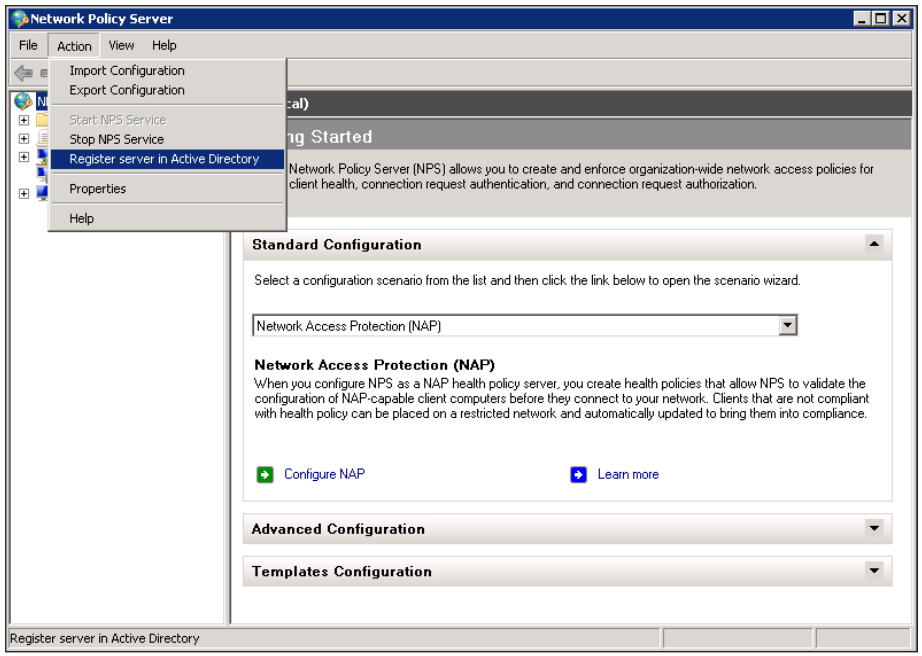


Step 16: Type a valid display name, select the **Publish Certificate in Active Directory** check box, click **Apply**, and then close the MMC console.



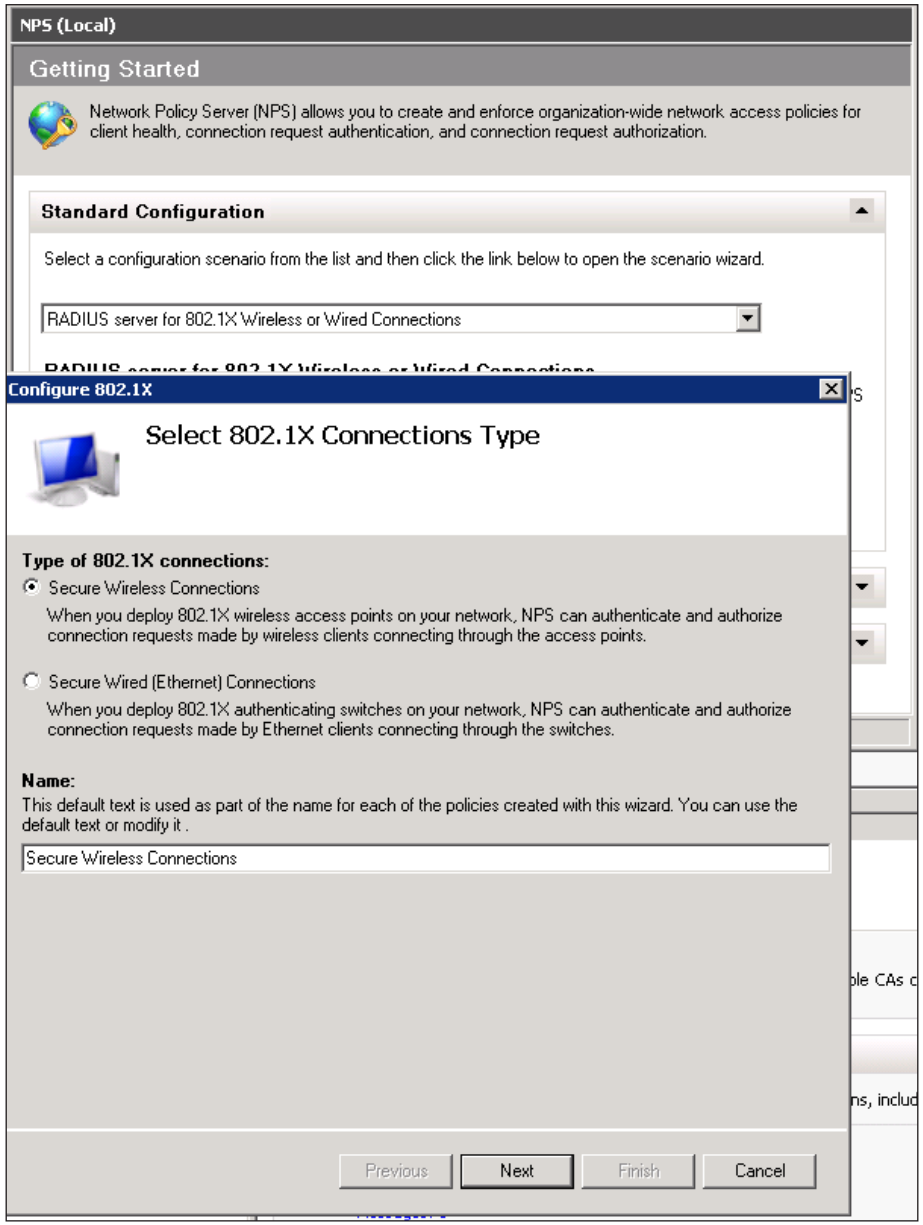
Step 17: Open the Network Policy Server administrative console from Administrative Tools.

Step 18: Right-click the parent node **NPS (Local)**, click **Register server in Active Directory**, click **OK**, and then click **OK** again.



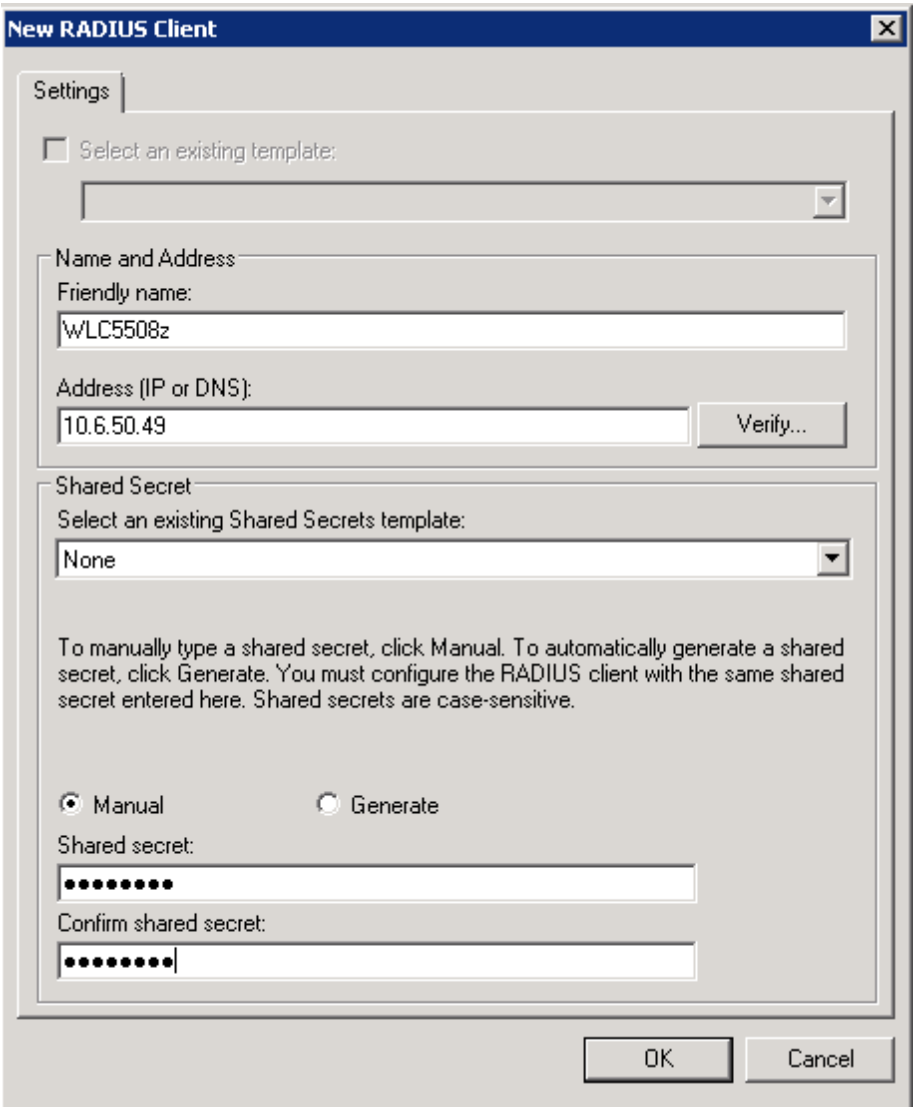
Step 19: With the NPS (Local) node still selected, select **RADIUS server for 802.1X Wireless or Wired Connections** and then click **Configure 802.1X**.

Step 20: Under **Type of 802.1X connections**, select **Secure Wireless Connections** and then type an appropriate name for the policies that you want to create with this wizard.

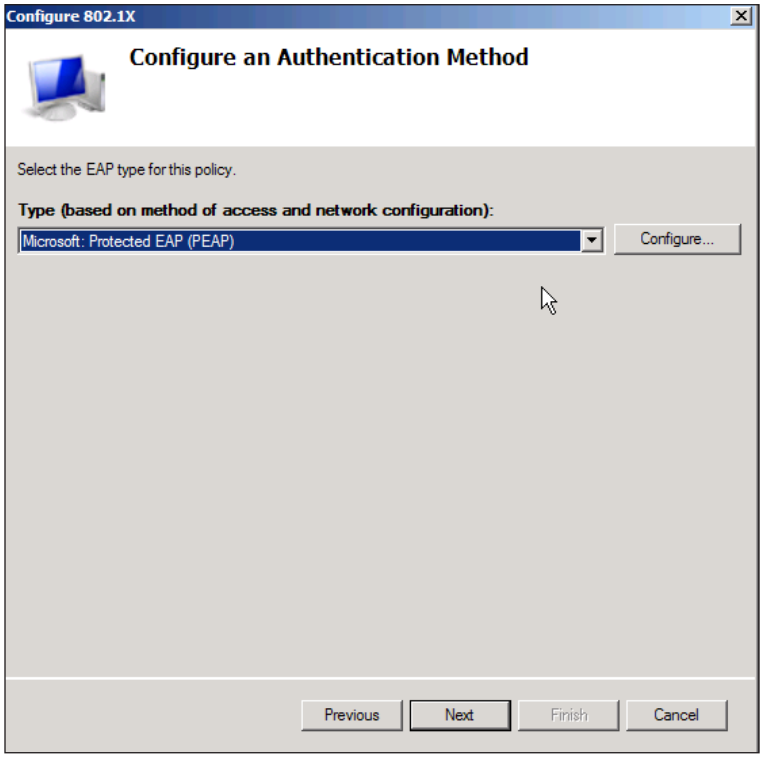


Step 21: Click **Add**.

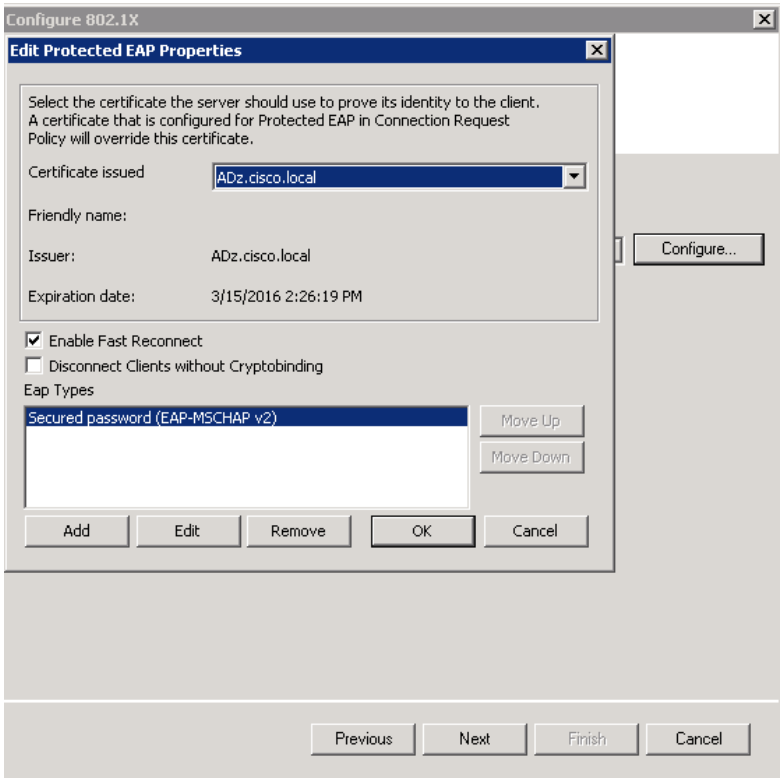
Step 22: The RADIUS client will be your wireless access point, so for the friendly name type in something to identify the access point (for example, AP01), and then provide the IP address or DNS entry for the access point.



Step 23: Click **Next**, select **Microsoft: Protected EAP (PEAP)**, and then click **Configure** (if you get an error message, you probably didn't follow Steps 1 through 4 correctly).

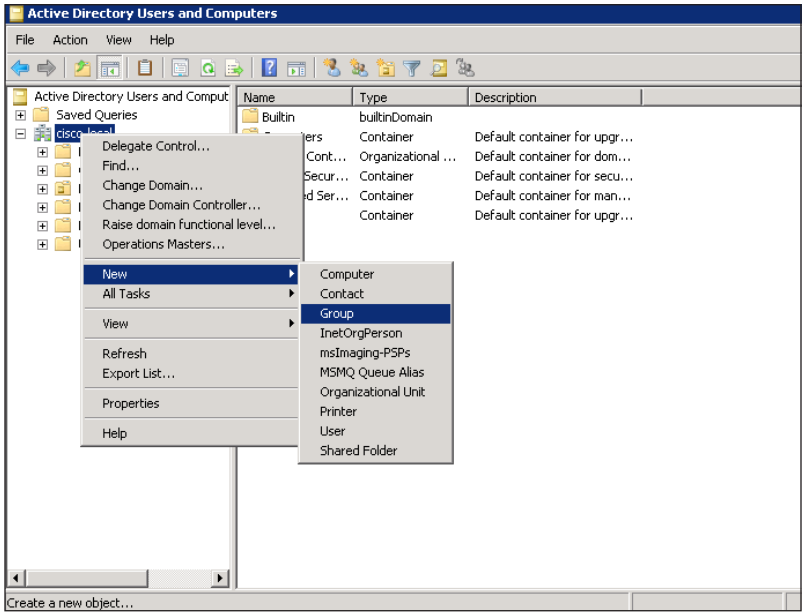


Step 24: Ensure that the **Certificate issued** drop-down list box has the certificate you enrolled in Step 4.

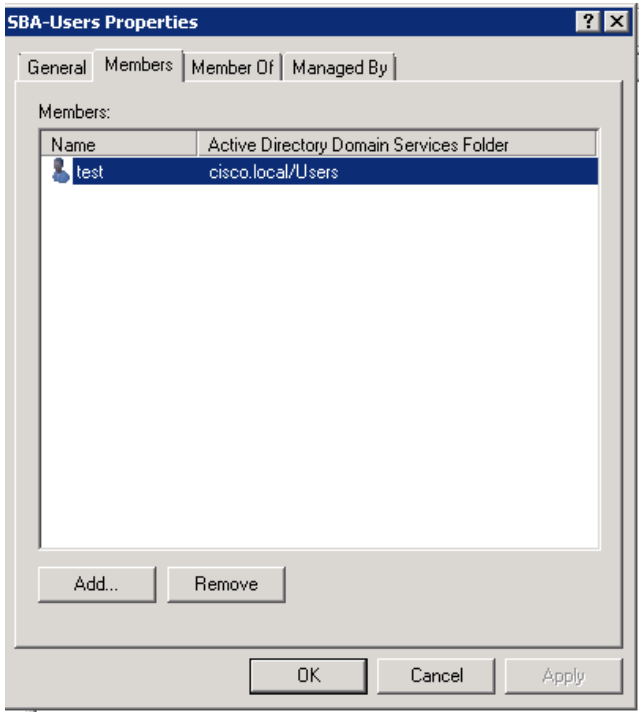


Step 25: In **Specify User Groups**, click **Add** to add a group that you already created, or perform the following steps to create a group and add users to the group.

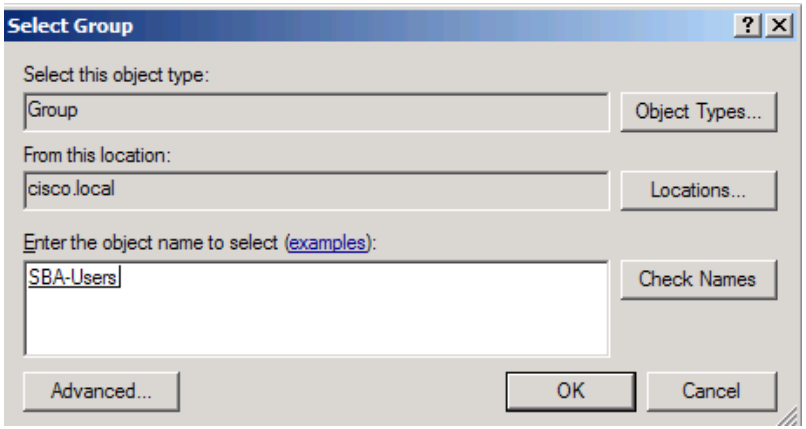
Step 26: Create a group called SBA-Users.



Step 27: Create a user named **test** and add it to the group created in the previous step.

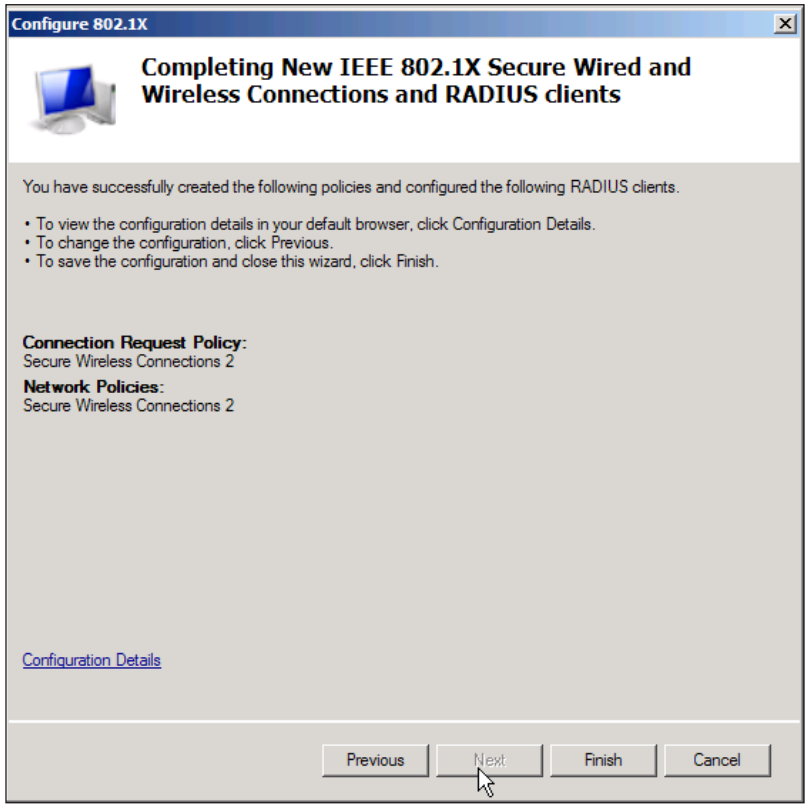


Step 28: Click **Next**, and then click **Add** to use an Active Directory group to secure your wireless (you should add both the machine accounts and user accounts to this group to allow the machine to authenticate on the wireless before the user logs in).



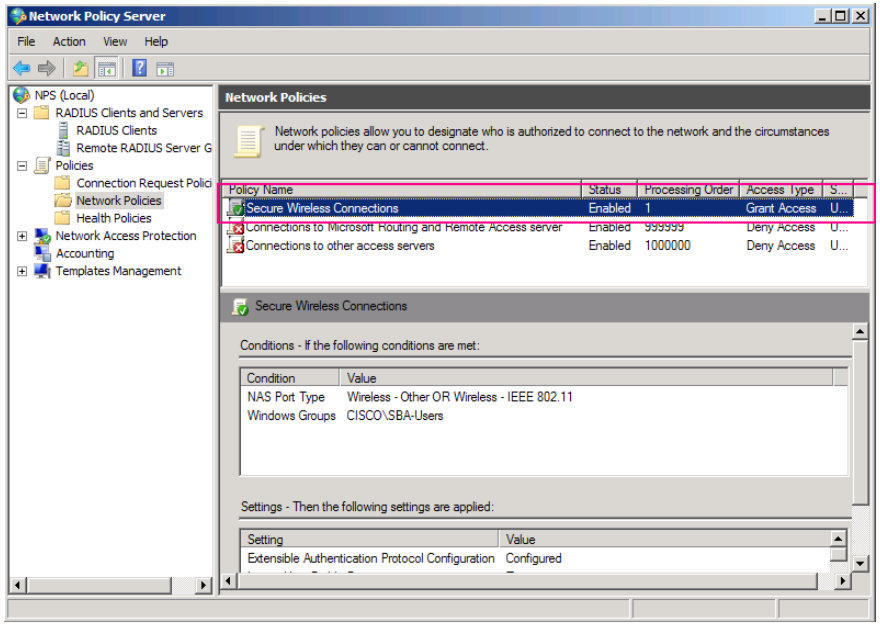
Step 29: On the next step of the wizard, you can configure VLAN information, otherwise just accept the defaults to complete.

Step 30: Click **Finish** to complete the configuration of 802.1x.



Step 31: Restart the Network Policy Server service.

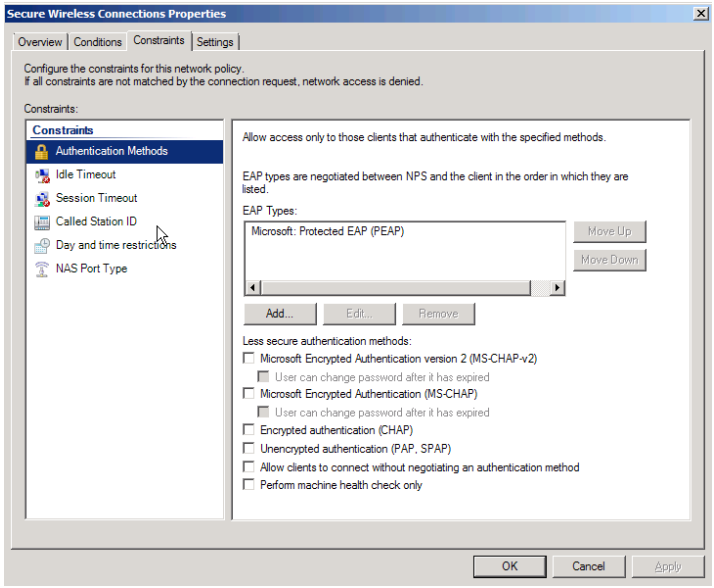
If you expand the Policies node now, you'll see that the wizard has created a Connection Request Policy and a Network Policy containing the appropriate settings to authenticate your wireless connection – You can create these individual policies manually, but the wizard is an easier method.



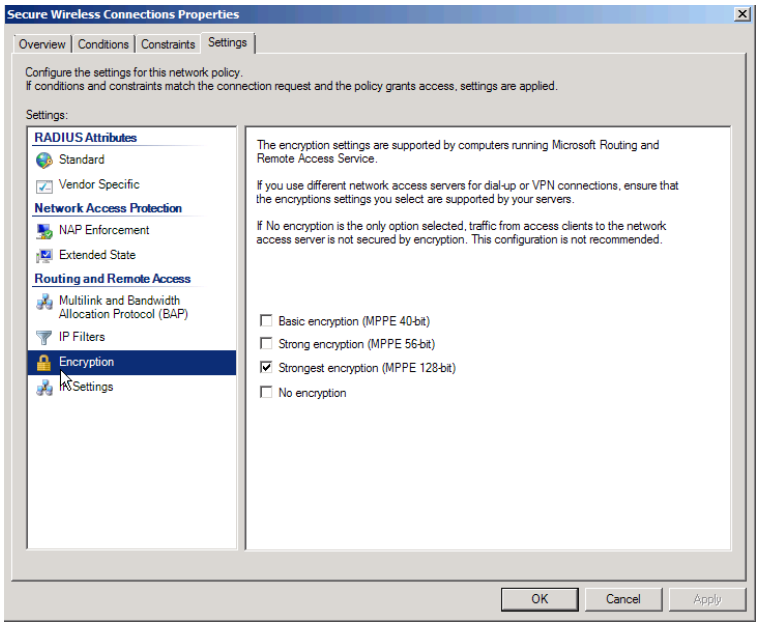
You can also remove the less secure authentication method options, and increase the encryption methods in the network policy if you want.

Step 32: Under the **Network Policies** node, open the properties of the newly created policy.

Step 33: On the **Constraints** tab, clear all of the check boxes under **Less secure authentication methods**.



Step 34: On the **Settings** tab, click **Encryption** and clear all check boxes except **Strongest encryption (MPPE 128-bit)**.

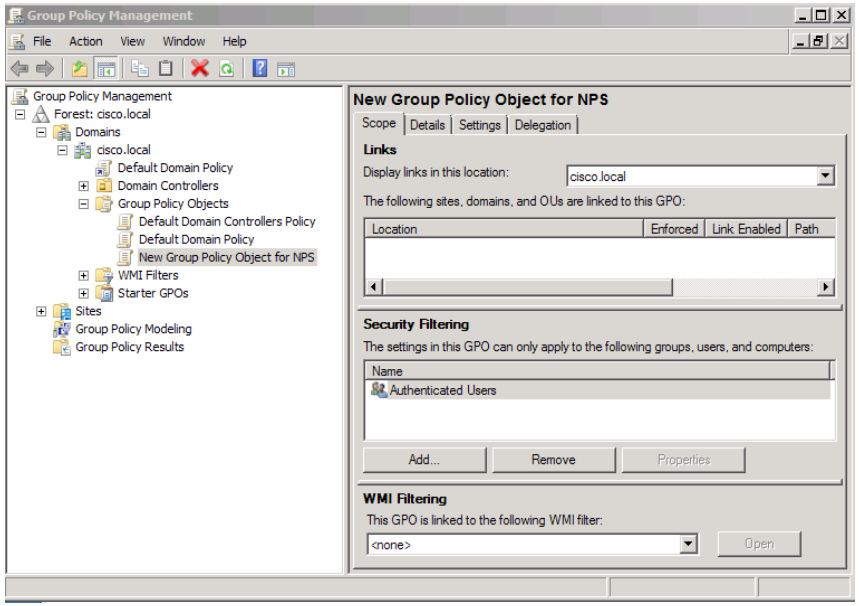


Step 35: Save the policy and then restart the Network Policy Server service.

Procedure 2 Set up certificate auto enrollment

Step 1: Open Group Policy Management.

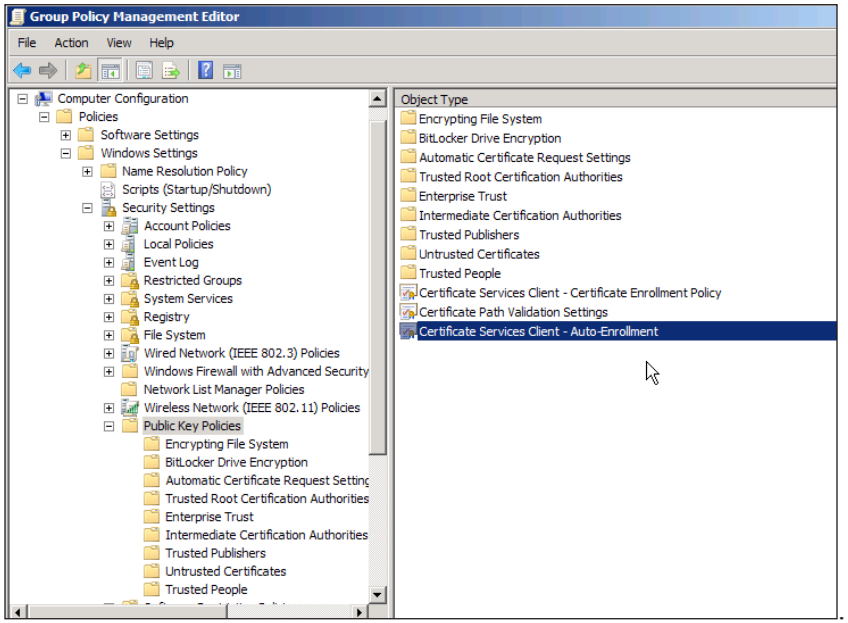
Step 2: Create a new GPO policy and name it appropriately.



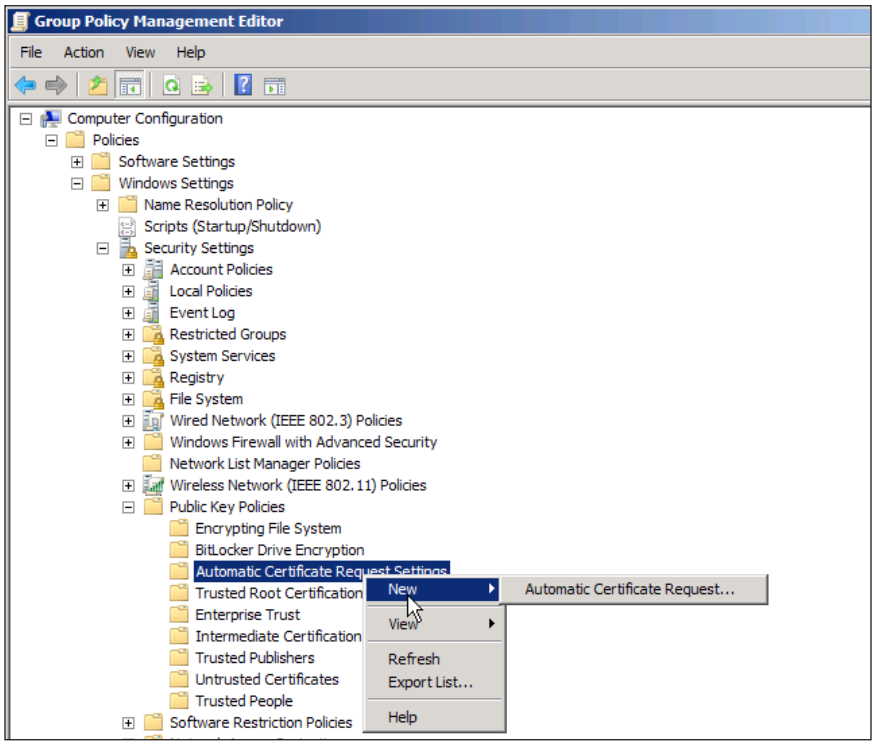
Step 3: Right-click the New Policy Object that you created and then click **Edit** to edit the settings of the group policy.

Step 4: Go to Computer Configuration\Policies\Windows Settings\Security Settings\Public Key Policies

In the details pane you should see the following list:

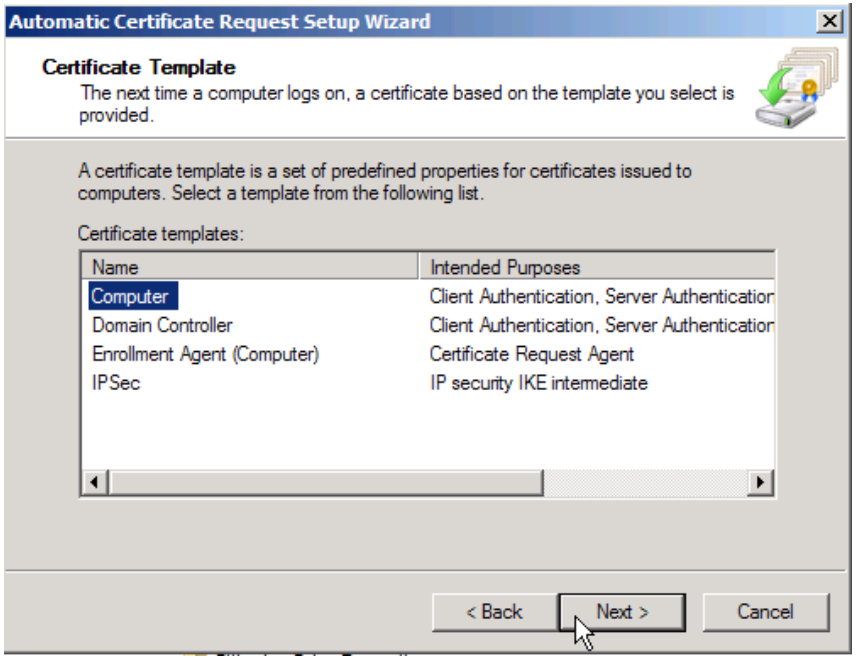


Step 5: Go to Computer Configuration\Policies\Windows Settings\Security Settings\Public Key Policies\Automatic Certificate Request Settings.

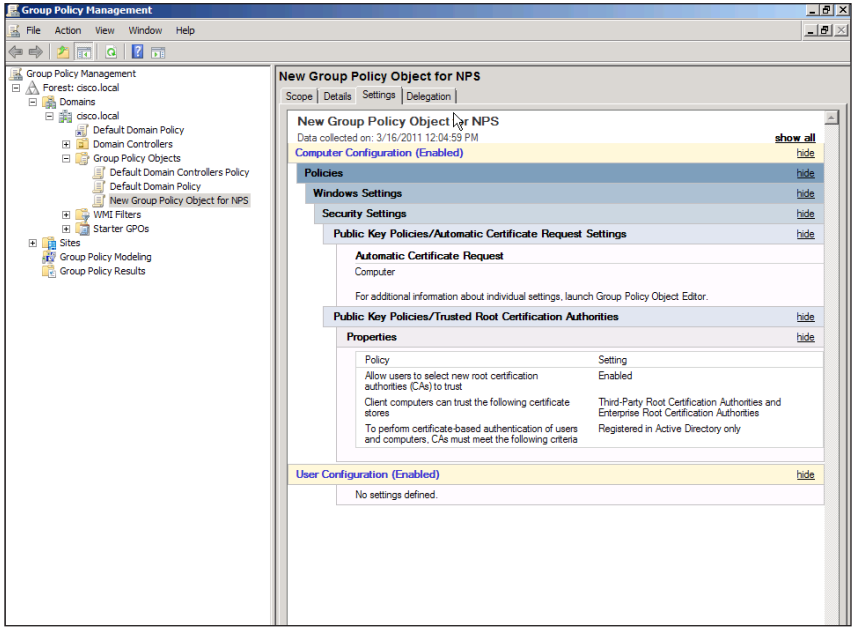


Step 6: Right-click in the details pane and click **New** > **Automatic Certificate Request**.

Step 7: In the Automatic Certificate Request Setup Wizard, select a Computer Certificate and then close the wizard.



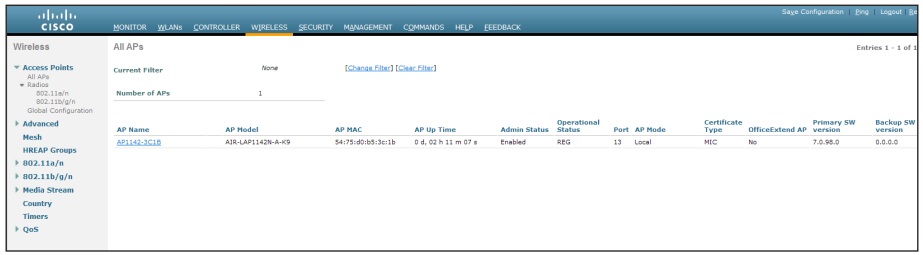
Step 8: In the GPO of the newly created policy, under the **Settings** tab in the right pane you should see the Public Key Policies\ Automatic Certificate Request Settings and Public Key Policies/ Trusted Root Certification Authorities details.



Procedure 3 Verifying on the wireless LAN controller

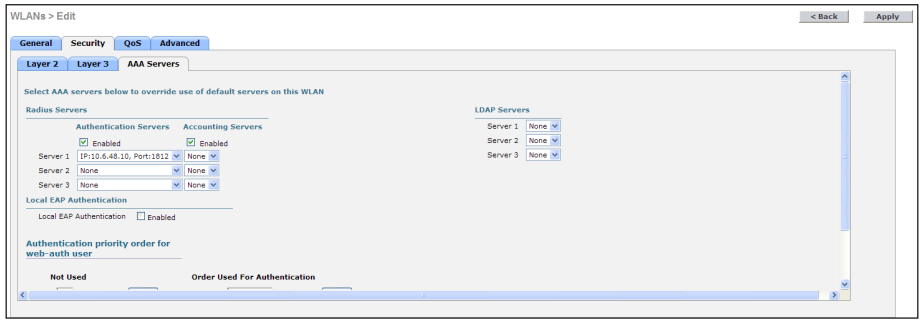
Step 1: Connect an AP to the access switch and configure the port as instructed in this guide.

The AP should be associated with the wireless LAN controller (WLC) and should appear in the WLC\Wireless.

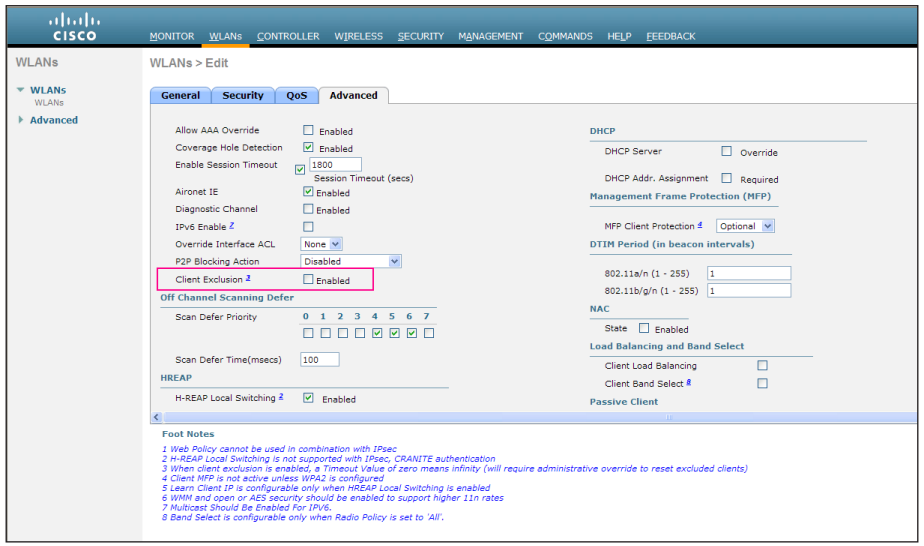


Step 2: Before connecting the Wireless devices for testing purposes verify the following settings on WLC:

- Click on the WLAN (Voicevlan and DataVLANs)
- Under the corresponding WLAN, click the **Security** tab, and then click the **AAA Servers** tab.
- Make sure that the **Server1** drop-down list has the **AD Ip and Port 1812** set to **None,** and then click **Apply**.

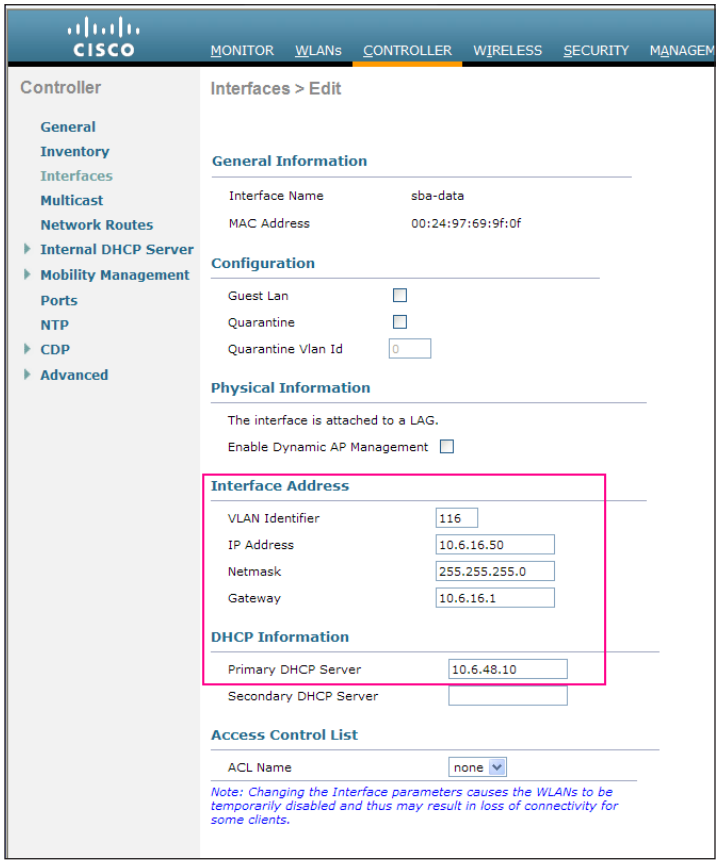


Step 3: Click **WLANs**, click the **Advanced** tab clear the **Client Exclusion Enabled** check box.



Step 4: Verify the Controller interfaces.

Click **Controller**, select the Data interface and then verify that the **VLAN Identifier**, **IP address**, **Gateway**, and **Primary DHCP Server** are provided.



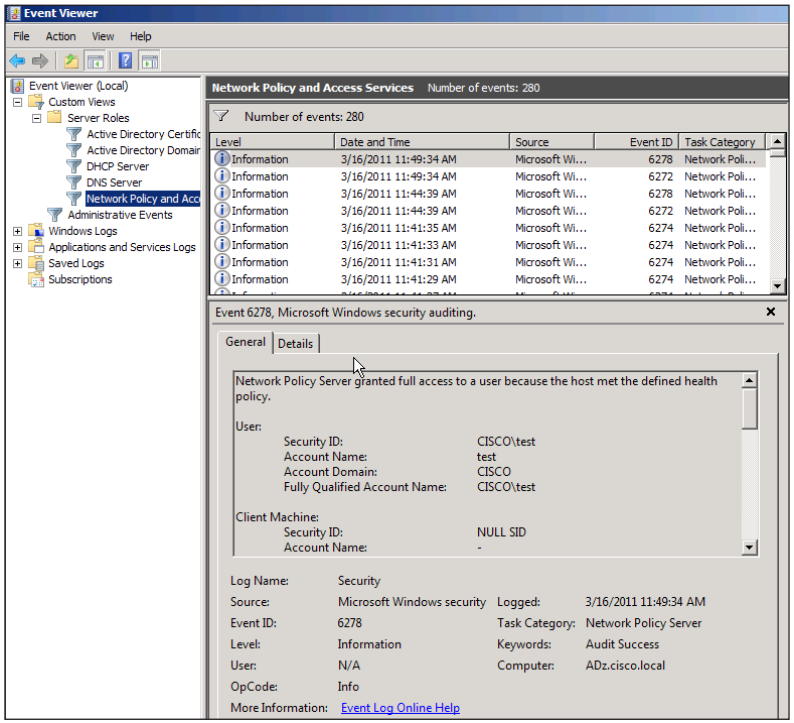
Step 5: Repeat the previous step for the Voice interface.

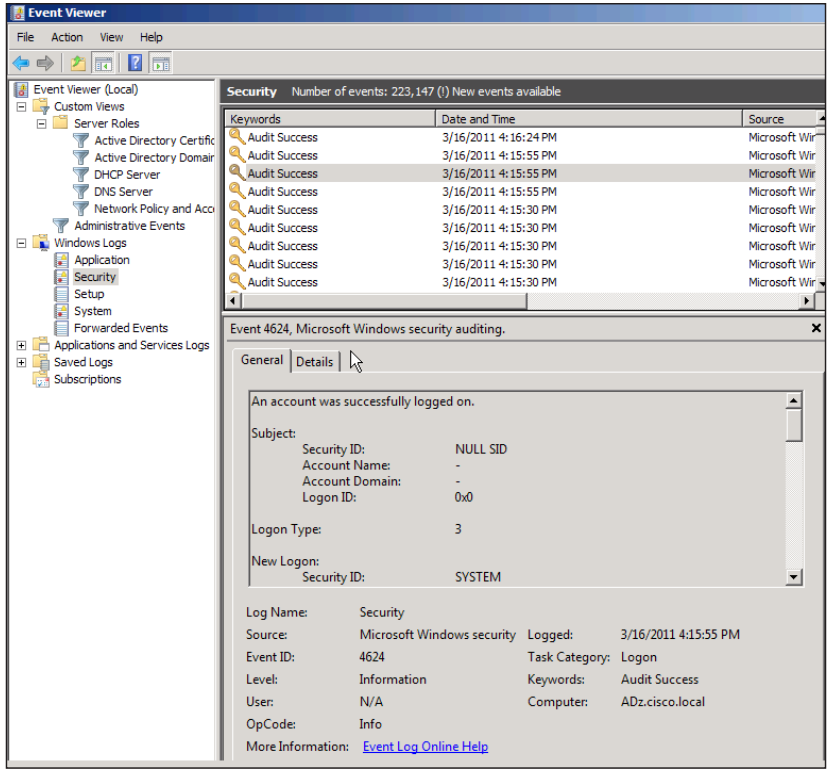
Step 6: Verify that Active Directory can ping WLC.

Procedure 4 Testing the DATA WLAN

Step 1: Connect a laptop to the Data SSID you created on WLC by using the username and password you added to SBA-Users (Group) you created on Active Directory.

Step 2: Verify that the RADIUS Requests and Accepts are reaching Active Directory. On Active Directory open Event Viewer \Custom Views\Server Roles\Network Policy and Access Services.





Step 3: Verify that the client appears on WLAN under **Monitor > Clients**. The client Mac address appears with a DHCP address assigned to it. This confirms that RADIUS Authentication was a success.

Appendix C: Changes

This appendix summarizes the changes to this guide since the previous Cisco SBA series.

- We changed DMZ VLANs and subnets.
- We added DMZ switch configuration guidance.
- We changed Internet Edge Firewall and Remote Access VPN configuration to be GUI-driven after initial configuration.
- We changed the guest WLAN subnet and VLAN to be contiguous with DMZ subnets.
- We moved WAAS head-end devices and Wireless LAN Controllers from connections on the server room switch to the core switch.
- We added Cisco 881 router for small remote sites.

Notes

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.**

B-0000512-1 2/12