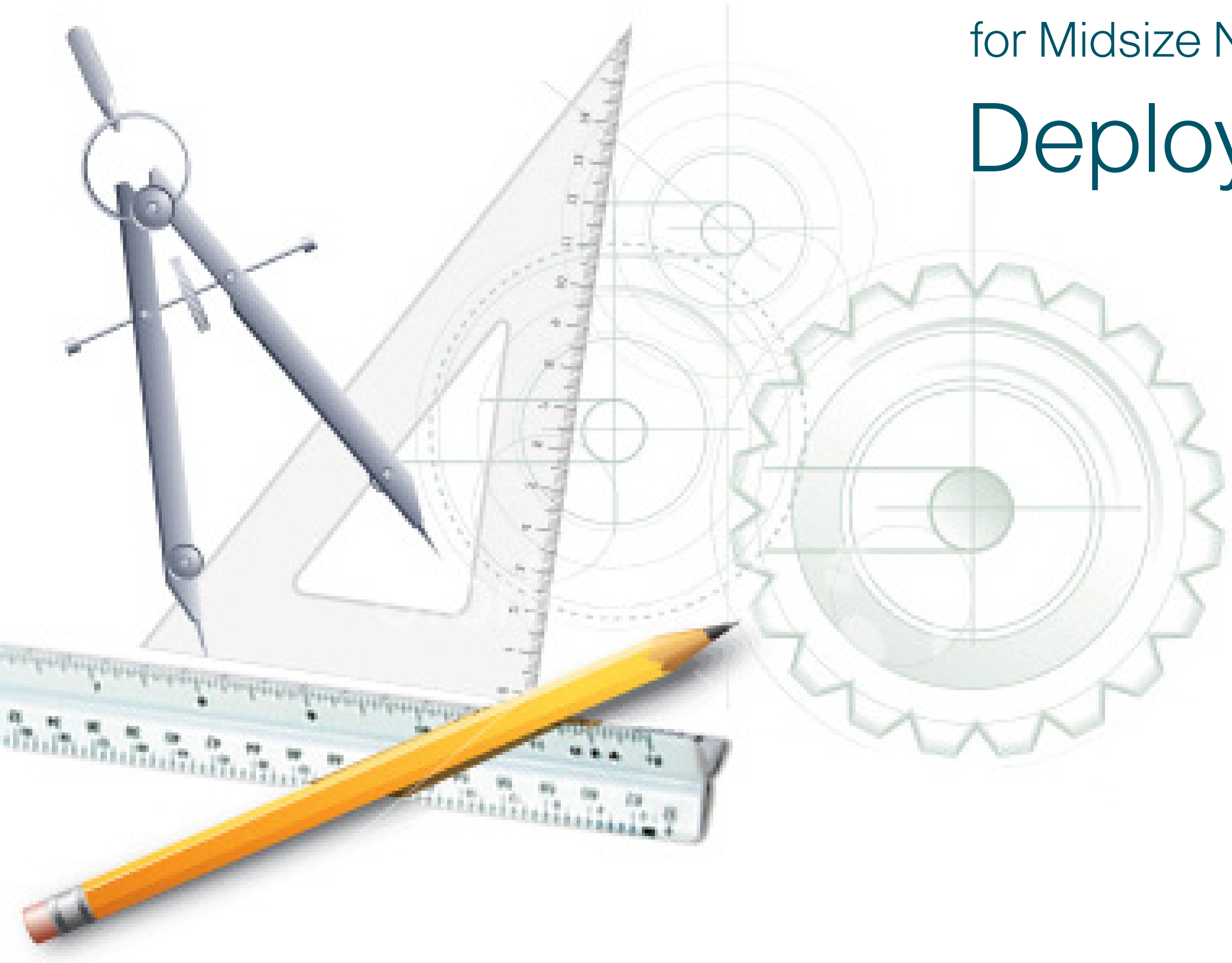
Smart Business Architecture
for Midsize Networks

Deployment Guide



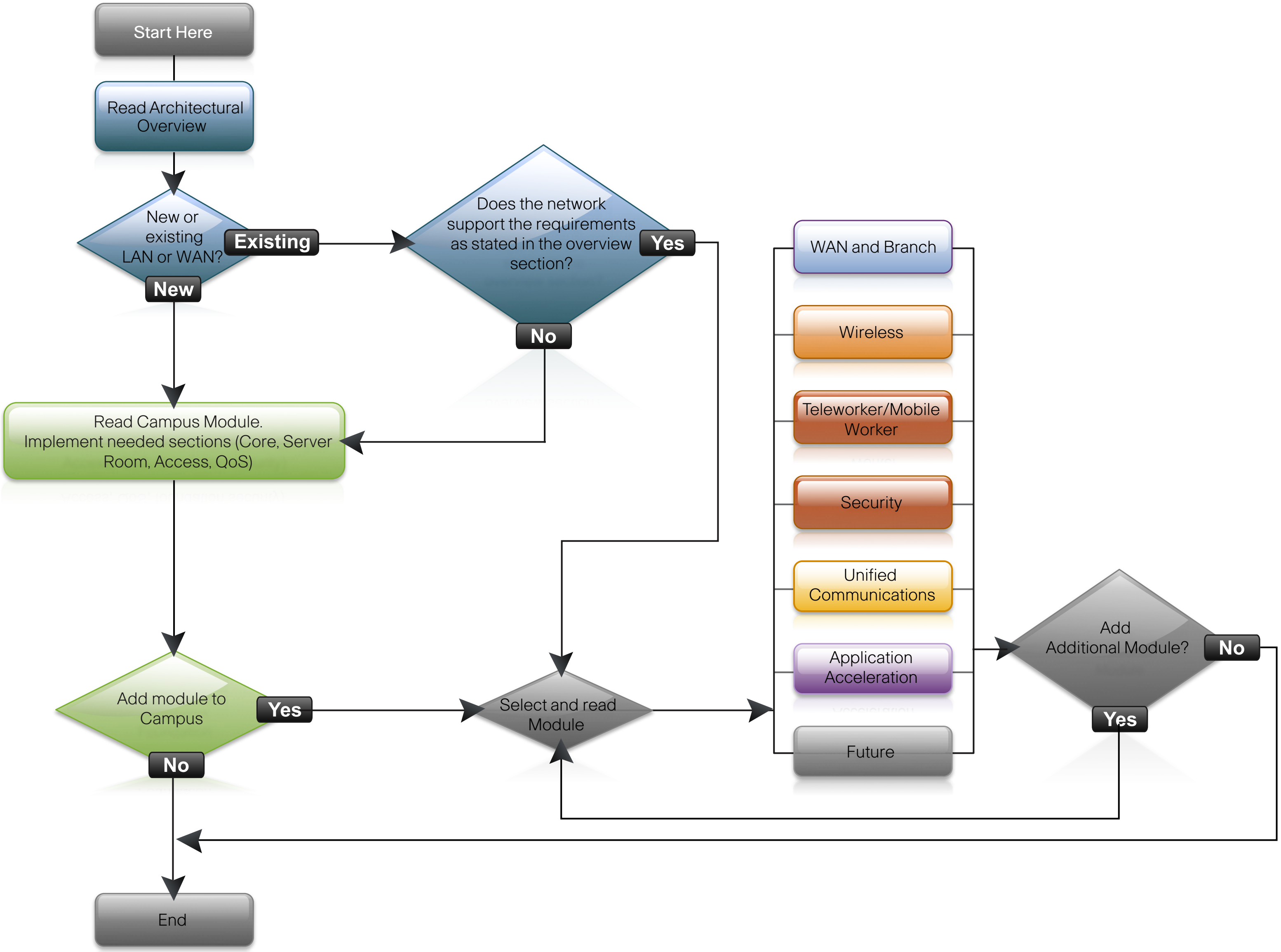
July 2009

Table Of Contents

ALL DESIGNS, SPECIFICATIONS, STATEMENTS, INFORMATION, AND RECOMMENDATIONS (COLLECTIVELY, "DESIGNS") IN THIS MANUAL ARE PRESENTED "AS IS," WITH ALL FAULTS. CISCO AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE. IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THE DESIGNS, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE DESIGNS ARE SUBJECT TO CHANGE WITHOUT NOTICE. USERS ARE SOLELY RESPONSIBLE FOR THEIR APPLICATION OF THE DESIGNS. THE DESIGNS DO NOT CONSTITUTE THE TECHNICAL OR OTHER PROFESSIONAL ADVICE OF CISCO, ITS SUPPLIERS OR PARTNERS. USERS SHOULD CONSULT THEIR OWN TECHNICAL ADVISORS BEFORE IMPLEMENTING THE DESIGNS. RESULTS MAY VARY DEPENDING ON FACTORS NOT TESTED BY CISCO. Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental. Cisco Unified Communications SRND (Based on Cisco Unified Communications Manager 7.x)

Deployment Made Easy Flow Chart

This flow chart is a navigational aid for using this Deployment Guide.
Follow the chart through the Campus Module then select the module you want to implement.



A Blueprint for Deployment Made Easy

We had one guiding principle with this new architecture designed by Cisco: Ease of Use.

For our Cisco partners servicing customers with 250-1000 connected users, we have designed an "out-of–the-box" deployment that is simple, fast, affordable, scalable, and flexible. We have designed it to be easy. Easy to configure, deploy, and manage.

The simplicity of this deployment, though, belies the depth and breadth of the architecture (and that's the point). Based on feedback from many customers and partners, Cisco has developed a solid network foundation with a flexible platform that does not require re-engineering to Network or User services. So whether you are adding advanced services during or after the core network deployment, time and expense won't be wasted reconfiguring what could have been configured to work with these services in the first place.

In a nutshell, this deployment has been architected to make your life a little bit—maybe even a lot—smoother. This architecture:

- Provides a solid foundation
- Makes deployment fast and easy
- Accelerates opportunities for Cisco partners to provide additional services
- Avoids the need for re-engineering of the core network

Using this Deployment Guide

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

The Deployment Guide starts with an **Architecture Overview**. It covers the basics of the deployment guide, the value for you and your customer, and the broad stroke features and benefits of this compelling design.

The next module covers **Global Configuration**. These are the elements that are universal among many, if not all, of the devices in the solution. Examples of this include Secure Shell (SSH) setup for secure remote management or Simple Network Management Protocol (SNMP) for monitoring and troubleshooting. Additionally, it covers the network management tools to configure, monitor, and troubleshoot this design.

The **Campus Module** covers how to deploy the Campus, Access, and Server Room networks. Quality of service (QoS) is also covered in the Campus module because it is a critical service that must be enabled on the base architecture to ensure a multitude of applications, such as real-time voice, high-quality video, and delay-sensitive data, is able to coexist on the same network.

The **Wide-Area Network (WAN) Module** includes the campus WAN edge, its connectivity to remote locations (branches), and network infrastructure at those locations.

The **Wireless Module** covers the wireless infrastructure for the campus and its use for employees to access the intranet and Internet and guest users to access the Internet.

The **Security Module** focuses specifically on the deployment of advanced security services such as firewalls, intrusion detection to protect information assets, and also the secure remote access configuration for teleworkers and remote mobile workers. Because security is such an important element in the design, it will be covered in multiple sections.

The **Unified Communications (UC) Module** shows you how to deploy Cisco® UC/IP telephony on top of the network foundation without re-engineering the core network. Many customers deploying data networks are looking to add voice over IP or IP telephony to their network—and this ease-of-use guide enables quick deployment of this service.

The **WAN Optimization Module** shows you how to optimize the bandwidth between a branch and main office, thereby ensuring economical use of your IT resources.

And last but not least, the **Appendix** provides the complete list of products used in the lab testing of this design. A companion guide to this document, "Smart Business Architecture for Midsize Networks Configuration Files Guide," can be found on Cisco.com. It has the specific product configuration files used in the test lab.

The Purpose of this Document

This is a deployment guide for Cisco partners and Cisco Systems®, Inc. Engineers whose customer base has 250-1000 connected users. It is meant for the Systems Engineers who will be deploying Cisco solutions at customer locations. It provides engineers step-by-step instructions to deploy these solutions. Because Cisco is delivering a modular architecture, you can deploy exactly what the customer needs quickly and efficiently.

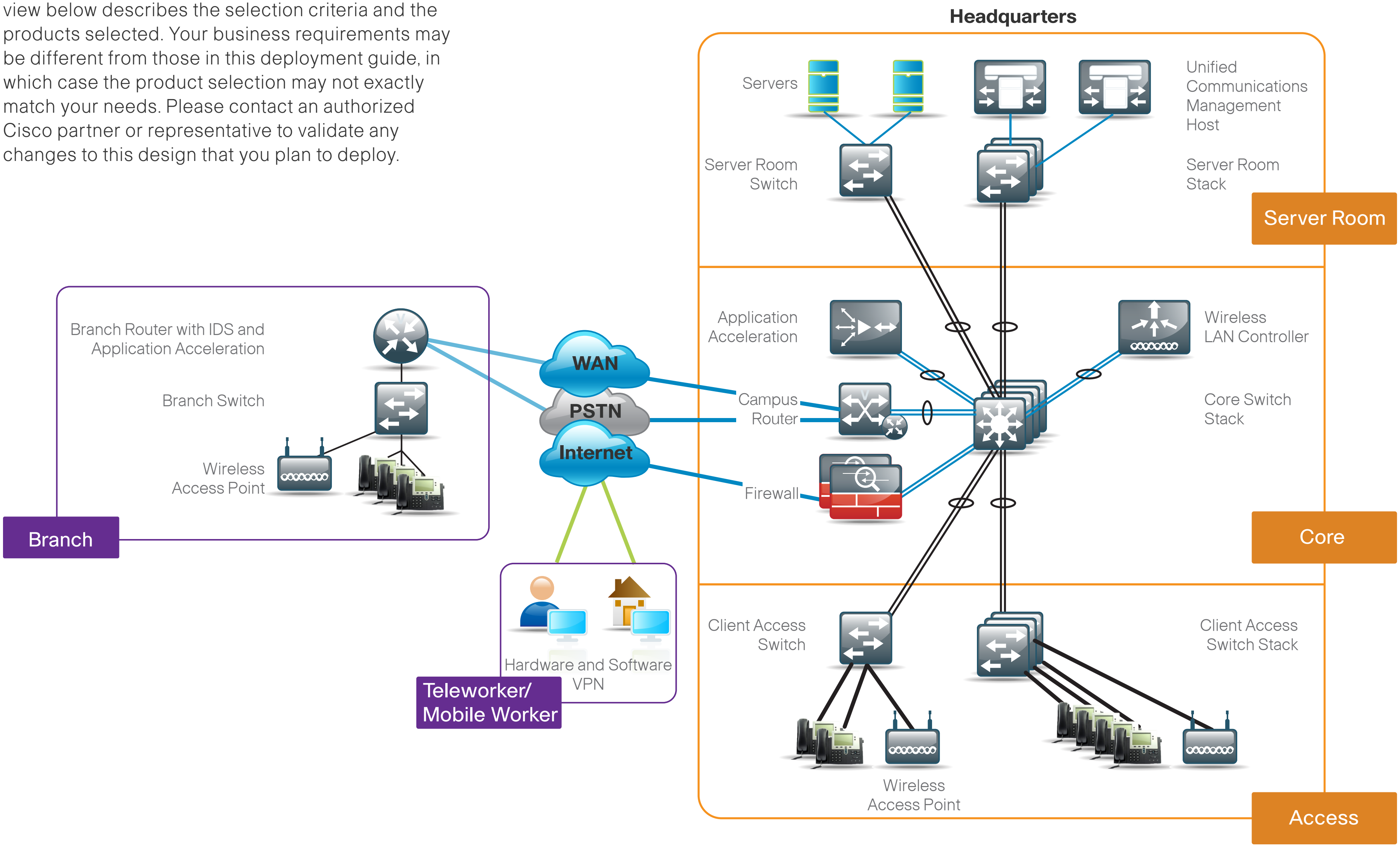
Design for Customers who

- Have 250-1000 connected employees
- Have up to 20 branches with approximately 20 employees each
- Require a solution for teleworker and mobile worker
- Require security for corporate resources
- Need wired and wireless network access for employees
- Require wireless guest access
- Require solutions for wired and wireless voice access
- Have external facing applications, which are hosted off-site
- Have a server room where internal business applications are located
- Want to reduce cost by optimizing WAN bandwidth
- Have IT workers with CCNA or equivalent experience
- Want the assurance of a tested solution
- Require a migration path for growth

Architectural Overview

The products and priorities for this design were based on requirements from customers, partners, and Cisco field personnel. The Architectural Overview below describes the selection criteria and the products selected. Your business requirements may be different from those in this deployment guide, in which case the product selection may not exactly match your needs. Please contact an authorized Cisco partner or representative to validate any changes to this design that you plan to deploy.

Network Architecture Baseline



Architectural Overview

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

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

The following section includes a list of products and the specific reasons for their selection based on the guiding principles outlined above.

Campus Module

The network 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.

In the design, two options are provided: The first option is for 250-600 users supported by a resilient core stack design using the Cisco Catalyst® 3750 switch. The second option is for 500-1000 users supported by a resilient Cisco Catalyst 4507R chassis equipped with dual supervisor modules.

Both provide the required fault tolerance and capacity. Another critical factor is port density, the number of physical ports needed to connect other devices from the other modules. The design is meant as a guideline. The actual product you select should be driven by your specific needs.

250-600 Users

The Cisco Catalyst 3750 product line is a fixed-port, stackable, Gigabit Ethernet switch that provides redundancy via the StackWise® technology. Further discussion is provided later in the Core module.

The Cisco Catalyst 3750 switch provides both Layer 3 and Layer 2 switching capabilities and is configured to route traffic between other modules in the campus network. In the future, should a business require more port density in the core or a move to a split core and aggregation/distribution layer, the current Cisco Catalyst 3750 switch can be repurposed. The dual function means it can also be reused in the server room or campus as an access switch. In the design validation, Cisco used a pair of stacked Cisco Catalyst 3750G-12S-E switches that use Small Form-Factor Pluggable transceivers, allowing for a port-by-port option of either twisted pair or fiber optic cables. In addition, the Cisco Catalyst 3750 stack provides in-service additions of stack members to add more port capacity. This ensures maximum availability and minimal downtime.

500-1000 Users

A design to support more users requires more ports and additional switching capacity to connect to the additional campus access switches. For this design we have selected a resilient Cisco Catalyst 4507R switch equipped with dual supervisor modules that provide the fault tolerance needed in the core. Its flexible chassis design allows for different line cards to match the number of uplink ports required.

Server Room and Campus Access

Both the server room and the campus access have the primary responsibility of connecting devices to the network. The main difference is the requirement in the campus access for Power over Ethernet (PoE). We have selected two product lines from which to choose: the Cisco Catalyst 3560 and Cisco Catalyst 3750 switches.

The Cisco Catalyst 3560 switch is an economical, nonstackable, Fast Ethernet or Gigabit Ethernet fixed-port product line that provides flexibility and features for many access-level switching environments. It comes in PoE and non-PoE versions. The Cisco Catalyst 3750G switch is a stackable Gigabit Ethernet fixed-port product line with higher overall capacity because of its 32-Gbps backplane and StackWise technology.

Both Cisco Catalyst 3560 and Cisco Catalyst 3750 switches include 10/100/1000 ports with PoE. While a PoE-capable device is not required in the server room, the marginal cost difference ensures a single product line can be used across multiple modules and repurposed as the infrastructure grows.

Why select a PoE-capable switch? PoE supports IP telephony, wireless access points, security cameras, and other low-power devices. PoE enables devices to be powered in a location using the twisted-pair cable without the expense of installing or modifying the building power in locations (such as in ceilings for installing cameras and wireless access points [AP], for example). Including PoE in the switch future proofs the network for the addition of these technologies without the need for the added cost of re-engineering the network foundation. While the configurations are different, the management and ability to use a single product line between multiple modules lowers operational expenses.

WAN Module

The headquarters WAN is the point of connection between the main office and remote branch locations. In this design, the WAN assumes that private and secure connections are provided by a service provider. While the design includes Internet access, the Internet is not used for connectivity between locations. The WAN interconnects all locations and aggregates traffic for the Internet at the headquarters.

When selecting a device, Cisco also considered the ability to support additional functions and services. Beyond the primary function of routing traffic between locations, the device may need to support voice media and gateway services in addition to optimization and security functions through the expansion capabilities provided by plug-in modules.

Given all these requirements, the **Cisco 3845 Integrated Services Router (ISR)** was the clear choice. The Cisco 3845 ISR is a flexible, modular platform enabling high-speed routing and other services, such as voice, for connectivity needs between the campus/headquarter and remote branch locations.

The remote **branch** locations need to support up to 20 users with computers, IP phones, and wireless. The computers will be using desktop applications as well as email and other company applications, which are accessed over the WAN to the server room at the headquarters. The IP phone system also needs to be supported through the WAN. The local switch should support PoE for the IP phones and wireless AP, so they do not require external power.

In addition, QoS and WAN optimization offer cost savings by efficient use of the LAN and WAN. Additionally, threat mitigation security measures are provided as remote workers often have laptop computers that are placed on unsecure networks.

The **Cisco 2811 ISR** is the platform that meets the requirements for connecting the branch via the WAN back to the headquarters. It provides integrated services with the Intrusion Protection System (IPS), Advanced Integration Module (AIM) for security, and Wide-Area Application Services Network Module (NM) for optimization of data, voice, and video over the WAN.

For computer, IP phone, wireless AP, and other office network connectivity, the **Cisco 3560G** (either 24 or 48 ports), is the product selected at the branch for this design. It enables simple network access plus the required PoE. In keeping with the principle of ease of use, it has the same command set as the Cisco Catalyst 3750 switches and other Cisco Catalyst 3560 switches used in the campus, keeping deployment and operational cost to a minimum.

The final device is the wireless AP. In this design, the **Cisco AIR-LAP1140** Series was chosen as it is a PoE-capable product that can be centrally managed from the headquarters using a wireless LAN controller.

Security Module

Within the design, there are many requirements and opportunities for security features. The deployment guide has already covered a few, including IDS on the WAN and branch, VPN software and hardware for the mobile teleworker and small office or home office (SOHO) worker. There is also a certain level of security at the access port level where office devices are connected to the switch; this will be covered in more detail in the individual 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 5510**. The ASA 5510 is a hardened multifunction device providing firewall capability, VPN, and SSL VPN access for remote/mobile users. It also has a slot for an additional services module, and in this design, the additional services module added is the IPS module.

IPS SSM Functionality

The IPS module adds the ability to inspect application layer data for attacks and block malicious traffic.

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, an alert can be sent to the appropriate resource, and an action can be taken to resolve the issue.

Teleworker and Remote worker

The foundation for both teleworkers and remote workers is the use of virtual private network (VPN) technologies.

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 provides a software VPN client for this purpose.

Teleworkers are users that work from a primary location that is neither the main office nor a remote branch. This location is typically a home office. Most teleworkers' activities don't warrant the cost of a dedicated WAN connection to the main office, but still have many of the connectivity requirements of the branch or office worker. Therefore, connecting back to the main office via the Internet is more economical, but the Internet is inherently insecure. They need to connect a computer, IP phone, and perhaps a printer and wireless AP at their location. The teleworker needs a secure connection and ports for their networked office equipment, which includes PoE for their IP phone and AP.

The **Cisco ASA 5505** is a perfect match for this situation. It is an economical, full-functioning firewall with eight 10/100 ports (two of which are PoE) to support an IP phone and/or AP. The Cisco ASA 5505 also provides a hardware-based VPN for secure connections from the teleworker location back to the headquarters. The device can be preconfigured before being shipped to the teleworker location. It is both simple to use and deploy while providing the required security.

UC/IP Telephony Module

Companies are looking to maximize the return on investment in their data network infrastructure. One of the more widespread technologies being deployed is IP telephony. IP telephony is basically the migration of the old standalone phone switch to a software-based switch—and the use of the data network as the physical transport for voice communications, rather than a separate cabling plant for data and voice communications. The market category that defines IP telephony and other forms of communications, including video, is known as unified communications (UC). This design ensures all modules support Cisco UC solutions from the onset. Therefore, no additional work or re-engineering of the network foundation is required to add Cisco UC, specifically IP telephony, to this design.

Cisco's Unified Communications has two software components. The first is the **Cisco Unified Communications Manager**. The communications manager is the hub for interconnecting and managing IP telephony and other communication applications. The second is the **Cisco Unity® Connections**. Unity connections provide services such as voicemail for 1000 users, voicemail integration with your email inbox, and many other productivity features.

Because UC applications, such as IP telephony and voicemail, have different processing and storage requirements based on the number of users and the features applied, it is important to select the appropriate platform based on expected usage. This design recommends the **Cisco Unified Communications MCS 7835** and the **Cisco Unity Connections MCS 7825**.

Wireless Module

As the work environment becomes more mobile, the needs of companies are changing—and Cisco technology and products are evolving to meet those needs. With a focus on the expanding wireless capabilities, Cisco recommends using a wireless mobility network for voice and data services in order to provide data connectivity for employees, voice connectivity for wireless IP phones, and wireless guest access for visitors to connect to the Internet.

Utilizing a Wireless LAN Controller approach simplifies deployment, security and operations when compared to multiple standalone Access Points. In addition guest access, client management, AP management, upgrade, rouge AP detection and performance monitoring all become centralized. In addition the WLC approach provides the foundation for advanced wireless mobility features, services and scalability.

WAN Optimization Module

Remote branch locations must connect back to the main office. This connectivity affects the bottom line of a business and, therefore, it's critical to maximize its usage for cost-effectiveness. In the last three to four years, a new class of product, called **WAN Optimization**, has allowed greater amounts of voice and data to traverse these links without incurring the additional cost of buying more bandwidth. Similar to the UC module, the ability to add WAN Optimization with minimal cost and effort is an essential requirement.

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

The WAAS solution is comprised of three components, an application acceleration device at each branch location, an application acceleration endpoint at the headquarters that acts as a collection point for the remote locations, and a Central Manager that is the control point for the entire WAAS solution. In the lab, we used a Cisco Wide-Area Engine (WAE) 502 NM within the router at the branch, a Cisco WAE 512 appliance for the application acceleration endpoint at the headquarters, and a Cisco WAE 512 as the central manager at the headquarters.

Please refer to the WAAS Configuration Guide on Cisco.com or contact a Cisco WAAS specialist when designing your WAAS solution to ensure optimal performance.

TECH TIP: Any underlined command is wrapped to fit this document's format and should be entered at the command line as one complete command.

Technology Overview

Within the Midsize Networks design, there are some settings that are common across multiple systems. There are also system settings that simplify and secure the management for the solution. This module provides recommendations for those settings. The actual setting and values will depend on your current network configuration. Please review all settings and configuration changes before submitting them.

For reference, the configuration files for the products used in this deployment guide are in the Appendix.

Each section and module in this deployment guide contains commands or screens meant to guide the reader through the steps to configure a specific product. In most cases, the command or screen is preceded by a description of what the command or screen is used for.

Text in italics and colored to match the specific module are commands to be entered at the command line of a product. There are also some "boot wizards." These are command line step-by-step instructions that walk the user through the configuration of a specific product and require a console connection.

Please read through each module before attempting the installation so you are fully familiar with the commands and design and their potential impact to your network.

System Administration

Usernames and Passwords

Password encryption should be enabled. Adhere to your corporate standards to address compliance requirements with both internal and external guidelines and regulations.

TECH TIP: Text in italics and colored to match the section are commands to be entered at the command line.

!Set password and encrypt

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

Each device is directed back to the same system for its internal clock synchronization. The devices should be set to your local time zone.

!Synchronize system clock and local time zone
clock timezone UTC -8

```
clock summer-time UTC recurring
!
```

Set VLAN Trunking Protocol to transparent. This forwards VTP information from other switches, but does not incorporate VTP updates in the local database. Switches in transparent mode are not active members of a VTP Domain. They store their own VLAN configuration in NVRAM.

```
vtp mode transparent
```

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. All connected devices must support UDLD for the protocol to successfully identify and disable unidirectional links. When UDLD detects a unidirectional link, it disables the affected port 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 port trunks, especially with fiber, which can be susceptible to unidirectional failures.

In normal mode, if the link state of the port is determined to be unidirectional, then the port will continue to forward traffic normally but will be marked as "undetermined." The port will cycle through the regular Spanning Tree Protocol states and will continue to forward traffic. In aggressive mode, the port will enter "errdisable" state and will be effectively shut down. To recover from "errdisable," you have to shut down and restart the port by issuing the shut and no shut commands. UDLD does not function any differently for either mode. The same messages are sent and the same messages are expected to be received. The modes only differ in the way that UDLD reacts to a unidirectional link failure.

```
udld aggressive
```

SSH

It is recommended that you enable SSH for remote management. Set SSH to version 2 as it is more secure than version 1 and is supported by most SSH clients.

When enabling SSH, you will need to generate RSA Keys. The following is an example of the commands to enable SSH and secure the access request via an access list.

```
ip domain-name [domain name]
Ip ssh version 2
crypto key generate rsa general-keys modulus
2048
```

TECH TIP: All IP addresses, VLAN numbers, and other specific values used in the configuration guide are for example purpose only.

Secure authentication can be enabled either locally or using an authentication server. Again, it is best to adhere to your company policies.

```
line vty 0 15
  login local
  transport input ssh
  access-class 55 in

access-list 55 permit 192.168.28.0 0.0.0.255
```

Domain Name Services

Using a fully qualified domain name rather than the IP address ensures access to the network, services, and specific devices even if the IP addresses change. It is also required for the IP telephony gateway. In our configuration, we added DHCP services in the core. Below are two examples of the pools of IP addresses for "access" clients and "voice" clients, including the domain name and DNS server IP to enable DNS service. Option 150 in the voice pool is a specific configuration command defining default gateway and the TFTP Server IP Address for voice services.

```
ip dhcp pool access
   network 192.168.8.0 255.255.255.0
   default-router 192.168.8.1
   domain-name [cisco.com]
   dns-server 192.168.28.10

ip dhcp pool voice
   network 192.168.12.0 255.255.255.0
   default-router 192.168.12.1
   dns-server 192.168.28.10
   option 150 ip 192.168.28.20 192.168.28.21
   domain-name [cisco.com]
```

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).

HTTP Access

These enable the use of the web-based GUI for both standard HTTP (TCP 80) and HTTPS (TCP 443).

```
ip http server
ip http secure-server
```

Each device is directed back to the same system for its network time synchronization. The devices should also be set to your local time zone.

TECH TIP: If you only want to allow secured access to the switch web interface, remove the command "`ip http server`"

Setting Spanning Tree

The design ensures there are no loops, but if any physical or logical loops are accidentally configured, the spanning-tree commands will ensure no actual routing loops occur.

```
spanning-tree mode rapid-pvst
spanning-tree extend system-id
spanning-tree vlan 1-1005 priority 24576
```

For network management, each device has a read only (cisco) and read write (cisco123) SNMP community defined. SNMP version (2c) was used.

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

VLAN Configuration

VLAN configuration has been simplified by matching the VLAN number to the IP subnet.

Headquarters

Vlan1	Management	192.168.1.0
Vlan8	HQ Data	192.168.8.0/24
Vlan10	HQ Wireless Data	192.168.10.0/24
Vlan12	HQ Voice	192.168.12.0/24
Vlan14	HQ Wireless Voice	192.168.14.0/24
Vlan16	Wireless Guest	192.168.16.0/24
Vlan28	Server Farm A	192.168.28.0/24
Vlan29	Server Farm B	192.168.29.0/24
Vlan31	Core Routing	192.168.31.0/24

Branch

Vlan64	Wired Data	192.168.64.0/24
Vlan65	Wired Voice	192.168.65.0/24
Vlan69	Wireless Data	192.168.69.0/24
Vlan70	Wireless Voice	192.168.70.0/24

Network Management

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 also provide a GUI. The extent to which each device can be configured after the initial boot setup from a GUI varies product by product.

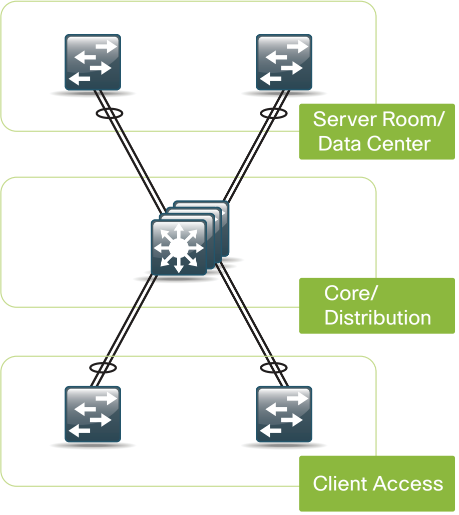
There are also a number of third-party tools available for day-two management. Once you have completed the deployment, these tools provide critical information in monitoring the network and applications and troubleshooting any problems that may arise.

Notes

Technology Overview

One of the most exciting advancements in this module is the resilient core design. This design diverges from current Core/Distribution/Access local-area network (LAN) models in several ways and, as shown in the diagram, the major change is in the core of the network. Instead of a pair of core boxes, there is a Resilient core. Physically, the core can be a stack of Cisco Catalyst 3750 switches or a highly available Cisco Catalyst 4507R switch. It is important to note that 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 has independent power and processors for each switch in the StackWise stack and the Cisco Catalyst 4507R switch has redundant supervisors, line cards, and power. Additionally, growth of the core is easily accomplished without the need for an outage by adding line cards to the Cisco Catalyst 4507R switch or by adding switches to the Cisco Catalyst 3750 stack.

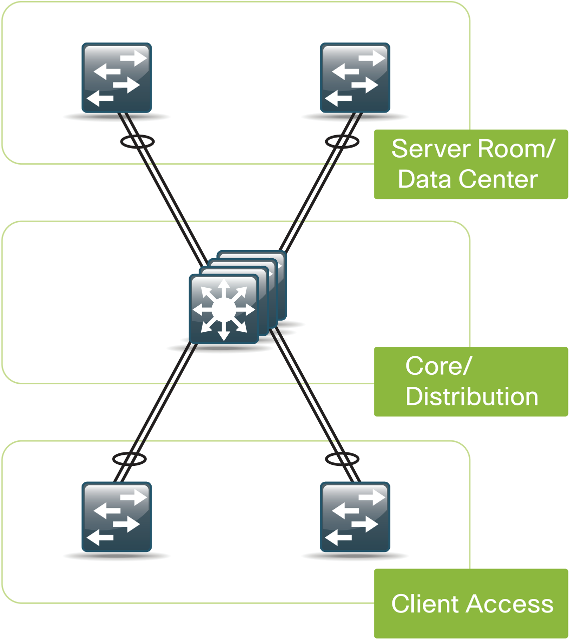
Campus Network



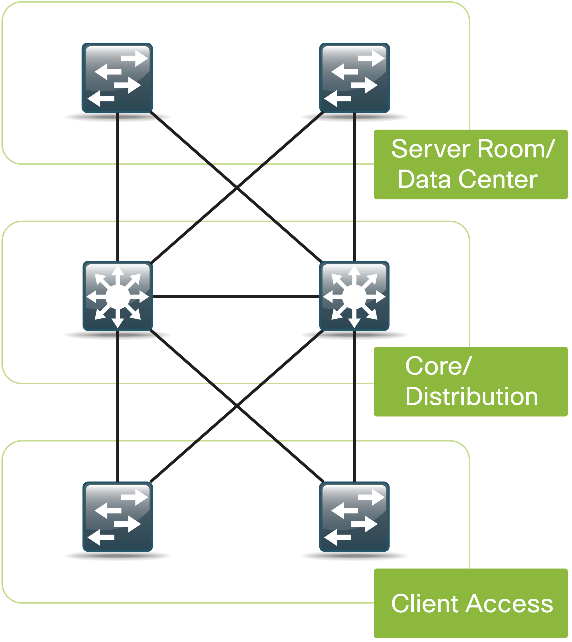
Resilient Core Design vs Dual Core Design

With a dual core design, each access layer switch has an uplink to each core switch.

Resilient Core Design



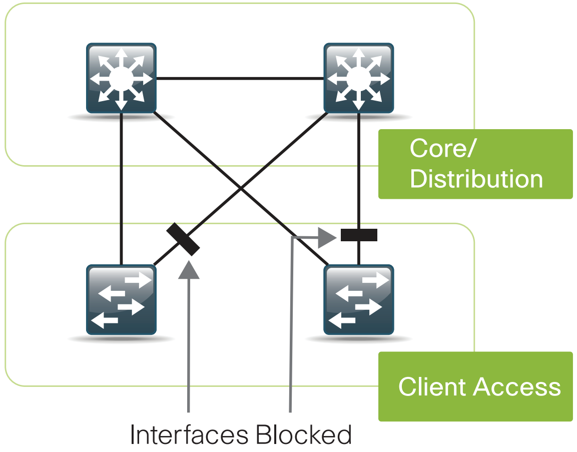
Dual Core Design



Dual Core Design

If the same VLAN is used across multiple access switches, then Spanning Tree Protocol has to be run to prevent Layer 2 loops in the network. Spanning tree has two main drawbacks: it has a slow recovery time when compared to other technologies; and to prevent loops, it has to block one of the Gigabit Ethernet links from the access layer, thus cutting the available bandwidth in half. To avoid the longer spanning-tree recovery times, it is possible to only carry the VLAN from the access to the core and to not trunk the VLAN between the two core switches, creating a "V" design so there is no looped topology. This allows for faster failure recovery, but it means that you have to configure separate VLANs for each access switch. In the past, this was an acceptable solution. But today, with voice and data VLANs for wired and wireless traffic, the number of VLANs and subnets that need to be configured can get large and unwieldy fast. IPv4 hosts only support a single default gateway.

Traditional Design with HSRP



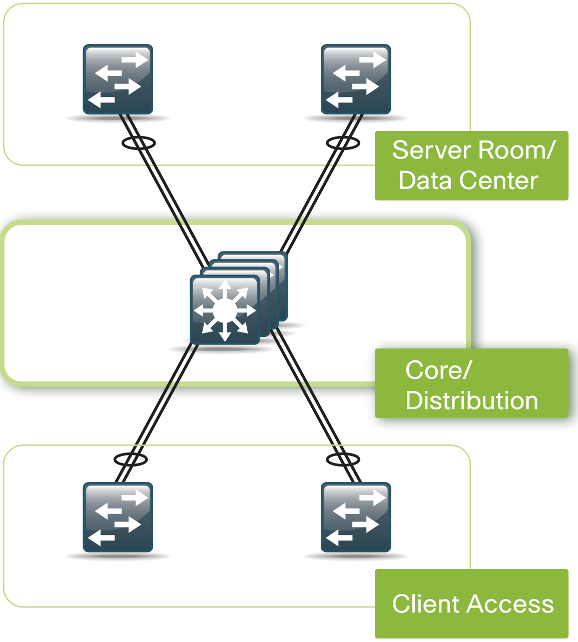
To make this single gateway address highly available, a first-hop redundancy protocol is used to make sure that the gateway IP is on a healthy switch. HSRP, GLBP, and VRRP are examples of first-hop redundancy protocols that are used to gain gateway redundancy. HSRP and VRRP are the most common FHRPs, but they only allow hosts on a VLAN 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 between the two core routers. Return traffic, which is typically the majority of the volume, is not load balanced, so the benefit does not adequately address the needs of most systems.

The Benefits of Resilient Core

With the resilient core model, both uplinks from the access go to the core as a Gigabit EtherChannel link split across multiple blades if the core is a Cisco Catalyst 4507R switch, or switches if the core is a stack of Cisco Catalyst 3750 switches. To the core and access switch, this appears as a single link.

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

Campus Network



With a **loop-free topology**, no failures require Spanning Tree Protocol to reconverge and recovery times are faster. Without loops, no uplinks are blocked; both links from the access switch to the core are load balanced via EtherChannel, so inbound and outbound data is split across the links for a more effective use of the links. It is also 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.

The core only has a single logical interface for each VLAN from the access layer. This eliminates the need to run a first-hop routing protocol, reducing the complexity of the configuration. If the access layer is large and requires multiple switches, they can be stacked and the EtherChannel uplink can be split across switches in the stack to minimize the impact of a switch or link failure or a larger Cisco Catalyst 4507R switch can be used in place of three or four stacked switches with a single chassis-based switch.

The server room switches can be stacked or separate and are connected to the core via EtherChannel uplinks just like the access layer switches. Servers can be dual homed into two standalone switches or connected to separate member switches in a stack for high availability and load balancing with “NIC teaming” (802.3ad port channeling).

The Core Configuration

The resilient core design simplifies the core configuration when compared to existing dual core models. Since the global configuration has been covered, we will now cover core-specific configuration only. The following is the core configuration for Cisco Catalyst 3750 Series switches and should work on any model in that product line. The switches used in this design were two Catalyst 3750G-12S stacked. Also included are any changes that are needed to make the configuration work on a Cisco Catalyst 4507R Core switch.

Layer 2 Configuration

With a resilient core design, we have a hub-and-spoke or star design. Even though we do not have spanning-tree blocking links in this design, the core should be configured to be root for all spanning-tree instances.

```
spanning-tree mode rapid-pvst
spanning-tree vlan 1-1005 root primary
```

TECH TIP: Spanning Tree Protocol should never be turned off. If a switch is cabled incorrectly or misconfigured, it could result in a loop that could cause a network outage.

EtherChannel links are provisioned from the core to the access layer and server farm switches, WAN router, and wireless LAN controller (WLC). When physically attaching devices to the core with an EtherChannel, is it important that the links be on separate switches in the core stack. For simplicity in the design, we channeled each port on the first Cisco Catalyst 3750 switch with the same port on the second Cisco Catalyst 3750 switch, so 3750-1 interface Gigabit Ethernet 1/0/1 was put in the same port channel as 3750-2 interface Gigabit Ethernet 2/0/1. In the CLI, EtherChannels are configured on interface port channels. It is recommended that you cable the devices together first before initiating the EtherChannel commands. The port channels for these links are configured as follows:

```
interface Port-channel1
 switchport trunk encapsulation dot1q
```

NOTE: The VLAN number used in this guide is for example purpose based on Cisco lab testing. The values you use may differ. Only necessary VLANs should be allowed on links (e.g., for access 1,8,12).

```
switchport trunk allowed vlan [VLAN]
switchport mode trunk
```

Here is the port channel configuration for the Cisco Catalyst 4507R switch:

```
interface Port-channel1
 switchport
 switchport trunk allowed vlan [VLAN]
 switchport mode trunk
```

The Cisco Catalyst 4500 Series does not need the command "switchport trunk encapsulation dot1q" and needs the command "switchport" because the ports are routed ports by default.

The port configuration is identical on the physical ports that make up the EtherChannel. Port channels are associated with physical interfaces with the channel-group command. The following example is from the Cisco Catalyst 3750-12s switches used in the lab; in this configuration, the interfaces Gigabit Ethernet 1/0/1 and 2/0/1 were used.

The links from the core need to carry multiple VLANs in most cases. To accomplish this, 802.1Q VLAN tagging is used. The switch port is configured as a trunk so it can carry several VLANs on one physical link, and the encapsulation type is set to dot1q. Limiting or pruning the VLANs that can exist on the link to the one that needs to exist on the switch on the other end is considered a best practice. This is accomplished with the "switchport trunk allowed vlan" command.

```
interface GigabitEthernet [port number]
 switchport trunk encapsulation dot1q
```

These ports connect to an access layer switch so only access VLANs are allowed over the trunk.

```
switchport trunk allowed vlan 1,8,12
switchport mode trunk
mls qos trust cos
auto qos voip trust
```

Channel groups that span multiple switches in a stack must be set to "on."

```
channel-group 1 mode on
spanning-tree link-type point-to-point
```

The Cisco Catalyst 4507R switch does not require "switchport trunk encapsulation dot1q" and does not support auto QoS on trunk ports.

Port configuration for connection to the WAN router:

```
interface Port-channel12
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 31
 switchport mode trunk

interface GigabitEthernet [port number]
 switchport trunk encapsulation dot1q
```

Only the VLAN that is used for LAN WAN interconnectivity is allowed on this trunk; it is configured for a trunk so that later it is easy to add additional VLANs for future services.

```
switchport trunk allowed vlan 31
switchport mode trunk
mls qos trust dscp
auto qos voip trust
channel-group 12 mode on
spanning-tree link-type point-to-point
```

For devices that are dual homed to the core for high availability, but do not connect via EtherChannel, like the firewalls, here is the configuration. No port channel is configured here because the firewalls each have a separate inside interface.

```
interface GigabitEthernet [port number]
 switchport trunk encapsulation dot1q
```

Core routing VLAN and guest VLAN are allowed to the firewall.

```
switchport trunk allowed vlan 16,31
switchport mode trunk
spanning-tree link-type point-to-point
```

Layer 3 Configuration

EIGRP was chosen as the routing protocol because it is easy to configure, does not require a large amount of planning, and can scale to large networks. EIGRP routing configuration:

```
ip routing
router eigrp 1
```

If there is another address space besides what is listed, then another network statement would be needed here.

```
network 192.168.0.0 0.0.255.255
no auto-summary
passive-interface default
```

All routing devices are connected to VLAN 31 in the core.

```
no passive-interface Vlan31
```

Multicast allows a single stream of data to be sent to multiple endpoints simultaneously and more efficiently than unicast.

```
Multicast routing configuration:
ip multicast-routing distributed
```

On the Cisco Catalyst 4500 Series, use the command:

```
ip multicast-routing
```

Specify the interface that connects to the WAN as the PIM BSR and RP candidate. In this network it is Vlan31.

```
ip pim rp-address 192.168.31.1
```

Add the following command to all interfaces:

```
ip pim sparse-mode
```

If there is no external server for address assignment, an IOS DHCP server can be run on the core switch. This prevents the IOS DHCP server from assigning addresses 1-10 for network 192.168.8.0/24:

Here is an example of a single scope:

```
ip dhcp excluded-address 192.168.8.1
192.168.8.10
ip dhcp pool access network 192.168.8.0
255.255.255.0
default-router 192.168.8.1
domain-name [cisco.com]
dns-server [DNS server IP]
```

If you are running an external DHCP server, you need the following command on the VLAN interfaces:

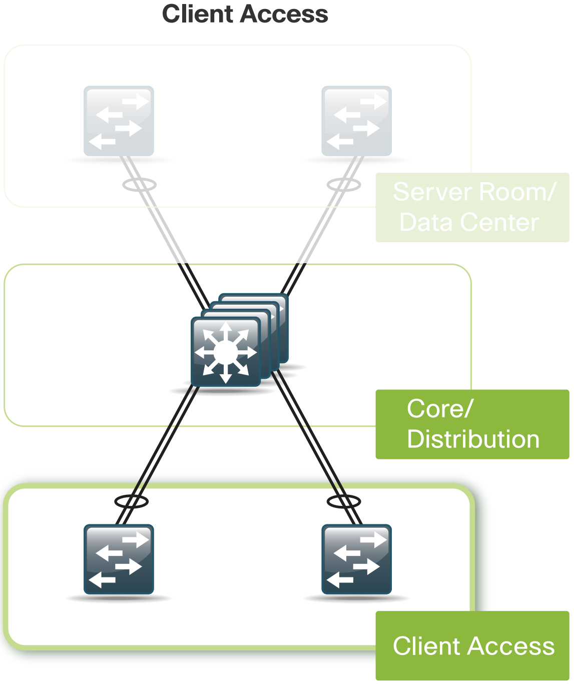
```
ip helper-address xxx.xxx.xxx.xxx
```

This represents the IP address of your external DHCP server.

TECH TIP: At the end of each section within a module, you may want to check the running configuration file against the configuration file in the appendix of this deployment guide to ensure accuracy of the configuration.

Notes

Technology Overview



Client Access

In this design, the access layer configuration is very simple. It was designed so that the same port configuration can be used for a standalone computer, an IP phone, an IP phone with an attached computer, or wireless access point. For **added security** at the access layer, several port-level features have been enabled. **Port security** limits the number of MAC addresses that can be active on a single port. This protects against MAC flooding attacks. **DHCP snooping** prevents rogue DHCP servers from operating on the network and helps protect against DHCP starvation attacks. **ARP inspection** ties an IP address to a MAC address and protects against ARP spoofing attacks. And **IP source guard** prevents attacks that use spoofed source IP addresses.

The access layer switch can be standalone or a switch stack. The connection from the access to the core is an EtherChannel. If there are multiple switches in a stack, the channel should be split across switches in the stack to improve high availability. If there are three or more switches in the stack, the uplinks should be on switches that are not stack master. To configure a switch to be the stack master, use the following command:

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

To make access port configuration easier, the switches support the range command. This allows you to issue a command once and have it apply to several ports at the same time. Since most of the ports in the access layer will be configured identically, it can save a lot of time. For example, the command:

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

would allow you to enter commands on all 24 ports (Gig 0/1 to Gig 0/24) simultaneously.

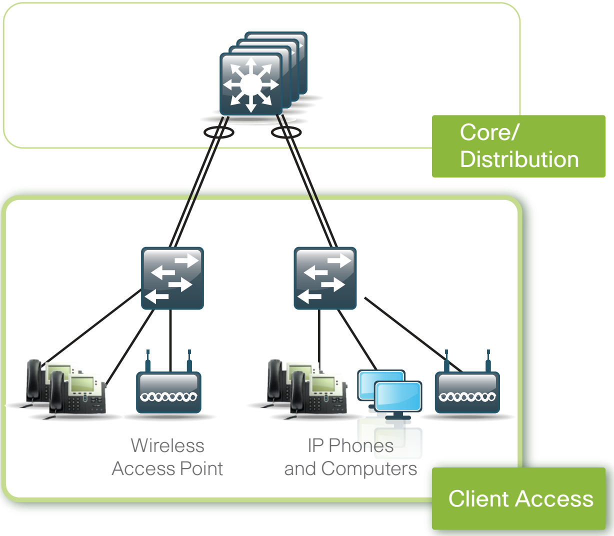
NOTE: There are variants of this command based on the type of ports and specific switch being configured.

To configure DHCP snooping and ARP inspection, there are a few global switch commands that are needed:

```
ip dhcp snooping vlan [VLAN range]
ip dhcp snooping

ip arp inspection vlan [VLAN range]
```

Here is the configuration for the port channel. The VLANs allowed on the trunk are pruned to only the VLANs that are active on the access switch. ARP inspection and DHCP snooping are set to trust on the uplink ports as hosts do not plug directly into them so no inspection is needed.



```
interface Port-channel1
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,8,12
 switchport mode trunk
 ip arp inspection trust
 ip dhcp snooping trust
```

The physical interfaces for the EtherChannel are configured as trunks with only the necessary VLANs allowed. QoS is trusted here since it is on a network link and not connected directly to a host.

ARP inspection and DHCP snooping is also trusted because it is a network infrastructure connection.

```
interface GigabitEthernet [port range]
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,8,12
 switchport mode trunk
 ip arp inspection trust
 mls qos trust dscp
 auto qos voip trust
 channel-group 1 mode on
 spanning-tree link-type point-to-point
 ip dhcp snooping trust
```

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

```
interface GigabitEthernet [port number]
 switchport access vlan [data VLAN]
 switchport mode access
 switchport voice vlan [voice VLAN]
```

Allows 11 MAC addresses to be active on the port; additional MAC addresses are considered to be in violation and their traffic will be dropped:

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

Sets the aging time to 2 minutes:

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

Restrict will drop traffic from MAC addresses that are in violation, but will not shutdown the port so an IP phone will still function:

```
switchport port-security violation restrict
switchport port-security aging type inactivity
ip arp inspection limit rate 100
```

Tells the switch to trust the QoS markings from the phone:

```
mls qos trust device cisco-phone
mls qos trust cos
auto qos voip cisco-phone
```

Shortens the time it takes for the port to go into a forwarding state:

```
spanning-tree portfast
```

Disables the port if another switch is plugged into the port:

```
spanning-tree bpduguard enable
ip verify source
ip dhcp snooping limit rate 100
```

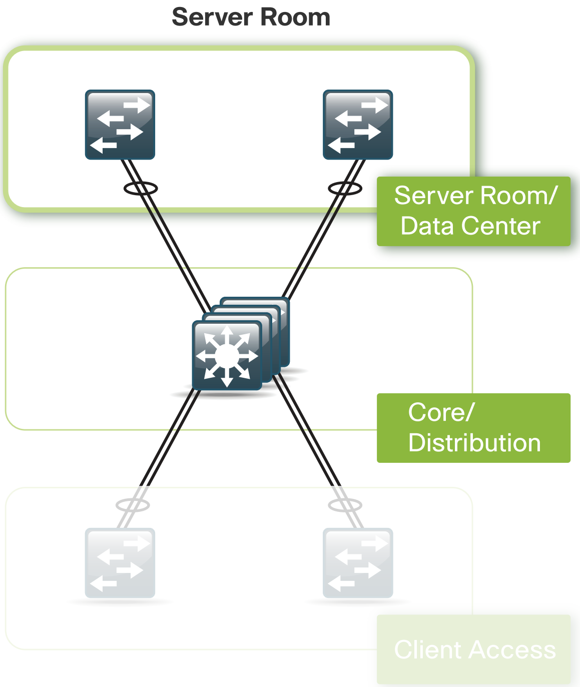
TECH TIP: Ports that become error disabled will not automatically recover and have to be manually enabled. To enable automatic recovery, use the global command

```
errdisable recovery cause all
```

Notes

Server Room

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.



Here is the config for the EtherChannel to the core:

```
interface Port-channel1
 switchport trunk encapsulation dot1q
```

VLANs pruned to just the ones that are active in the server farm:

```
switchport trunk allowed vlan 1,28-29
switchport mode trunk

interface GigabitEthernet [port numbers that match the vlans]
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,28-29
 switchport mode trunk
 mls qos trust dscp
 auto qos voip trust
 channel-group 1 mode on
 spanning-tree link-type point-to-point
```

Here is a sample port configuration for server connectivity. The server ports trust the QoS marked by the server. This is required for UC servers in the solution and may be needed depending on the applications running on other servers:

```
interface GigabitEthernet1/0/1
```

Set the port to the VLAN that you want the server to be a member of:

```
switchport access vlan [vlan]
switchport mode access
mls qos trust dscp
auto qos voip trust
spanning-tree portfast
spanning-tree bpduguard enable
```

Notes

Technology Overview

Quality of service (QoS) is an essential function of the network infrastructure devices used throughout this design. QoS **enables** a multitude of user services and applications, including **real-time voice, high-quality video, and delay-sensitive data, to coexist** on the same network. In order for the network to provide predictable, measurable, and sometimes guaranteed services, it must manage bandwidth, delay, jitter, and loss parameters. Even if you do not require QoS for your current applications, the use of QoS for management and network protocols protects the network functionality and manageability under both normal and abnormal traffic conditions.

The **goal** of this design was to provide sufficient classes of service to allow voice, interactive video, critical data applications, and management traffic to be added to the network either from the initial deployment or in later phases with minimum system impact and engineering effort.

The following QoS classifications are applied throughout this design. This table is for reference only.

Application	Layer 3 Classification			Layer 2 CoS
	IPP	PHB	DSCP	
IP Routing	6	CS6	48	6
Voice	5	EF	46	5
Interactive Video	4	AF41 AF42	34 36	4
TelePresence	4	CS4	32	4
Locally Defined Mission-Critical Data	3	AF31	26	3
Call Signaling	3	CS3	24	3
Transactional Data	2	AF21	18	2
Network Management	2	CS2	16	2
Bulk Data	1	AF11	10	1
Scavenger	1	CS1	8	1
Best Effort	0	0	0	0

QoS Configuration

The network infrastructure QoS configuration for this design will be split into two sections: local-area network (LAN) and wide-area network (WAN). QoS-specific configurations for other technologies that will utilize the network infrastructure will be covered in those respective sections.

Local-Area Network

The switches used in this design all use the following basic configuration commands:

```
mls qos
```

This command enables QoS globally, within the switch, and must be enabled prior to any QoS commands listed below. After `mls qos` has been enabled, the most effective way to configure QoS for platform-specific best practices is to use one of the `auto qos` interface commands. For all wired access ports, we recommend using the `cisco-phone` version. This allows for an untrusted personal computer and/or a trusted Cisco® IP phone to be connected and automatically sets QoS parameters:

```
auto qos voip cisco-phone
```

When this command is first applied, it will auto generate the mls global configuration, which includes QoS mapping and queuing configuration specific to the switch. Server farm switches will not normally have IP phones attached. Also, the default “trust” using this command is for class of service (CoS), which is not the typical method used by servers that classify their traffic. Therefore, for the server farm switches, we configure `auto qos voip trust` on the interface as this will auto generate the `qos global` commands. Then the default of trust CoS can be changed to trust DSCP as required on a per-interface basis using the mls qos trust dscp interface command.

All interswitch interfaces trust DSCP. We configured `mls qos trust` DSCP on all access, server farm, and core interfaces that provide interswitch connections.

Before covering the (WAN) QoS, we should mention some specific requirements for other technologies deployed on the foundation network. The wireless access points (APs) for this design allow for their placement on any access port with autoconfiguration of IP address and the wireless LAN controller (WLC). However, the default QoS for access ports is to distrust IP phone devices from vendors other than

Cisco. Therefore, the AP access port QoS configuration needs to be modified to the following:

NOTE: The specific port configured is based on where the AP is plugged in.

```
interface GigabitEthernet1/0/3
 auto qos voip trust
 mls qos trust dscp
```

This interface configuration is the same for interswitch uplinks, switch to router links, wireless LAN controller, Cisco Unified Communications Manager, and Cisco Unity Connections appliances.

Wide-Area Network

Due the variety of WAN interfaces and service provider offerings, it is advised to consult with the service provider for specific configuration details for connecting to their WAN service. The following description will explain the basic concepts and how to provision bandwidth for future traffic needs. The following is a sample configuration that provides for Unified Communications (UC) of voice and video, as well as prioritizing interactive data traffic. The QoS configuration for the WAN provides five additional classes of service in addition to the default Best Effort class. These additional classes can be configured even if there are no plans to use them in the immediate future, as the bandwidth assigned is still available for other traffic. To further simplify the configuration in the design, the allocation of bandwidth is based on a percentage of the available interface or link speed.

The configuration is split into two parts: the first part maps QoS classifications to a class; the second part is then defined as a policy, which is then applied to the WAN interface. The first part is defined as follows:

```
class-map match-all Interactive-Video
match ip dscp af41  af42
class-map match-any Network-Control
match ip dscp cs6
match ip dscp cs2
class-map match-all Critical-Data
match ip dscp af21  af22
class-map match-all Call-Signalling
match ip dscp cs3
class-map match-all Voice
match ip dscp ef
```

The above example defines classes for voice traffic, Interactive Video (video conferencing), Network Control (network protocols and management traffic), and Critical Data (highly interactive, such as telnet, Citrix, and Oracle thin clients).

The second part of the configuration uses the class names and defines the maximum guaranteed bandwidth allocated to each. One additional “default” class is also added that defines the minimum allowed bandwidth available for Best Effort traffic:

```
policy-map WAN
 class Voice
   priority percent 10
 class Interactive-Video
   priority percent 35
 class Network-Control
   bandwidth percent 10
 class Critical-Data
   bandwidth percent 15
   random-detect dscp-based
 class Call-Signalling
   bandwidth percent 5
 class class-default
   bandwidth percent 25
   random-detect
```

Normally, the sum of all the bandwidth allocations cannot exceed 75 percent, still allowing for 25 percent availability for network traffic. However, this can be changed using the interface command:

```
max-reserved-bandwidth
```

Notably, ensuring sufficient bandwidth is defined in the Network Control class for correct operation.

On lower-speed circuits, below a T1 or E1, additional bandwidth can be saved for voice traffic by enabling header compression if the router CPU is sufficient. By enabling this, you reduce a low bandwidth voice call using the G.729 code from 24 kbps to approximately 11 kbps. Header compression must be enabled at both ends of the WAN circuit to function. The additional command is added to the Voice class within the policy:

```
class Voice
 priority percent 10
 compression header ip rtp
```

Bandwidth provisioning is a key feature that defines our QoS policy based on typical traffic patterns. Voice bandwidth will be covered in the Unified Communications section. Video has been defined as a placeholder for a later phase, and as there is no video traffic, the bandwidth will be available to other traffic classes.

When we transition from the WAN to the LAN, we need to keep the QoS classifications used at Layer 3 (DSCP) consistent with Layer 2 (CoS) within the LAN. As the router at the campus is attached directly to the Core via Layer 3, there is no requirement there; however, at the branch where the router is connected to the LAN using Layer 2, we need to add the following commands to the branch router and apply them to the interface attached to the switch:

```
policy-map Lan-Edge
 class class-default
 set cos dscp
interface FastEthernet0/0.64
 description Access Subnet
 encapsulation dot1Q 64
 ip address 192.168.64.1 255.255.255.0
 service-policy output Lan-Edge
```

Technology Overview

The routers selected in this deployment model have been chosen because of their ability to provide data, voice, and video connectivity between sites and their capacity for routing traffic. The deployment includes various WAN and voice interfaces, as well as additional capacities for security, Wide-Area Application Services, and Cisco Unified Communications modules.

For the main site, a **Cisco ISR 3845** was selected in order to provide the routing capacity to support twenty remote sites, each with T1/E1 connectivity speeds or below. The router at the main site can also provide Unified Communications media resources and gateway functions. Therefore, it was configured with sufficient DSPs and a dual T1/E1 HWIC, which supports WAN and PSTN PRI configurations using a single HWIC slot.

The branch site routers were selected based on the speed of the WAN being a T1/E1, support for a WAAS NM, IPS Security AIM, PSTN interfaces, and Media resources for Unified Communications (including the ability to support Unified Survivable Remote Site Telephony users). The **Cisco ISR 2811** is the selected platform. Consistent with the main site, this router is provisioned with DSPs and a dual T1/E1 HWIC. If needed, the T1/E1 port can be used for PSTN PRI access to support Unified Communications.

NOTE: Any specific interfaces and IP addresses are examples based on the Cisco lab used to validate the Deployment Guide. Your interfaces and IP addresses may differ.

WAN Router Interface Configuration

Due to the breadth of WAN service offerings and multitude of possible hardware and software configurations, this deployment guide covers a generic example for a T1 /E1 leased line.

With the HWIC, either a T1 or E1 can be used, so it is necessary to specify the mode. This is achieved using:

```
card type t1 0 0
```

This is a global configuration command, where 0 0 specifies the HWIC is in card slot 0 and WIC slot 0.

Clocking for the router is configured to use Port 0 on the T1/E1 HWIC. First, the card must be enabled to provide clocking, and then, the clock is selected with a priority of 1 (highest) using the following global configuration commands:

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

The following commands select port 0 on the HWIC as the source of the clock, which is set to be recovered from the line, therefore, synchronizing to the service provider network. The second command may vary based on the service speed. In this deployment, however, the channel group command allocates all 24 timeslots to a serial interface 0/0/0:0, which is created after issuing this command:

```
controller T1 0/0/0
 clock source line primary
 channel-group 0 timeslots 1-24
```

The resulting serial interface from the channel group command allows us to configure the address required for the WAN. In our case, the network subnet was 10.0.1.0/30:

```
interface Serial0/0/0:0
 ip address 10.0.1.1 255.255.255.252
 ip pim sparse-mode
 load-interval 30
 max-reserved-bandwidth 100
 service-policy output WAN
```

To enable dynamic routing, we used EIGRP with the same autonomous system number as the other router and switches. Using the network command, we enabled EIGRP on all interfaces within the network range specified, all within this router:

```
router eigrp 1
 network 10.0.1.0 0.0.0.255
 network 192.168.0.0 0.0.255.255
 no auto-summary
```

LAN Headquarters Router Configuration

The headquarters router is connected to the core switches, and both Gigabit Ethernet interfaces use EtherChannel for high availability. Each interface is connected to a different switch or blade in the core stack or modular switch.

LAN interface configuration is:

```
interface Port-channel1
 no ip address
 hold-queue 150 in
!
interface Port-channel1.31
 encapsulation dot1Q 31
 ip address 192.168.31.2 255.255.255.0
!
interface GigabitEthernet0/0
 no ip address
 duplex auto
 speed auto
 media-type rj45
 channel-group 1
!
interface GigabitEthernet0/0.31
 channel-group 1
!
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
 media-type rj45
 channel-group 1
!
interface GigabitEthernet0/1.31
 channel-group 1
```

In addition to the EtherChannel configuration, we are defining the LAN interface as a trunk interface (802.1q). Now, and possibly in the future, there may be a need for another VLAN for additional purposes, such as wired guest access. By defining the configuration this way at the start, we can easily add further subinterfaces with minimum disruption.

LAN Branch Site Router Configuration

The branch site router configuration is similar to the headquarters, except that there is no EtherChannel and there are more subinterfaces since the router is providing Layer 3 switching at the branch:

```
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet0/0.64
 description Access Subnet
 encapsulation dot1Q 64
 ip address 192.168.64.1 255.255.255.0
!
interface FastEthernet0/0.65
 description Voice Subnet
 encapsulation dot1Q 65
 ip address 192.168.65.1 255.255.255.0

interface FastEthernet0/0.69
 description Wireless Access
 encapsulation dot1Q 69
 ip address 192.168.69.1 255.255.255.0

interface FastEthernet0/0.70
 description Wireless Voice
 encapsulation dot1Q 70
 ip address 192.168.70.1 255.255.255.0
```

The following configuration enables data, voice, wireless, and guest wireless access services at the branch.

NOTE: The subinterfaces and IP addresses used in this guide are specific to this deployment guide. Please ensure you use the right router interfaces and IP addresses for your deployment.

Notes

Technology Overview

As the work environment becomes more mobile, the needs of companies are changing—and Cisco technology and products are evolving to meet those needs. With a focus on the expanding wireless capabilities, Cisco recommends using a wireless mobility network for voice and data services in order to provide data connectivity for employees, voice connectivity for wireless IP phones, and wireless guest access for visitors to connect to the Internet.

With ease of deployment one of the core goals, this wireless network design is secure and expandable and covers the headquarters and branch sites connected via a WAN. It does not cover the radio frequency (RF) design.

What's New

In the past, the simplest approach was to use standalone access points (APs), yet each needed to be managed individually and lacked the ability to expand the functionality.

At the center of this new design is a **Wireless LAN Controller (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® 4400** Series that provides support for up to 100 APs each. For simplicity, the design uses a single unit, although multiple units can be grouped to provide additional capacity and high availability. In our design, we specifically used the Cisco 4402 WLC, which has two Small Form-Factor Pluggable (SFP)-based distribution ports that will be used to provide EtherChannel connectivity to the core switches or Cisco 4500 Series blades, and can be either copper or fiber, depending on distance and choice.

The APs used at the headquarters are **Cisco 1140 Series** Lightweight Access Points with 802.11a/b/g/n support. Power is provided by standard PoE from the switches, allowing APs to be deployed without installing or modifying existing building electrical outlets (which is often the case as APs are typically mounted on the ceiling).

The APs selected for the branch are **Cisco 1140 APs** providing 802.11a/b/g/n. In normal conditions, they operate in Lightweight mode; if connectivity between the branch and the headquarters is down, they operate in Standalone mode.

Deployment

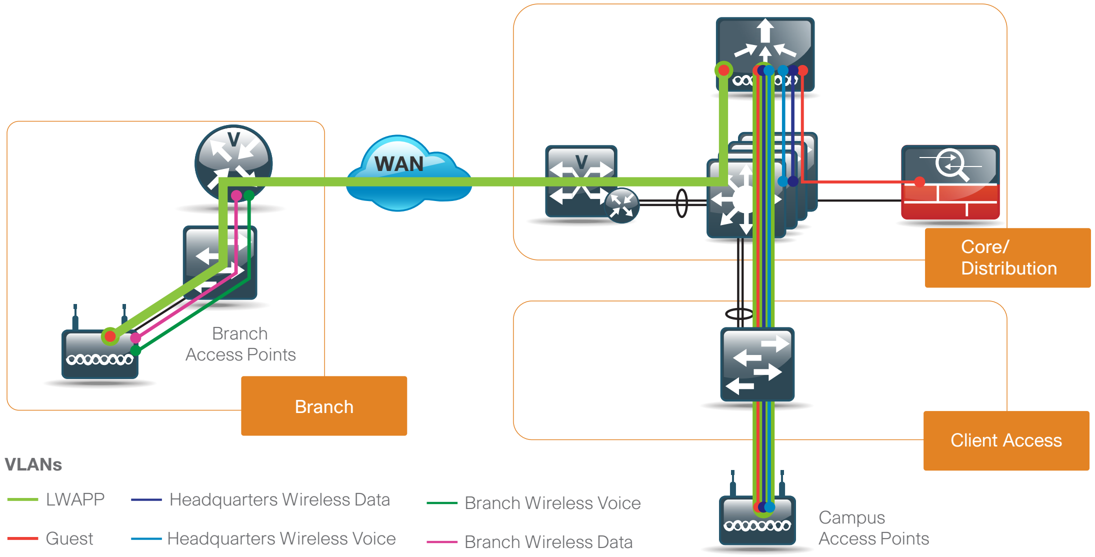
The deploying of wireless mobility requires a RADIUS server for authentication and a DNS entry for the APs to locate the WLC.

At the headquarters, there will be campuswide data wireless LAN (WLAN) and a separate voice WLAN that will be terminated at the WLC.

Each branch site will also have its own data and voice WLANs that will terminate within the branch to avoid traversing the WAN when accessing local resources. A single guest WLAN is deployed for the headquarters and all the branch sites, which is then tunneled back to the WLC and onto a specific VLAN that connects to the Adaptive Security Appliance (ASA) providing secure access to the Internet. The guest WLAN has no wireless security and uses open authentication. Access to the Internet is controlled using web authentication that uses an expiring guest account created locally on the WLC.

After the WLC is physically installed and powered up, connect distribution port 1 and 2 into core switch 1 and 2, respectively (or separate blades), and configure an EtherChannel between them. The VLANs used in the following configuration are for HQ wireless data (10), HQ wireless voice (14), and wireless guest (16), with VLAN 31 being used for the management and access point manager interfaces:

```
interface Port-channel11
 description WLAN Controller
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 10,14,16,31
 switchport mode trunk
```



```
interface GigabitEthernet1/0/11 and 2/0/11
 description WLAN Controller
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 10,14,16,31
 switchport mode trunk
 srr-queue bandwidth share 10 10 60 20
 queue-set 2
 priority-queue out
 mls qos trust dscp
 auto qos voip trust
 channel-group 11 mode on
 spanning-tree link-type point-to-point

interface Vlan10
 description Data WLAN
 ip address 192.168.10.1 255.255.255.0

interface Vlan14
 description Voice WLAN
 ip address 192.168.14.1 255.255.255.0

interface Vlan16
 description Guest SET NO IP ADDRESS
 no ip address

interface Vlan31
 description Network Services and WAN Router
 ip address 192.168.31.1 255.255.255.0
```

Use the following to deploy wireless mobility:

```
Management and AP-Manager VLAN is 31
Management Interface address 192.168.31.64/24
ap-manager Interface address 192.168.31.65/24
Default DHCP server address 192.168.1.1
Virtual Interface address 10.10.10.10
Mobility / RF group name = default
Initial SSID = CAB_Guest
```

Next, using the console port and after powering up the WLC, you will be prompted by a setup script. The onscreen prompts are in *italics* and the answers entered are in **bold**.

After the initial hardware boot process is complete, you will see the following on the screen:

Welcome to the Cisco Wizard Configuration Tool

Use the '-' character to backup

Would you like to terminate autoinstall? [yes]:no

Step 1: Enter a system name.

System Name [Cisco_7e:8e:43] (31 characters max): **HQ WLC**

Step 2: Enter an administrator username and password.

NOTE: Do not use the username below. When entering the passwords, the characters echo back as "*" symbols.

Enter *Administrative User Name (24 characters max):* **Admin**

Enter Administrative Password (24 characters max): *****

Re-enter Administrative Password : *****

Step 3: Use DHCP for the service ports Dynamic Host Control Protocol (DHCP) address.

Service Interface IP Address Configuration [none] [DHCP]: **DHCP**

Step 4: Enable Link Aggregation.

Enable Link Aggregation (LAG) [yes][NO]: **yes**

Step 5: Enter the IP address and subnet mask for the management interface (i.e., IP address **192.168.31.64**, netmask **255.255.255.0**, default gateway **192.168.31.1,** and VLAN **31**).

Management Interface IP Address: **192.168.31.64**

Management Interface Netmask: **255.255.255.0**

Management Interface Default Router: **192.168.31.1**

Management Interface VLAN Identifier (0 = untagged): **31**

Step 6: Enter the default DHCP server for clients.

(In this deployment guide, it is **192.168.1.1**, which is the DHCP server configured on the Core switches. Alternatively, this can be a DHCP server address in the server farm.)

Management Interface DHCP Server IP Address: **192.168.1.1**

Step 7: Enter the AP Manager address—this needs to be on the same subnet as the management interface (i.e., **192.168.31.0**).

AP Manager Interface IP Address: **192.168.31.65**

The AP Manager Interface DHCP server defaults to the same as the Management Interface DHCP server. Select the default by pressing the enter key.

AP-Manager is on Management subnet, using same values

AP Manager Interface DHCP Server (192.168.1.1):

Step 8: The virtual interface is used in our deployment for guest web authentication (i.e., **10.10.10.10**).

Virtual Gateway IP Address: **10.10.10.10**

Step 9: Enter a name that will be used as the default mobility and RF group (i.e., default). Select NO for Symmetric Mobility Tunneling.

Mobility/RF Group Name: **default**

Enable Symmetric Mobility Tunneling [yes][NO]: **no**

Step 10: Enter an initial SSID of Guest.

Network Name (SSID): **Guest**

Step 11: Enter no to make clients use DHCP IP Addresses.

Allow Static IP Addresses [YES][no]: no

Step 12: Enter no to configure RADIUS as we will configure this later using the GUI.

Configure a RADIUS Server now? [YES][no]: no

The default WLAN security policy requires a RADIUS server.

Step 13: Enter the correct country code for the country you are deploying in. (Enter help to get a list of valid country codes.)

Enter Country Code list (enter 'help' for a list of countries) [US]: US

Step 14: Enter yes to enable all wireless networks. (802.11a will typically be used for wireless IP Phones, 802.11b/g/n will typically be 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 15: Enable the WLC's radio resource management (RRM) auto RF feature by entering **yes**.

Enable Auto-RF [YES][no]: yes

Configure a NTP server now? [YES][no]: no

Configure the system time now? [YES][no]: yes

Enter the date in MM/DD/YY format: 12/01/08

Enter the time in HH:MM:SS format: 10:04:00

Configuration correct? If yes, system will save it and reset. [yes][NO]: yes

Configuration saved!

Resetting system with new configuration...

At this point, the WLC will save the configuration and reboot. When the onscreen prompt appears, enter the username and password used in Step 2.

To verify the basic installation, use show port summary to confirm that both ports are up and enabled. Use show port summary to confirm that the IP addresses and VLAN for the AP Manager and management interfaces are correct. Notably, the port used by both is Link Aggregation Group (LAG), which groups the two distribution ports together so that they can provide load balancing and high availability to the two core switches configured for EtherChannel.

Once all is confirmed, it will be possible to access the WLC GUI by using a web browser through a client connected to the wired network:

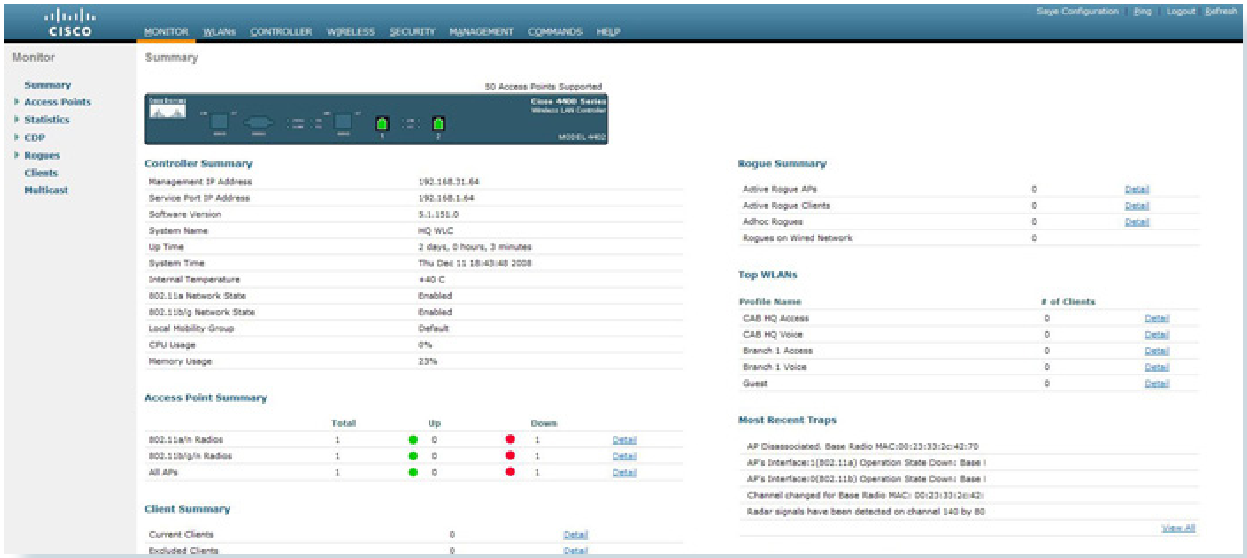
https://192.168.31.64

You may also use a DNS name if you have added a Host entry for the management IP address.

Before further configuration on the WLC, confirm that there is a Host entry for ***cisco-lwapp-controller*** with the ***ap-manager*** IP address in the DNS server specified in the DHCP pools or DHCP server scopes. (In this case, the DNS server is 192.168.28.10.).

Using DHCP for the IP address, netmask, gateway, and DNS server information, the AP will then use DNS to resolve **cisco-lwapp-controller** and establish a connection with the WLC to allow the enabling of the radios (they are disabled by default) and additional configuration. We recommend that you also define a DNS Host entry for the management IP address, although it is not required.

At the headquarters, the access ports, which are connected to the APs, should use standard access switch port configuration with one exception. The default trust must be changed from CoS to DSCP by using the interface command `mls qos trust dscp`.



Summary

Controller Summary

Management IP Address	192.168.31.64
Service Port IP Address	192.168.1.64
Software Version	5.1.151.0
System Name	HQ WLC
Up Time	2 days, 0 hours, 3 minutes
System Time	Thu Dec 11 18:43:48 2008
Internal Temperature	+40 C
802.11a Network State	Enabled
802.11b/g Network State	Enabled
Local Mobility Group	Default
CPU Usage	0%
Memory Usage	23%

Access Point Summary

	Total	Up	Down	
802.11a/n Radios	1	🟢 0	🔴 1	Detail
802.11b/g/n Radios	1	🟢 0	🔴 1	Detail
All APs	1	🟢 0	🔴 1	Detail

Client Summary

Current Clients	0	Detail
Excluded Clients	0	Detail

Rogue Summary

Active Rogue APs	0	Detail
Active Rogue Clients	0	Detail
Adhoc Rogues	0	Detail
Rogues on Wired Network	0	

Top WLANs

Profile Name	# of Clients	
CAB HQ Access	0	Detail
CAB HQ Voice	0	Detail
Branch 1 Access	0	Detail
Branch 1 Voice	0	Detail
Guest	0	Detail

Most Recent Traps

```
AP Disassociated. Base Radio MAC:00:23:33:2c:42:70
AP's Interface:1(802.11a) Operation State Down: Base I
AP's Interface:0(802.11b) Operation State Down: Base I
Channel changed for Base Radio MAC: 00:23:33:2c:42:
Radar signals have been detected on channel 140 by 80
```

View All

After logging into the web interface, we will be able to verify the basic health of the WLC on the Monitor>Summary page.

Please confirm that you saved the configuration (top right of the GUI) after any configuration steps.

This page shows the distribution ports that are up (green) and any APs that have established communications.

Wireless Guest Access

Below we present how to deploy a guest wireless network that allows visitors, with a guest username and password, to access the Internet at both head-quarters and branch sites.

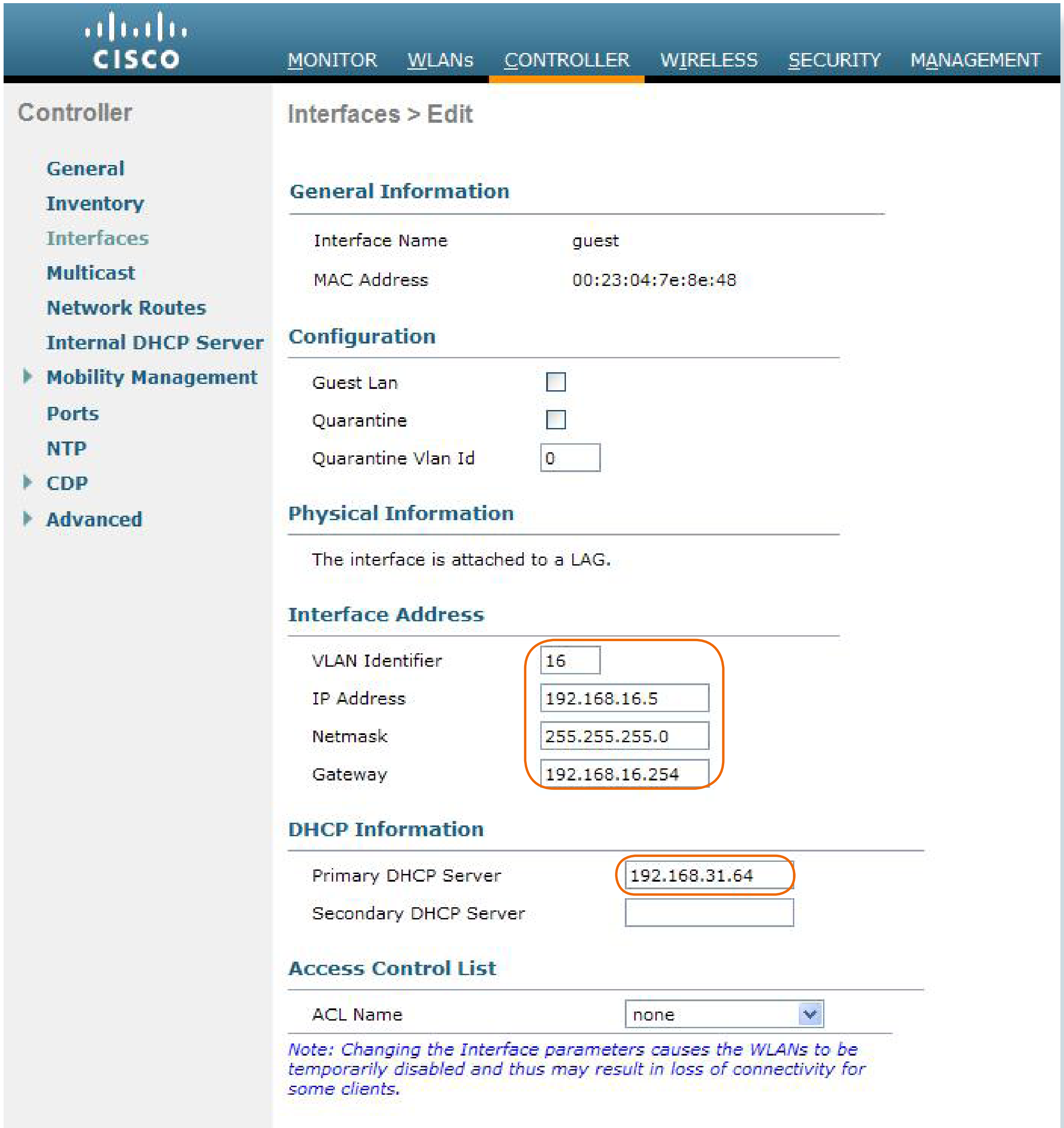
On the core switches, VLAN 16 was previously defined to trunk guest traffic specifically to the ASA. The VLAN interface on the core switch does not have an IP address as the default gateway for this subnet will be the ASA and does not allow access to the rest of the network. DHCP services and guest authentication will be provided by the WLC. The “guest” account on the WLC expires after a predetermined length of time (default is 24 hours), after which a new authentication is needed using a newly created user-name and password.

For this deployment, we will be using the following information to configure Wireless guest access:

```
VLAN 16
IP address 192.168.16.5
Netmask 255.255.255.0
Gateway 192.168.16.254
Primary DHCP Server 192.168.31.64
SSID CAB_Guest
```

Step 1: Confirm that VLAN 16 is allowed on the core switch interfaces connected to the ASA and WLC interfaces (VLAN 16).

Step 2: Configure an Interface on the WLC’s Controller page.



Interfaces > Edit

General Information

Interface Name	guest
MAC Address	00:23:04:7e:8e:48

Configuration

Guest Lan	□
Quarantine	□
Quarantine Vlan Id	0

Physical Information

The interface is attached to a LAG.

Interface Address

VLAN Identifier	16
IP Address	192.168.16.5
Netmask	255.255.255.0
Gateway	192.168.16.254

DHCP Information

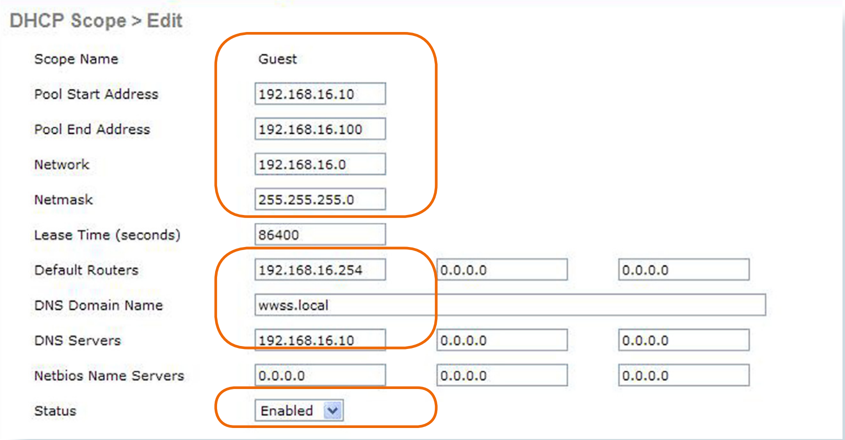
Primary DHCP Server	192.168.31.64
Secondary DHCP Server	

Access Control List

ACL Name	none

Note: Changing the Interface parameters causes the WLANs to be temporarily disabled and thus may result in loss of connectivity for some clients.

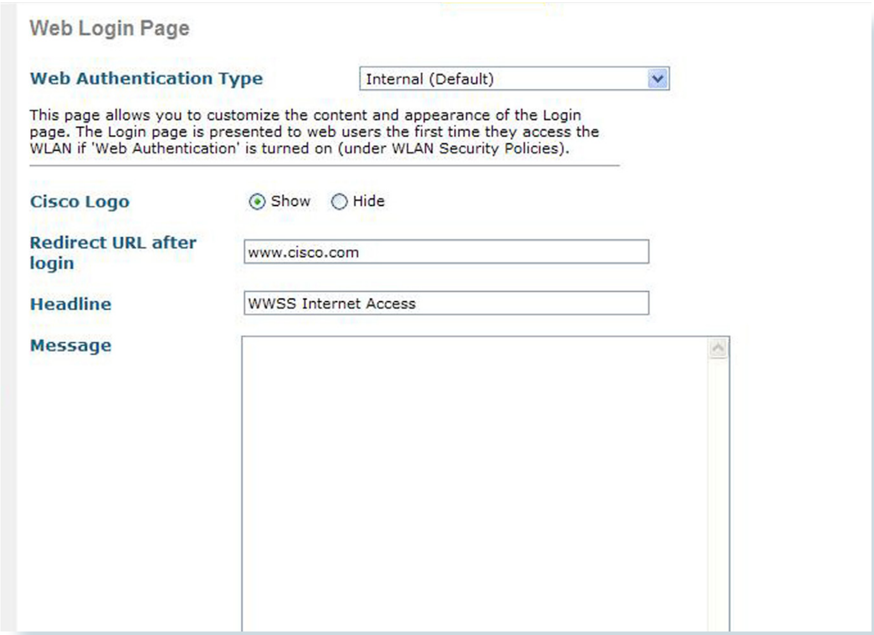
Step 3: Configure a DHCP scope on the WLC's Internal DHCP server. (Controller>Internal DHCP Server) and set the status to **Enabled**.



DHCP Scope > Edit

Scope Name	Guest		
Pool Start Address	192.168.16.10		
Pool End Address	192.168.16.100		
Network	192.168.16.0		
Netmask	255.255.255.0		
Lease Time (seconds)	86400		
Default Routers	192.168.16.254	0.0.0.0	0.0.0.0
DNS Domain Name	wwss.local		
DNS Servers	192.168.16.10	0.0.0.0	0.0.0.0
Netbios Name Servers	0.0.0.0	0.0.0.0	0.0.0.0
Status	Enabled		

Step 4: Customize the Web Auth Login page (Security>Web Auth>Web Login Page)



Web Login Page

Web Authentication Type Internal (Default)

This page allows you to customize the content and appearance of the Login page. The Login page is presented to web users the first time they access the WLAN if 'Web Authentication' is turned on (under WLAN Security Policies).

Cisco Logo ● Show ○ Hide

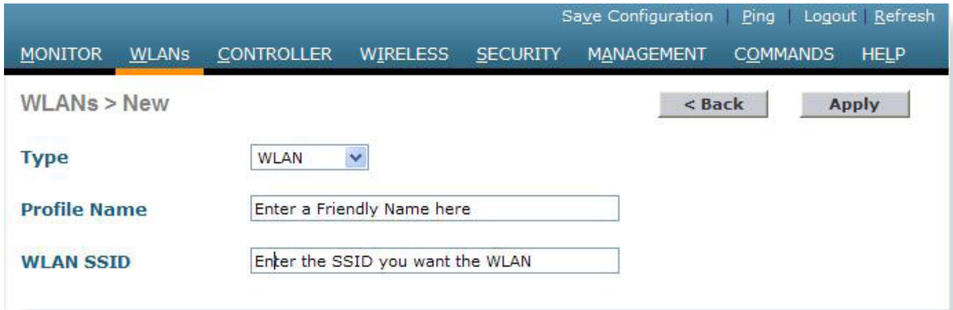
Redirect URL after login www.cisco.com

Headline WWSS Internet Access

Message

Step 5: Configure the Guest WLAN

Add a new WLAN by clicking on the "New..." button on the WLANs page.



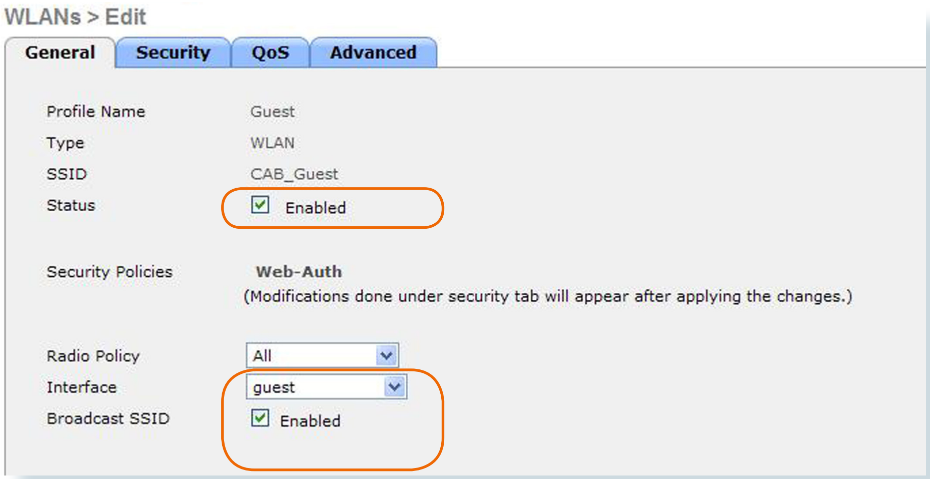
WLANs > New

Type WLAN

Profile Name Enter a Friendly Name here

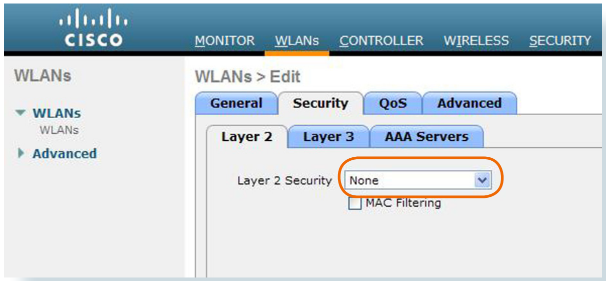
WLAN SSID Enter the SSID you want the WLAN

Click apply.
Set status to enable.
Set Interface to the one defined in Step 2 (guest).
Enable Broadcast SSID.



WLANs > Edit

Profile Name	Guest
Type	WLAN
SSID	CAB_Guest
Status	☑ Enabled
Security Policies	**Web-Auth** (Modifications done under security tab will appear after applying the changes.)
Radio Policy	All
Interface	guest
Broadcast SSID	☑ Enabled

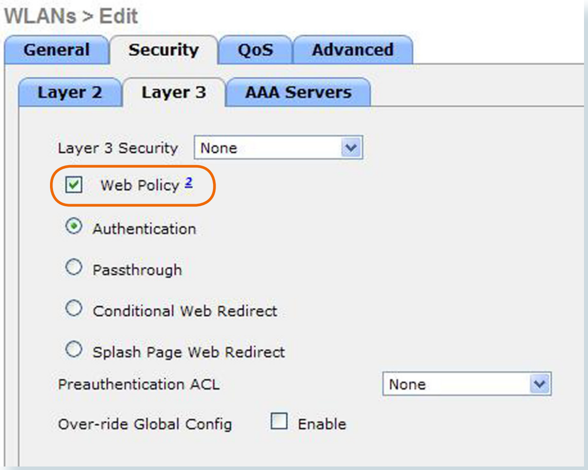


WLANs > Edit

Layer 2 Security: None

□ MAC Filtering

Set Layer 2 Security to **None.**



WLANs > Edit

Layer 3 Security: None

☑ Web Policy 2

● Authentication

○ Passthrough

○ Conditional Web Redirect

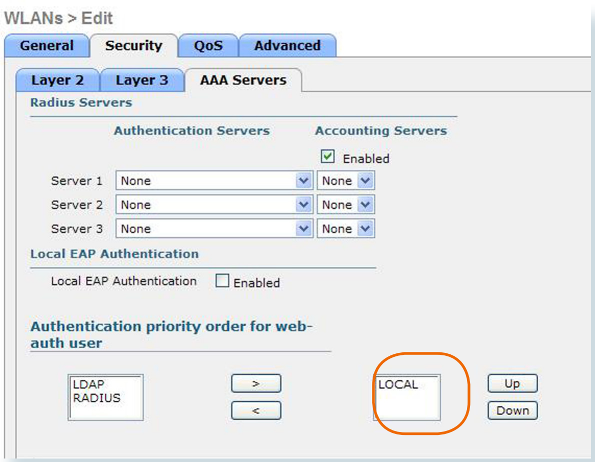
○ Splash Page Web Redirect

Preauthentication ACL: None

Over-ride Global Config: □ Enable

Set Layer 3 Security to **None**.

Check the Web Policy box to confirm that "Authentication" is selected.



WLANs > Edit

Radius Servers

	Authentication Servers	Accounting Servers
		☑ Enabled
Server 1	None	None
Server 2	None	None
Server 3	None	None

Local EAP Authentication

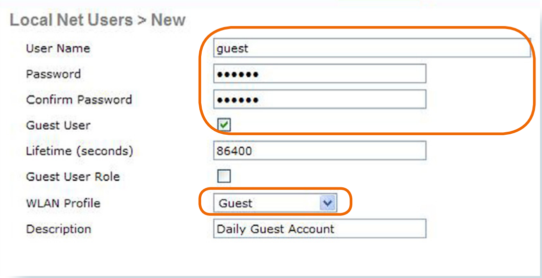
Local EAP Authentication □ Enabled

Authentication priority order for web-auth user

LDAP
RADIUS → LOCAL

Confirm that Local is the only method listed for Authentication of Web Auth users.

Step 6: Add a Guest user account (Security>Local Net Users).

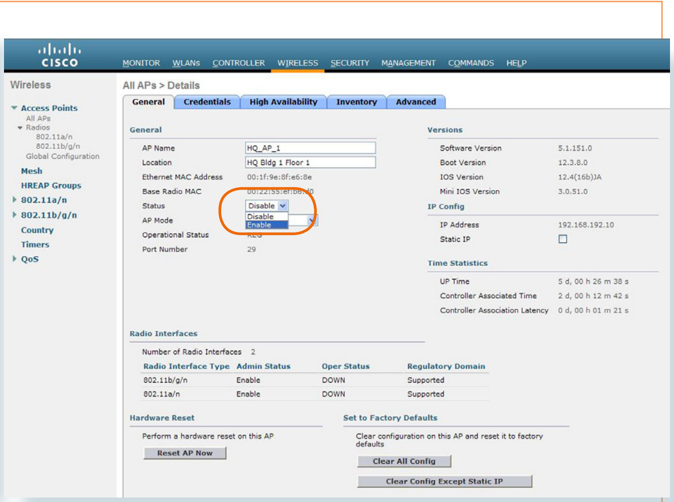


Local Net Users > New

User Name	guest
Password	••••••
Confirm Password	••••••
Guest User	☑
Lifetime (seconds)	86400
Guest User Role	□
WLAN Profile	Guest
Description	Daily Guest Account

Check the guest user box to allow the count to expire after 86400 seconds (1 day) and select the Guest WLAN profile.

We are now ready to enable the APs (Wireless>All APs).



All APs > Details

General

AP Name	HQ_AP_1
Location	HQ Bldg 1 Floor 1
Ethernet MAC Address	00:1f:9e:8f:e6:8e
Base Radio MAC	00:22:55:ef:b6:d0
Status	Disable (Disable / Enable)
AP Mode	
Operational Status	REG
Port Number	29

Versions

Software Version	5.1.151.0
Boot Version	12.3.8.0
IOS Version	12.4(16b)JA
Mini IOS Version	3.0.51.0

IP Config

IP Address	192.168.192.10
Static IP	□

Time Statistics

UP Time	5 d, 00 h 26 m 38 s
Controller Associated Time	2 d, 00 h 12 m 42 s
Controller Association Latency	0 d, 00 h 01 m 21 s

Radio Interfaces

Number of Radio Interfaces 2

Radio Interface Type	Admin Status	Oper Status	Regulatory Domain
802.11b/g/n	Enable	DOWN	Supported
802.11a/n	Enable	DOWN	Supported

Hardware Reset

Perform a hardware reset on this AP

Set to Factory Defaults

Clear configuration on this AP and reset it to factory defaults

Set AP Status to Enabled on every AP.

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 prompted for a username and password. Enter the guest account username and password and Internet access will be available for 24 hours.

By default, all APs in the deployment will have the guest WLAN. If you wish to restrict the Guest WLAN to specific APs, please refer to the "Restricting WLANs" section later for configuration details.

The data and voice WLANs at the headquarters and the branch will authenticate clients against Active Domain (AD) accounts. To achieve this, we will use Microsoft's Internet Authentication Server (IAS) to provide a RADIUS (Remote Authentication Dial In User Service) service.

RADIUS

This requires:

Step 1: Install IAS on a Windows Server.

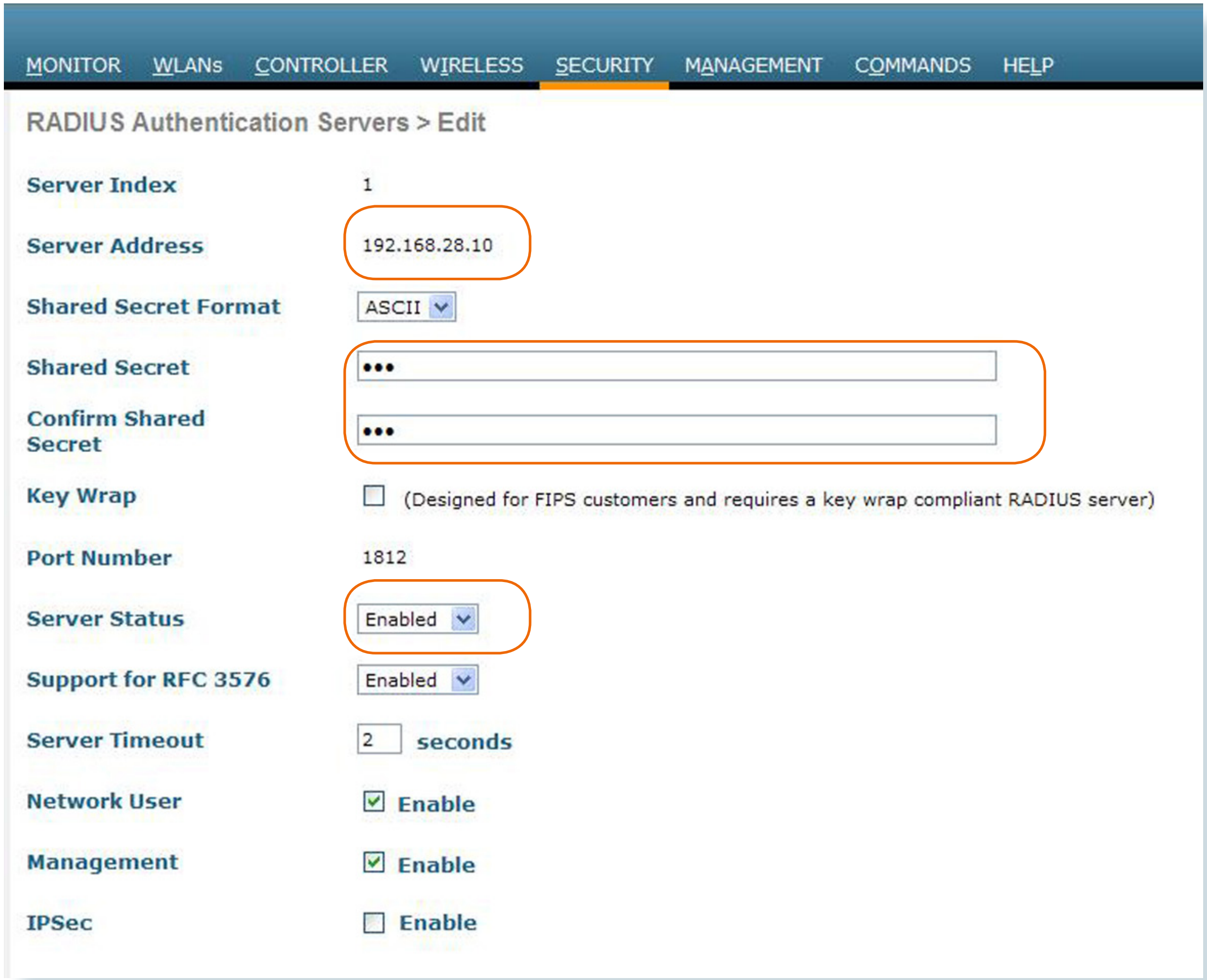
Step 2: Open the Internet Authentication Service Management Console.

Step 3: Using the Policy Wizard, add a "Wireless" policy with the group or users that will be allowed to connect to the wireless network (i.e., "Domain Users").

Step 4: Using the RADIUS Client's wizard, add a new client that will use the IP address (or DNS name) of the WLC management interface. You will need a shared secret in this step that will also be used when configuring the WLC RADIUS client.

On the WLC GUI, add a RADIUS server on the Security page.

In this example, IAS is installed on server 192.168.28.10 (this is also the DNS server) and uses the same shared secret used in Step 4.



RADIUS Authentication Servers > Edit

Server Index	1
Server Address	192.168.28.10
Shared Secret Format	ASCII
Shared Secret	•••
Confirm Shared Secret	•••
Key Wrap	□ (Designed for FIPS customers and requires a key wrap compliant RADIUS server)
Port Number	1812
Server Status	Enabled
Support for RFC 3576	Enabled
Server Timeout	2 seconds
Network User	☑ Enable
Management	☑ Enable
IPSec	□ Enable

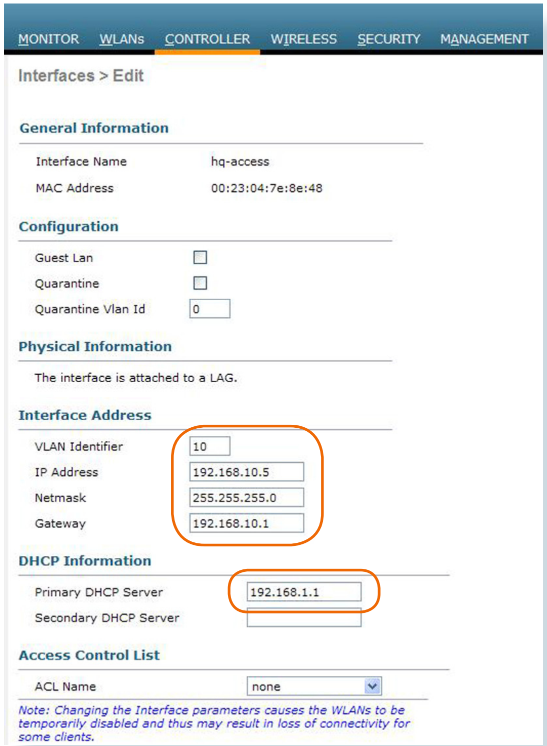
The following section provides data and voice WLANs for company employees at the headquarters. Each WLAN will have security, QoS, and be authenticated against the previously configured RADIUS server.

The following information will be used for the Data Access WLAN configuration:

```
VLAN 10
IP address 192.168.10.5
Netmask 255.255.255.0
Gateway 192.168.10.1
Primary DHCP Server 192.168.1.1

SSID CAB HQ Access
```

Step 1: Configure the Interface.



Interfaces > Edit

General Information

Interface Name hq-access
MAC Address 00:23:04:7e:8e:48

Configuration

Guest Lan □
Quarantine □
Quarantine Vlan Id 0

Physical Information

The interface is attached to a LAG.

Interface Address

VLAN Identifier 10
IP Address 192.168.10.5
Netmask 255.255.255.0
Gateway 192.168.10.1

DHCP Information

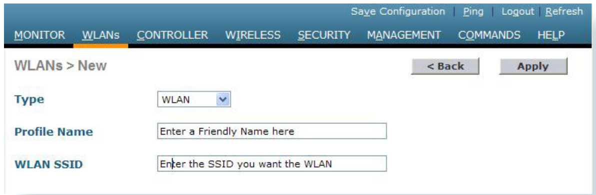
Primary DHCP Server 192.168.1.1
Secondary DHCP Server

Access Control List

ACL Name none

Note: Changing the Interface parameters causes the WLANs to be temporarily disabled and thus may result in loss of connectivity for some clients.

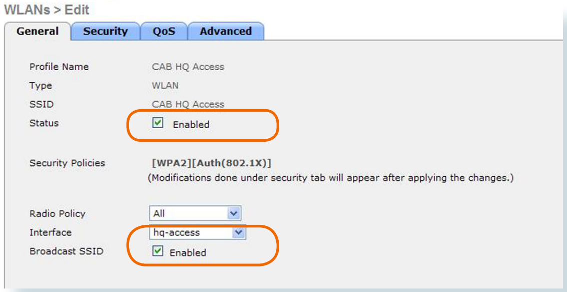
Step 2: Configure the WLAN.
Add a new WLAN by clicking on the "New..." button on the WLANs page.



WLANs > New

Type WLAN
Profile Name Enter a Friendly Name here
WLAN SSID Enter the SSID you want the WLAN

Click apply. Set status to **enable**.
Set Interface to the interface name used in Step 1 (hq-access).



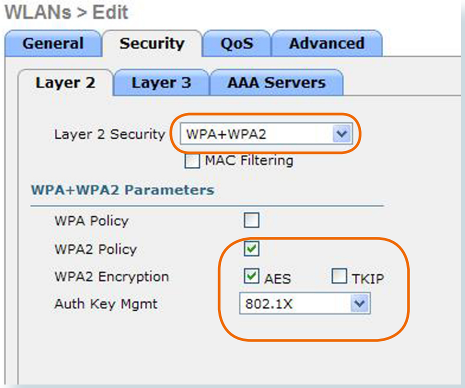
WLANs > Edit

Profile Name CAB HQ Access
Type WLAN
SSID CAB HQ Access
Status ☑ Enabled

Security Policies [WPA2][Auth(802.1X)]
(Modifications done under security tab will appear after applying the changes.)

Radio Policy All
Interface hq-access
Broadcast SSID ☑ Enabled

In this deployment, we are using WPA2 and 802.1x Authentication.



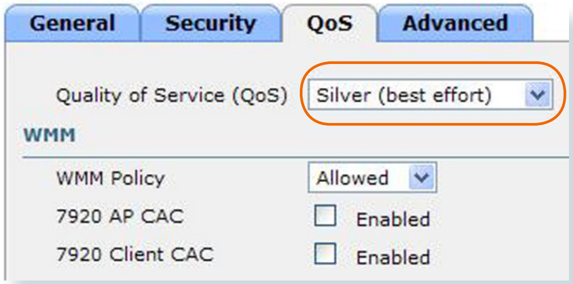
WLANs > Edit

Layer 2 Security WPA+WPA2
□ MAC Filtering

WPA+WPA2 Parameters

WPA Policy □
WPA2 Policy ☑
WPA2 Encryption ☑ AES □ TKIP
Auth Key Mgmt 802.1X

QoS for Data Access is left at the default of Silver (Best Effort).



Quality of Service (QoS) Silver (best effort)

WMM

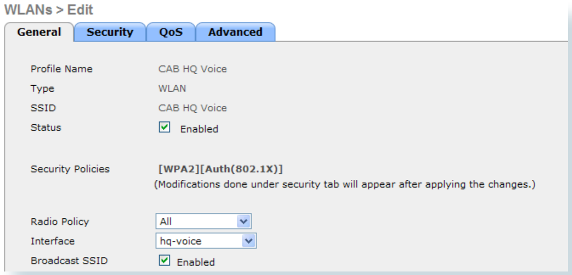
WMM Policy Allowed
7920 AP CAC □ Enabled
7920 Client CAC □ Enabled

All other settings are left at default.
The following information will be used for the Headquarters Voice WLAN configuration:

```
VLAN 14
IP address 192.168.14.5
Netmask 255.255.255.0
Gateway 192.168.14.1
Primary DHCP Server 192.168.1.1

SSID CAB HQ Voice
```

Repeat Steps 1 and 2 again with the voice WLAN configuration information, but set the QoS to Platinum instead of Silver.

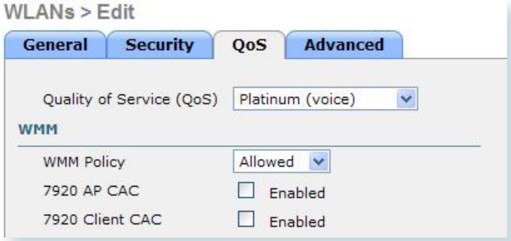


WLANs > Edit

Profile Name CAB HQ Voice
Type WLAN
SSID CAB HQ Voice
Status ☑ Enabled

Security Policies [WPA2][Auth(802.1X)]
(Modifications done under security tab will appear after applying the changes.)

Radio Policy All
Interface hq-voice
Broadcast SSID ☑ Enabled



WLANs > Edit

Quality of Service (QoS) Platinum (voice)

WMM

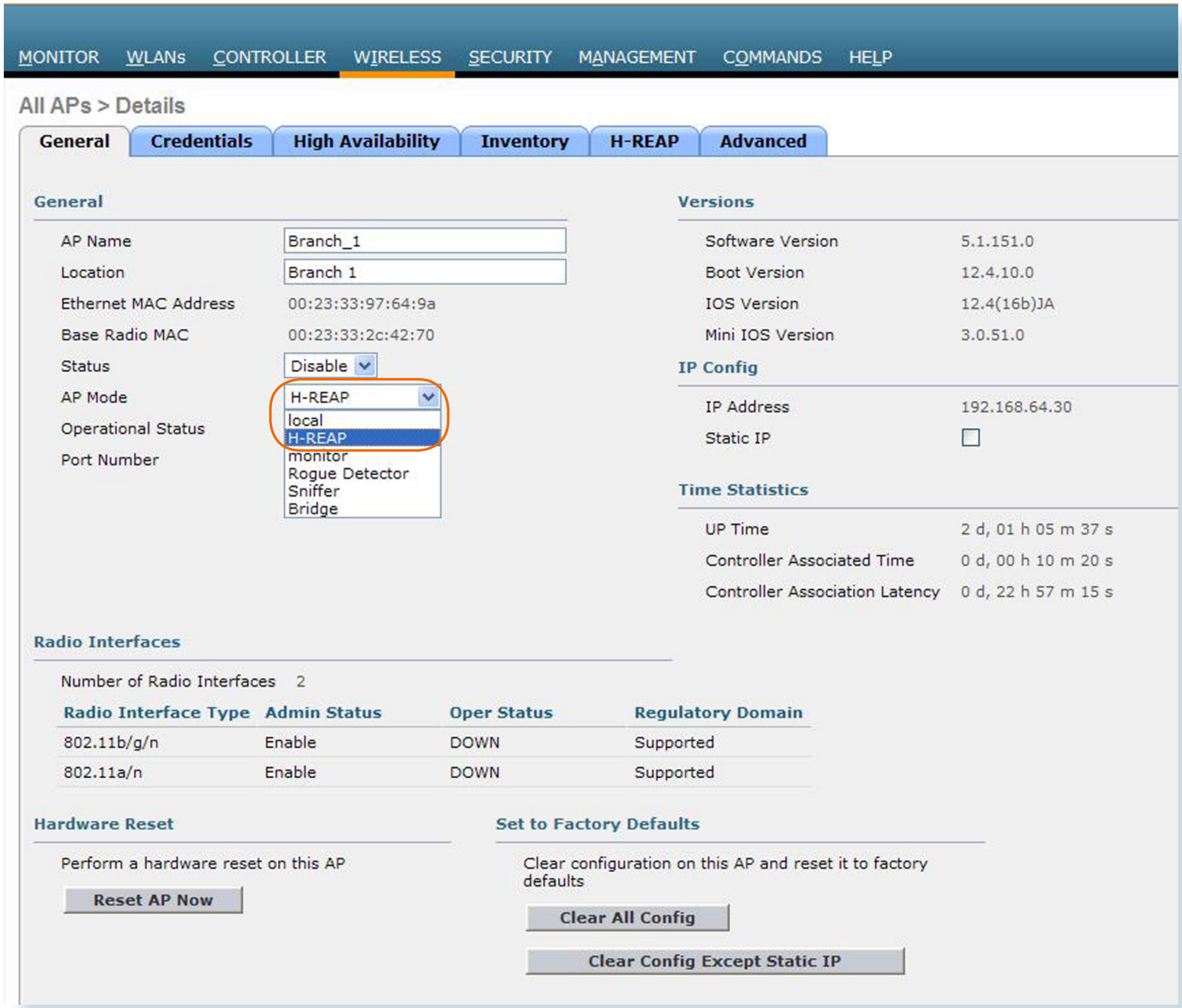
WMM Policy Allowed
7920 AP CAC □ Enabled
7920 Client CAC □ Enabled

Branch Wireless

Each branch site will have a site-specific Data and Voice WLAN, which is basically configured in the same way as the HQ WLANs with one fundamental difference.

At the HQ, the wireless users traffic is transported over LWAPP using the wired data VLAN to the WLC where it is switched out over the LAG Ports, which is a 802.1Q trunk into the resilient core as illustrated at the beginning of this module. If wireless traffic at the branch sites also behaved this way, the traffic between two devices within the branch is likely to be transported via LWAPP over the WAN to the WLC where it would be trunked into the core, to be routed back across WAN to its destination. This is especially a problem for Unified Communications as a wireless IP phone making a call out of the branch gateway would traverse the WAN twice, when in reality, it did not need to leave the branch at all. To resolve this, all but the guest WLAN in the branch will be switched locally by the APs in the branch; only the management, control, and guest traffic will be transported via LWAPP to the WLC at the HQ. This mode of operation is enabled by switching the AP from local to H-REAP mode under the Wireless>AP menu. Select each branch AP and change the mode as indicated in the following screen. Save the configuration and click the “Reset AP” button. The AP will rest and, after registering with the WLC, will have an additional H-REAP tab to allow for the additional configuration we will cover in the next part of this module.

Another benefit of H-REAP is that the AP can operate autonomously should it lose contact with the WLC due to a WAN outage, for example. This, however, would require additional configuration as the wireless authentication is carried out using services located across the WAN at the HQ and is outside the scope of this deployment guide.



All APs > Details

General

AP Name	Branch_1
Location	Branch 1
Ethernet MAC Address	00:23:33:97:64:9a
Base Radio MAC	00:23:33:2c:42:70
Status	Disable
AP Mode	H-REAP
Operational Status	
Port Number	

Versions

Software Version	5.1.151.0
Boot Version	12.4.10.0
IOS Version	12.4(16b)JA
Mini IOS Version	3.0.51.0

IP Config

IP Address	192.168.64.30
Static IP	□

Time Statistics

UP Time	2 d, 01 h 05 m 37 s
Controller Associated Time	0 d, 00 h 10 m 20 s
Controller Association Latency	0 d, 22 h 57 m 15 s

Radio Interfaces

Number of Radio Interfaces 2

Radio Interface Type	Admin Status	Oper Status	Regulatory Domain
802.11b/g/n	Enable	DOWN	Supported
802.11a/n	Enable	DOWN	Supported

Hardware Reset

Perform a hardware reset on this AP

Set to Factory Defaults

Clear configuration on this AP and reset it to factory defaults

Wireless Module

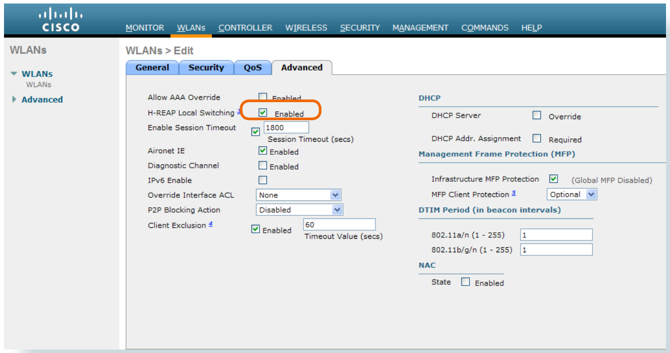
The following information is used for the branch site deployment:

```
Branch Data WLAN
VLAN 69
IP address 192.168.69.5
Netmask 255.255.255.0
Gateway 192.168.69.1
DHCP Server 192.168.64.1
SSID “CAB Br1 Access”
Silver QoS

Branch Voice WLAN
VLAN 70
IP Address 192.168.70.5
Netmask 255.255.255.0
Gateway 192.168.70.1
DHCP Server 192.168.64.1
SSID “CAB Br1 Voice”
Platinum QoS
```

The branch WLANs are configured using the same method as the headquarters WLANs, but with the following additional steps:

- When defining the interface, you may use a VLAN on the headquarters WLC; however, it will not be allowed on the core switches. It still needs to be defined to allow for the configuration of the IP parameters in order to match those required at the branch.
- When defining a WLAN at the branch that terminates the traffic locally, check the H-REAP Local Switching box on the advanced tab.



WLANs > Edit

Allow AAA Override □ Enabled
H-REAP Local Switching [3] ☑ Enabled
Enable Session Timeout ☑ 1800 Session Timeout (secs)
Aironet IE ☑ Enabled
Diagnostic Channel □ Enabled
IPv6 Enable □
Override Interface ACL None
P2P Blocking Action Disabled
Client Exclusion [4] ☑ Enabled 60 Timeout Value (secs)

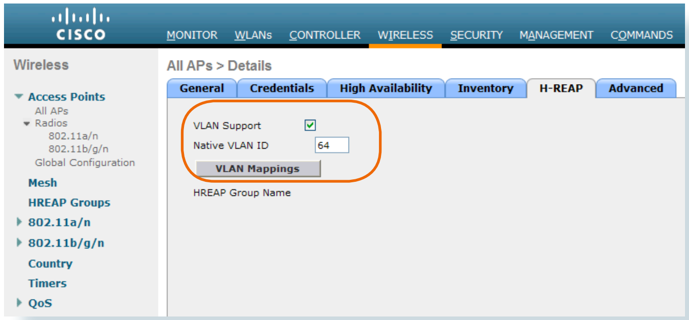
DHCP
DHCP Server □ Override
DHCP Addr. Assignment □ Required

Management Frame Protection (MFP)
Infrastructure MFP Protection ☑ (Global MFP Disabled)
MFP Client Protection [5] Optional

DTIM Period (in beacon intervals)
802.11a/n (1 - 255) 1
802.11b/g/n (1 - 255) 1

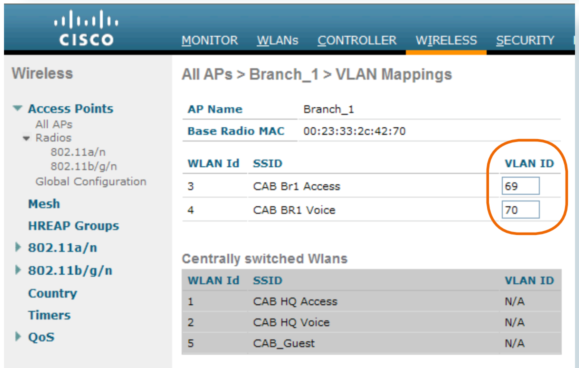
NAC
State □ Enabled

After the WLANs have been defined, they need to be mapped to the correct local VLANs at the branch site. This is achieved on the Wireless>All APs page by selecting the branch AP and configuring the *VLAN Mappings* on the *H-REAP* tab.



All APs > Details

VLAN Support ☑
Native VLAN ID 64
HREAP Group Name



All APs > Branch_1 > VLAN Mappings

AP Name	Branch_1
Base Radio MAC	00:23:33:2c:42:70

WLAN Id	SSID	VLAN ID
3	CAB Br1 Access	69
4	CAB BR1 Voice	70

Centrally switched Wlans

WLAN Id	SSID	VLAN ID
1	CAB HQ Access	N/A
2	CAB HQ Voice	N/A
5	CAB_Guest	N/A

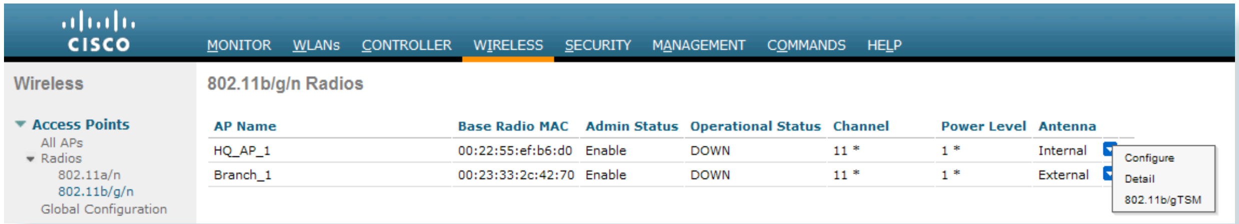
Notes

As WLANs are added to the system, they will be available on all APs by default; however, the ability to restrict WLANs to geographic regions or specific APs can be configured using the Configure menu on the Wireless>Radios page.

In this deployment, we restrict the WLANs to their specific sites, yet allow Guest to be available everywhere.

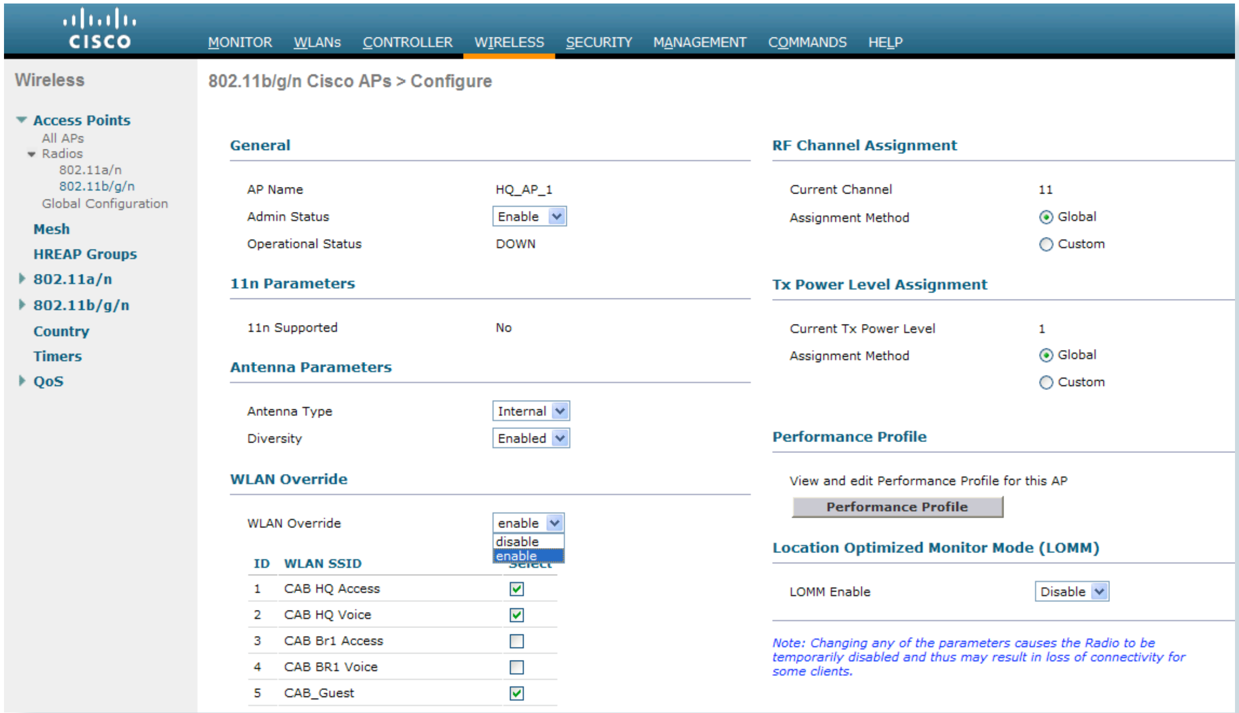
The following enables only the headquarters and guest WLANs for an AP at the headquarters.

The corresponding configuration is made on the branch APs to allow only the local branch WLANs and the guest WLAN.



802.11b/g/n Radios

AP Name	Base Radio MAC	Admin Status	Operational Status	Channel	Power Level	Antenna
HQ_AP_1	00:22:55:ef:b6:d0	Enable	DOWN	11 *	1 *	Internal
Branch_1	00:23:33:2c:42:70	Enable	DOWN	11 *	1 *	External



802.11b/g/n Cisco APs > Configure

General

AP Name	HQ_AP_1
Admin Status	Enable
Operational Status	DOWN

11n Parameters

11n Supported	No

Antenna Parameters

Antenna Type	Internal
Diversity	Enabled

WLAN Override

WLAN Override	enable

ID	WLAN SSID	Select
1	CAB HQ Access	☑
2	CAB HQ Voice	☑
3	CAB Br1 Access	□
4	CAB BR1 Voice	□
5	CAB_Guest	☑

RF Channel Assignment

Current Channel	11
Assignment Method	● Global ○ Custom

Tx Power Level Assignment

Current Tx Power Level	1
Assignment Method	● Global ○ Custom

Performance Profile

View and edit Performance Profile for this AP

Location Optimized Monitor Mode (LOMM)

LOMM Enable	Disable

Note: Changing any of the parameters causes the Radio to be temporarily disabled and thus may result in loss of connectivity for some clients.

The following interface and DHCP configuration was added to the branch router to support the branch WLANs:

```
ip dhcp pool Wireless_Access
   network 192.168.69.0 255.255.255.0
   domain-name cisco.com
   dns-server 192.168.28.10
   default-router 192.168.69.1
!
ip dhcp pool Wireless_Voice
   network 192.168.70.0 255.255.255.0
  domain-name cisco.com
  dns-server 192.168.28.10
   default-router 192.168.70.1
   option 150 ip 192.168.28.20 192.168.28.21
```

The 150 DHCP option for wireless voice pool provides the IP addresses of the Cisco Unified Communications Manager Configuration Servers and is therefore optional.

```
interface FastEthernet0/0.69
 description Wireless Access
 encapsulation dot1Q 69
 ip address 192.168.69.1 255.255.255.0

interface FastEthernet0/0.70
 description Wireless Voice
 encapsulation dot1Q 70
 ip address 192.168.70.1 255.255.255.0
```

Branch Site Access Switch Configuration

The branch access switch port configuration is different than the headquarters, as the data and voice VLANs terminate locally, thus requiring a trunk port configuration:

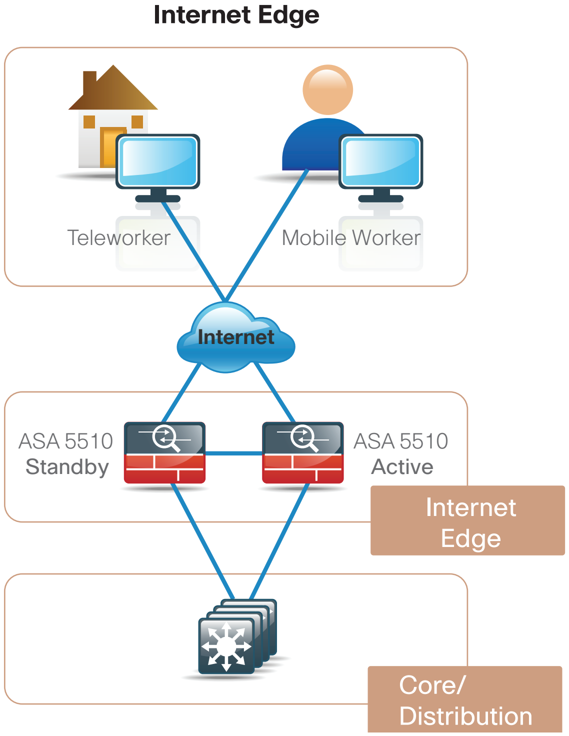
```
interface GigEthernet0/5
 description Wireless Access Point
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 64
 switchport trunk allowed vlan 64,69,70
 switchport mode trunk
 srr-queue bandwidth share 10 10 60 20
 priority-queue out
 mls qos trust dscp
 auto qos voip trust
 spanning-tree bpduguard enable
```

Where VLAN 64 is the native data VLAN for this branch, VLAN 69 is the wireless data VLAN and VLAN 70 is the wireless voice VLAN.

Notes

Technology Overview

Security is an integral part of every network deployment today—both because of the need to have secure, reliably available networks and protect information assets, and because of regulatory compliance requirements. With most networks connected to the Internet and potentially vulnerable to a constant barrage of worms, viruses, and targeted attacks, companies must be vigilant in protecting their network, user data, and customer information. This section covers Firewall, VPN, and intrusion prevention systems (IPSs). As regulatory requirements vary by country and industry, this document will not be an exhaustive coverage of specific regulatory requirements.



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. At this point in the network, it is common to have a Firewall, a VPN appliance, and an IPS appliance. In this design, the Cisco Adaptive Security Appliance (ASA) is deployed at the Internet edge and performs the function in a single, low-cost device. In this section, we cover basic Firewall setup and VPN configuration. IPS will be covered in its own section since dedicated IPS appliances and router-integrated IPS are also deployed at other places throughout the network.

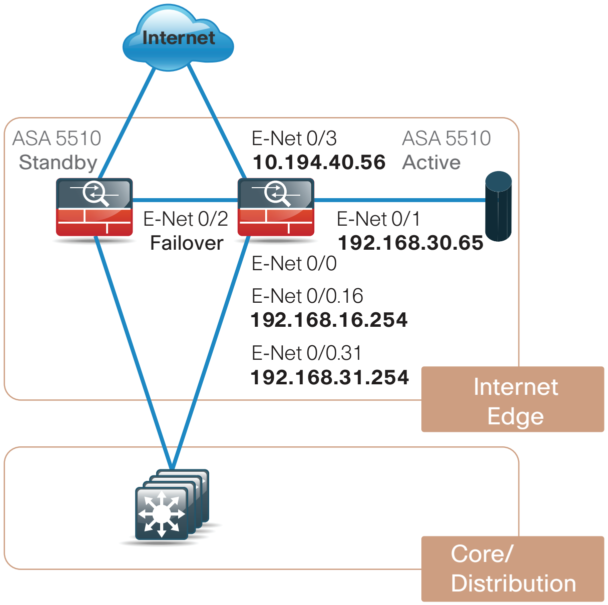
Firewall Setup

The Cisco ASAs are set up as a highly available active/standby pair. Active/standby is used rather than an active/active configuration, because it is a much simpler configuration; it allows for the use of the same appliance for Firewall and VPN (VPN functionality is disabled on the ASA in active/active), and the Internet link speeds in this design do not surpass the performance of a single ASA appliance. In the event that the active ASA appliance fails or needs to be taken out of service for maintenance, the secondary ASA appliance will take over all Firewall, IPS, and VPN functions. The ASA is running EIGRP on the inside to simplify the routing configuration and so changes to the campus and WAN do not require routing configuration changes on the ASA. There is a DMZ configured in case there is a need for Internet-accessible servers to be hosted on site, but 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 guest Internet access.

The Cisco ASA can be configured from the command line or from the graphical user interface Cisco Adaptive Security Device Manager (ASDM). The default configuration in this example for the Cisco ASA 5510 and other Cisco ASA 55xx Series appliances is:

```
interface management 0/0
ip address 192.168.1.1 255.255.255.0
nameif management
security-level 100
no shutdown
asdm logging informational 100
asdm history enable
http server enable
http 192.168.1.0 255.255.255.0 management
dhcpd address 192.168.1.2-192.168.1.254
management
dhcpd lease 3600
dhcpd ping_timeout 750
dhcpd enable management
```

To configure the ASA via CLI, connect to the console port and use a terminal client.



Basic Setup

To get the Firewall up and running, you need to configure the interfaces, setup routing, and failover. NOTE: IP addresses and specific interfaces in this example are only for demonstration purposes and will likely differ in your network. Refer to Figure x.x.

First, configure the host and domain name for your ASA:

```
hostname [ASA5510]
domain-name cisco.com
```

Configure and enable password and console/telnet password:

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

Next, the Firewall interfaces need to be configured so that connectivity to the inside and outside networks is enabled. You will notice that the interfaces have a standby IP address in addition to the main address. This is part of the failover Firewall configuration and will be covered more in the failover section. All interfaces on the ASA have a security-level setting. The higher the number, the more secure the interface. Inside interfaces are typically assigned 100, the highest security level, and 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.

In this configuration, multiple VLAN interfaces are trunked to Ethernet 0/0, the inside interface. The 31 VLAN carries the internal corporate traffic and the 16 VLAN is for wireless guest access.

```
interface Ethernet0/0
 no nameif
 no security-level
 no ip address
!
interface Ethernet0/0.16
 vlan 16
 nameif guest
 security-level 0
 ip address 192.168.16.254 255.255.255.0 
standby 192.168.16.253
!
interface Ethernet0/0.31
 vlan 31
 nameif inside
 security-level 100
 ip address 192.168.31.254 255.255.255.0 
standby 192.168.31.253
!
```

Ethernet 0/1 is a DMZ network for hosts that need to be reached directly from the Internet.

```
interface Ethernet0/1
 nameif DMZ
 security-level 50
ip address 192.168.30.65 255.255.255.192
standby 192.168.30.66
!
interface Ethernet0/2
description LAN/STATE Failover Interface
!
```

Ethernet 0/3 is the outside interface and is connected to the ISP.

```
interface Ethernet0/3
 nameif outside
 security-level 0
 ip address 10.194.40.56 255.255.255.0 
standby 10.194.40.55
!
```

Active/Standby Failover

For failover to work, both units have to be identical. They need to be the same model, with identical licenses and SSMs (if SSMs are installed). The secondary ASA unit needs to be powered up and cabled to the same networks as the primary. In this example, Ethernet 0/2 is the failover interface and a crossover cable connects the primary and secondary units on this interface. The failover interface is also the state failover interface, meaning that all session state is replicated from the primary to the standby unit on this interface. There can be a substantial amount of data, and it is recommended that this be a dedicated interface. To configure failover between two ASAs, here are the necessary commands:

```
failover
failover lan unit primary
failover lan interface failover Ethernet0/2
failover replication http
failover link failover Ethernet0/2
failover interface ip failover 192.168.30.1 
255.255.255.252 standby 192.168.30.2
```

A standby address must be configured for each shared interface between the active and standby ASAs. The standby will always be configured with the standby address. If the standby ASA becomes active, it will take over the primary address, and the other ASA in the pair will get the standby address if it is still online.

```
ip address 192.168.31.254  255.255.255.0 
standby 192.168.31.253
```

As an option, the failover timers can be tuned to speed up failover in the event of a device or link failure. With the default, depending on the failure, the 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 ASA with low to average load, the poll times can be tuned down without performance impact.

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

Routing Configuration for ASA

As you can see, all the interfaces except the inside interface are set to "passive." There are no other routers with which we want to communicate routing information on these interfaces—and we do not want to leak out any internal information to a less secure network. We are redistributing static routes, because the ASA is the gateway of last resort as the dedicated and only connection to the Internet from the corporate network. Redistributing static routes causes the ASA to advertise a default to the rest of the network so that if a specific network cannot be accessed, the traffic will route to the ASA and it will send the traffic out to the Internet.

```
router eigrp 1
 network 192.168.0.0 255.255.0.0
 passive-interface guest
 passive-interface DMZ
 passive-interface outside
 redistribute static

route outside 0.0.0.0 0.0.0.0 10.194.40.1 1
```

Configuring NAT/PAT

One last step is required to get basic Internet connectivity for inside hosts. Since the inside network is numbered using RFC 1918 addressing that is not Internet routable, we need to translate the inside private addresses to an outside public address. For this configuration, we are going to translate all inside addresses to the public address of the outside interface.

```
global (outside) 1 interface
nat (inside) 1 192.168.0.0 255.255.0.0
```

Remote Management

After the initial setup of the ASA, you are able to connect to the device remotely for convenient configuration, management, and troubleshooting.

The following configuration allows for remote connectivity from any internal network via HTTPS or SSH. The ASA can have limited access to just a single address or can be accessed through a management network by changing the network statements below:

```
http server enable
http 192.168.0.0 255.255.0.0 inside
ssh 192.168.0.0 255.255.0.0 inside
ssh version 2
```

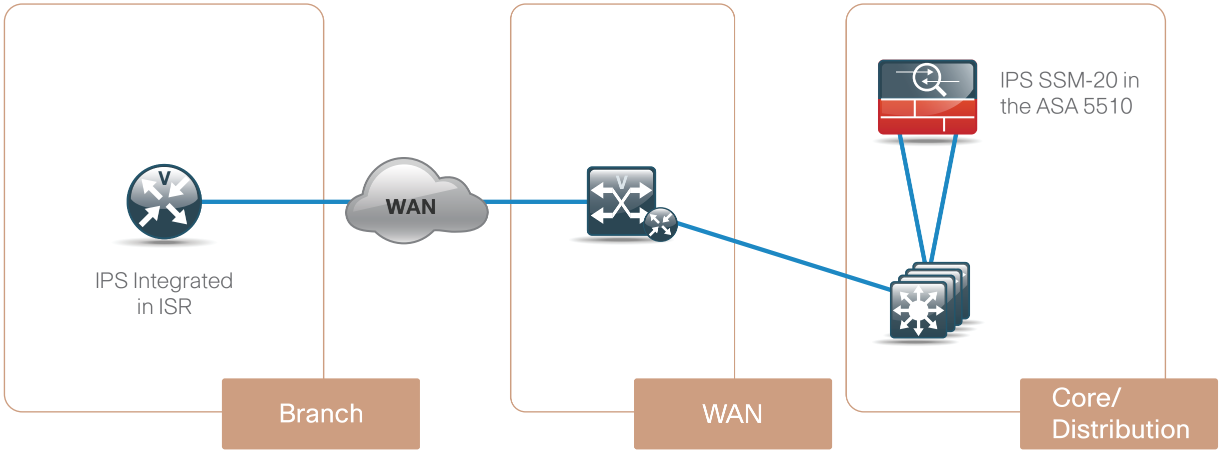
A username and password must be configured; this can be configured locally on the ASA, or the ASA can point at a server for AAA. As a safeguard, it is important to have an account configured locally in case the ASA loses connectivity to the AAA server.

```
username cisco password [password]
```

TECH TIP: All passwords in this document are examples and should not be used in production configurations. Follow your companies password policy, or if no policy exists, a minimum of 8 characters with a combination of uppercase, lowercase, and numerals should be used.

Notes

IPS – Intrusion Prevention System



IPS

Cisco offers IPS in several form factors and performance levels. IPS can be deployed on its own as a standalone service with the Cisco 4200 series appliances, integrated into the ASA with the SSM modules, or integrated into the ISR routers as an AIM module. All of the IPS devices deployed in this design are in promiscuous mode. This allows all the traffic in the network to be inspected without any possibility of network disruption. Once the normal traffic on the network is understood and a policy is created that satisfies the needs of the company, the IPS sensors can be switched from promiscuous mode to inline mode and begin actively blocking attack or out-of-policy traffic. If the company does not require inline functionality and is deploying IPS for compliance reasons, the sensors can be left in promiscuous mode where blocking is not required. Visibility into what is going on inside a corporate network is a great advantage when following up on possible attack, auditing policy, or general troubleshooting; the value of IPS in promiscuous mode should not be overlooked.

This design has **IPS deployed** at three key locations in the network. The **first** IPS, the SSM-20 in the Cisco ASA 5510, is deployed in the Internet Edge. This sensor gives the company the ability to look at traffic coming in and out of the network from the Internet and is a good inspection point for VPN traffic after it is decrypted. The **second** is a Cisco IPS 4200 series sensor connected to the core of the network that can look at traffic off of selected VLANs. This sensor can inspect traffic to and from the server, between wireless and the wired network, and traffic going between the LAN and WAN. The **third** sensor in this network is in the ISR at the branch. In the past, it was possible to centralize IPS at the headend of the WAN, since all traffic had to flow through the headquarters before it could get to anywhere else in the network. Today, though, it is common for branch sites to be able to communicate with other branches or even have Internet access directly with WAN technologies like MPLS.

To configure the IPS module there is an initial setup script that needs to be run on the IPS.

In this example, we are configuring the IPS module in an ASA. To start, log in to the ASA and session to the IPS SSM module:

```
ASA5510# session 1
Opening command session with slot 1.
Connected to slot 1. Escape character
sequence is 'CTRL-^X'.
```

The default username and password for the IPS is username:cisco password:cisco. If you are at this point on any of the Cisco IPS sensors, the setup is identical:

```
login: cisco
Password:
Last login: Tue Dec  9 12:28:24 on pts/1
```

```
***NOTICE***
This product contains cryptographic
features and is subject to United States
and local country laws governing import,
export, transfer, and use. Delivery of
Cisco cryptographic products does not imply
third-party authority to import, export,
distribute, or use encryption. Importers,
exporters, distributors, and users are
responsible for compliance with U.S. and
local country laws. By using this product
you agree to comply with applicable laws and
regulations. If you are unable to comply with
U.S. and local laws, return this product
immediately. A summary of U.S. laws governing
Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/
stqrg.html

If you require further assistance,
please contact us by sending email to
export@cisco.com.

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

At any point, you may enter a question mark
'?' for help.

User ctrl-c to abort configuration dialog at
any prompt.

Default settings are in square brackets '[]'.

Current time: Tue Dec 9 11:52:58 2008

Setup Configuration last modified: Tue Dec 09
12:29:33 2008
```

Enter the hostname, IP address for the external management interface, and the networks from which the IPS module is reachable:

```
Enter host name[sensor]: IPSSSM20B
Enter IP
interface[192.168.1.2/24,192.168.1.1]:
192.168.1.57/24,192.168.1.1

Modify current access list?[no]: yes

Current access list entries:
  No entries
Permit: 192.168.0.0/16
Permit:
Modify system clock settings?[no]:
```

The following configuration was entered:

```
service host
network-settings
host-ip 192.168.1.57/24,192.168.1.1
host-name IPSSSM20B
telnet-option disabled
access-list 192.168.0.0/16
ftp-timeout 300
no login-banner-text
exit
time-zone-settings
offset 0
standard-time-zone-name UTC
exit
summertime-option disabled
ntp-option disabled
exit

[0] Go to the command prompt without saving
this config.
[1] Return to setup without saving this
config.
[2] Save this configuration and exit setup.
[3] Continue to Advanced setup.
```

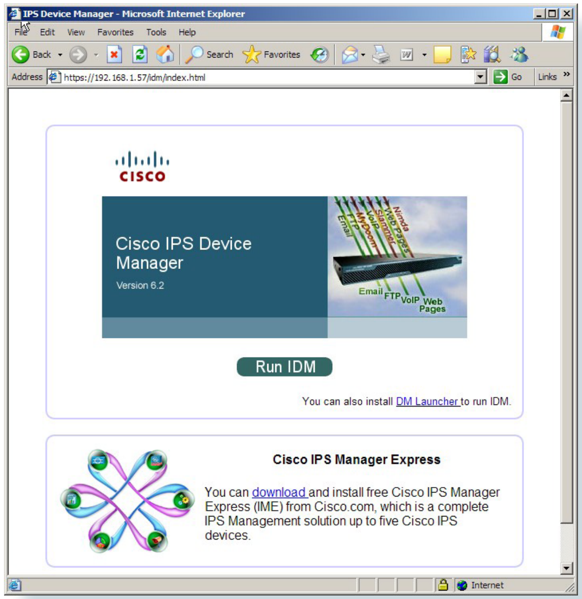
Finally, save the configuration. There is no need to go on to the advanced setup at this point.

```
Enter your selection[3]: 2
--- Configuration Saved ---
Complete the advanced setup using CLI or IDM.
To use IDM,point your web browser at
https://<sensor-ip-address>.  sensor# exit

Remote card closed command session. Press any
key to continue.

Command session with slot 1 terminated.
ASA5510#
```

Now that the IPS is reachable via the management interface, we can use the GUI for the remainder of the configuration. To access the sensor, connect to HTTPS://192.168.1.57. This is the screen you should see upon initial access:



IPS Device Manager - Microsoft Internet Explorer

Address https://192.168.1.57/idm/index.html

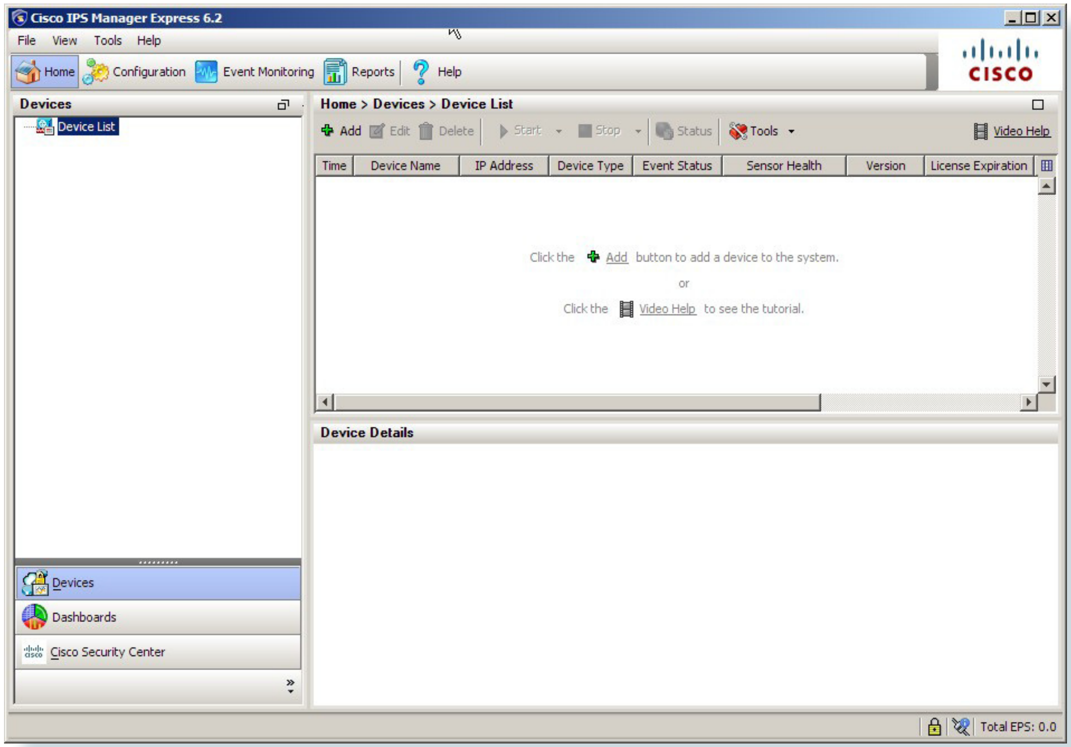
Cisco IPS Device Manager
Version 6.2

You can also install DM Launcher to run IDM.

Cisco IPS Manager Express

You can download and install free Cisco IPS Manager Express (IME) from Cisco.com, which is a complete IPS Management solution up to five Cisco IPS devices.

Since we are configuring several sensors in this network, we want to use Cisco IME (IPS Manager Express). It allows for management and monitoring of up to 5 IPS sensors from a single application. To download IME, go to the IPS initial webpage and the link provided to install on your local machine now. Next, launch IME and you should see the starting IME home screen. To add a sensor, click on the **[add]** button under devices.

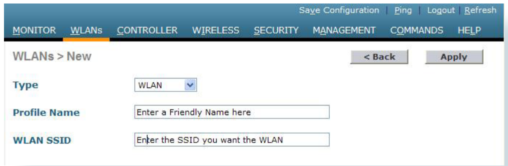

Cisco IPS Manager Express 6.2
File View Tools Help
Home Configuration Event Monitoring Reports Help
cisco
Devices
Device List
Home > Devices > Device List
Add Edit Delete Start Stop Status Tools Video Help
Time Device Name IP Address Device Type Event Status Sensor Health Version License Expiration
Device Details
Devices
Dashboards
Cisco Security Center
Total EPS: 0.0

Click the Add button to add a device to the system.

or

Click the Video Help to see the tutorial.

At this point, for adding a sensor, we need to enter the sensor name, IP address, and the username and password. For IME to add the sensor, it must be running on a machine whose IP address is part of the permitted addresses in the network configured on the sensor during initial setup.

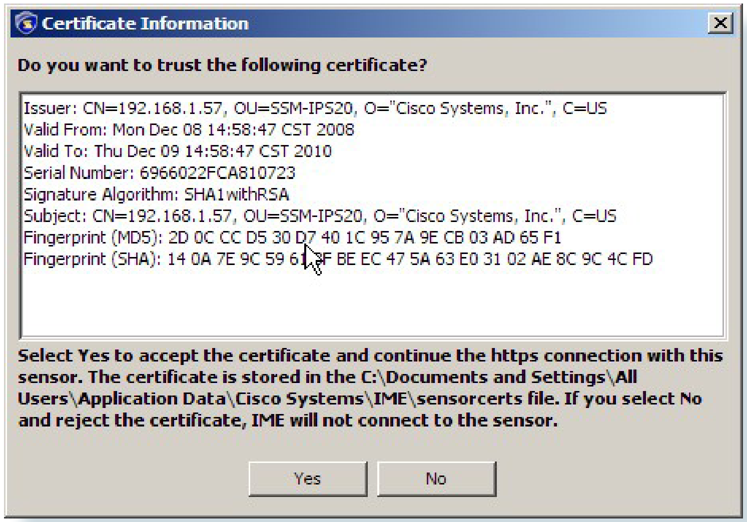

Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
WLANs > New
< Back
Apply

Type: WLAN

Profile Name: Enter a Friendly Name here

WLAN SSID: Enter the SSID you want the WLAN

You should receive a message asking if you want to accept the client certificate from the sensor. Review the certificate information and confirm that it matches the data you entered during setup. If everything is correct, click **[yes]**.



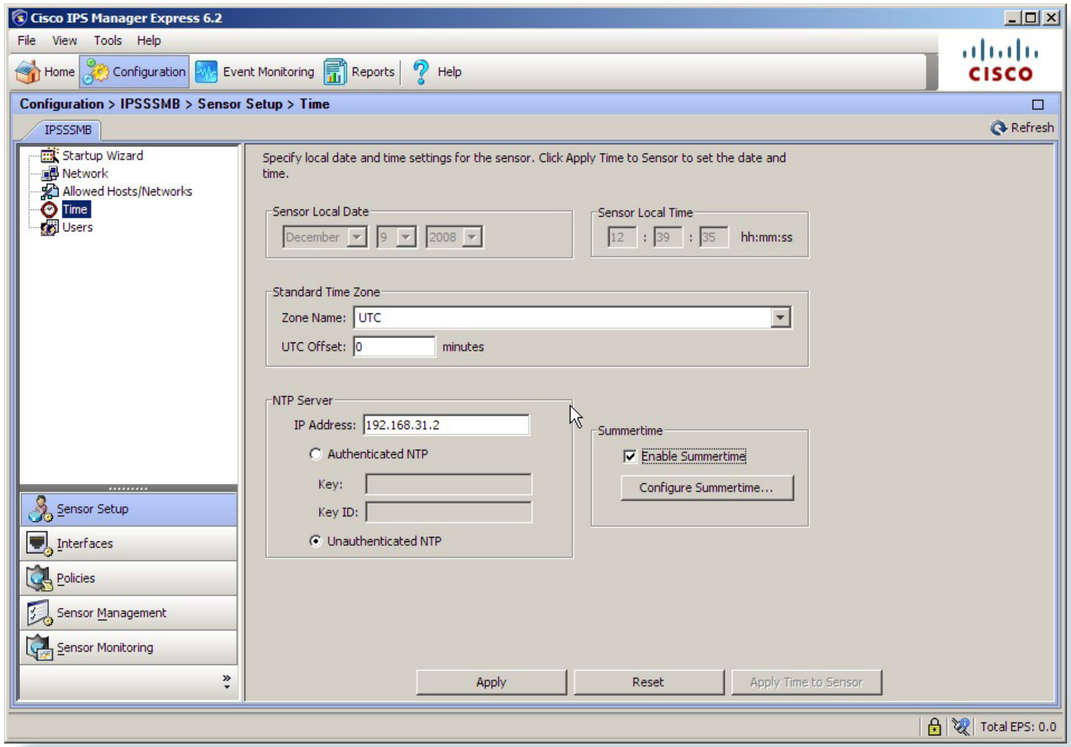
Certificate Information

Do you want to trust the following certificate?

```
Issuer: CN=192.168.1.57, OU=SSM-IPS20, O="Cisco Systems, Inc.", C=US
Valid From: Mon Dec 08 14:58:47 CST 2008
Valid To: Thu Dec 09 14:58:47 CST 2010
Serial Number: 6966022FCA810723
Signature Algorithm: SHA1withRSA
Subject: CN=192.168.1.57, OU=SSM-IPS20, O="Cisco Systems, Inc.", C=US
Fingerprint (MD5): 2D 0C CC D5 30 D7 40 1C 95 7A 9E CB 03 AD 65 F1
Fingerprint (SHA): 14 0A 7E 9C 59 61 3F BE EC 47 5A 63 E0 31 02 AE 8C 9C 4C FD
```

Select Yes to accept the certificate and continue the https connection with this sensor. The certificate is stored in the C:\Documents and Settings\All Users\Application Data\Cisco Systems\IME\sensorcerts file. If you select No and reject the certificate, IME will not connect to the sensor.

Now click on **[Configure]** and **[Time]** and enter the IP address of your NTP server. Time synchronization is critical with IPS as this allows you to pinpoint the time an event occurred and compare it with other sensors in the network for optimal troubleshooting and system management.



Cisco IPS Manager Express 6.2

Specify local date and time settings for the sensor. Click Apply Time to Sensor to set the date and time.

Sensor Local Date: December 9 2008

Sensor Local Time: 12 : 39 : 35 hh:mm:ss

Standard Time Zone

Zone Name: UTC

UTC Offset: 0 minutes

NTP Server

IP Address: 192.168.31.2

○ Authenticated NTP

Key:

Key ID:

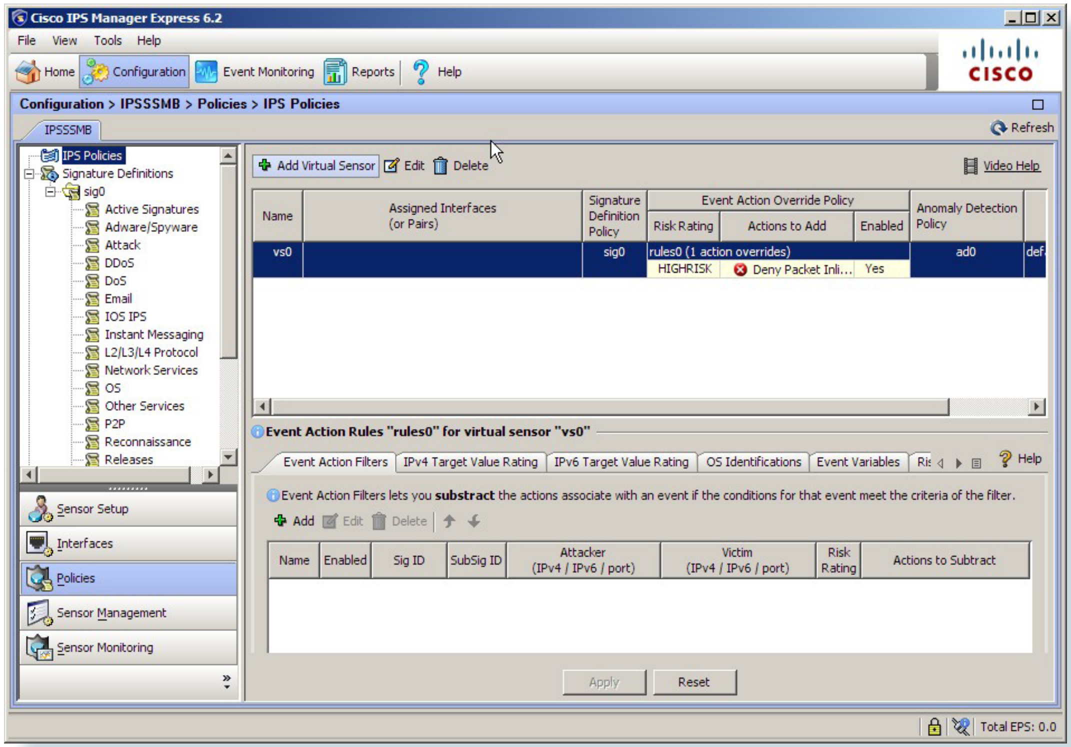
● Unauthenticated NTP

Summertime

☑ Enable Summertime

Configure Summertime...

To get the default policy associated with an interface, click on [Policies] and then edit the existing virtual sensor.



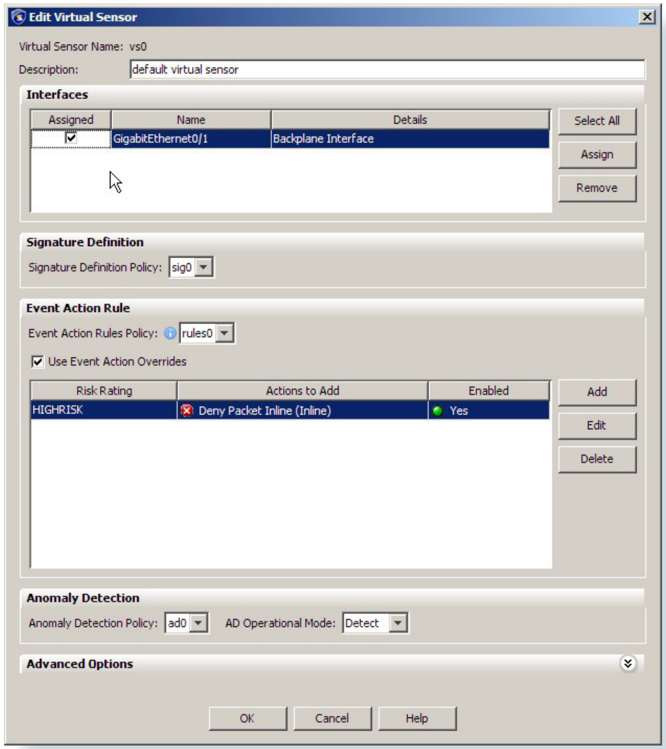
Name	Assigned Interfaces (or Pairs)	Signature Definition Policy	Event Action Override Policy			Anomaly Detection Policy	
			Risk Rating	Actions to Add	Enabled		
vs0		sig0	rules0 (1 action overrides)			ad0	def
			HIGHRISK	Deny Packet Inli...	Yes		

Event Action Rules "rules0" for virtual sensor "vs0"

Event Action Filters lets you **subtract** the actions associate with an event if the conditions for that event meet the criteria of the filter.

Name	Enabled	Sig ID	SubSig ID	Attacker (IPv4 / IPv6 / port)	Victim (IPv4 / IPv6 / port)	Risk Rating	Actions to Subtract

In this case, the IPS module in the ASA only has one interface. Select it, then click [OK] and [Apply].



Virtual Sensor Name: vs0

Description: default virtual sensor

Interfaces

Assigned	Name	Details
☑	GigabitEthernet0/1	Backplane Interface

Signature Definition

Signature Definition Policy: sig0

Event Action Rule

Event Action Rules Policy: rules0

☑ Use Event Action Overrides

Risk Rating	Actions to Add	Enabled
HIGHRISK	Deny Packet Inline (Inline)	● Yes

Anomaly Detection

Anomaly Detection Policy: ad0 AD Operational Mode: Detect

The basic sensor setup is now complete. Notably, all Cisco IPS sensors run the same software; therefore, the setup is always identical except for the number and type of interfaces that are associated with the virtual sensor.

Following are the model-specific instructions for sending network traffic to the sensor for inspection.

ASA 5510

This is a very basic policy that will match and inspect anything coming in or out of the ASA permitted by the access rules. The current mode is "promiscuous," which means that the IPS will only inspect traffic and will not take any drop action.

```
access-list inside_mpc extended permit ip 
192.168.0.0 255.255.0.0 any

access-list outside_mpc extended permit ip 
any 192.168.0.0 255.255.0.0

class-map inside-class
 match access-list inside_mpc
class-map outside-class
 match access-list outside_mpc

policy-map IDS-Inside
 class inside-class
ips promiscuous fail-open sensor vs0
policy-map IDS-Outside
class outside-class
ips promiscuous fail-open sensor vs0

service-policy IDS-Inside interface inside
service-policy IDS-Outside interface outside
```

ISR 2811

The IPS AIM module in the ISR router has a straightforward configuration. The recommended and easiest way to configure the module is to set the IDS-Sensor interface as an unnumbered interface associated to a physical or loopback interface on the ISR. Then configure the IPS module so that it is using an IP address from the same subnet as the interface that it was assigned to. In this example, the module is set to run in a fail-open mode, this allows the module to be taken offline without causing a network outage.

```
interface IDS-Sensor0/0
 ip unnumbered Loopback0
 service-module fail-open
 hold-queue 60 out
```

To connect to the IPS AIM module in the router, enter the following command:

```
service-module ids-Sensor 0/0 session
```

For management access, the router needs a route to the IDS interface so it knows where to send the traffic. Here is the route statement:

```
ip route 192.168.1.66 255.255.255.255 IDS-
Sensor0/0
```

This command must be applied to any interface where traffic inspection is required. Most commonly, traffic inspection is applied where the Ethernet interface connects to the local LAN. This is also where promiscuous or inline mode is specified. For initial deployment, promiscuous mode is preferred.

```
ids-service-module monitoring promiscuous
access-list 199
```

The access list below rejects all traffic. Traffic that is permitted by the IPS ACL bypasses the IPS and traffic that would be denied by the IPS ACL is sent to the IPS module for inspection; the example ACL below directs all traffic to be inspected:

```
access-list 199 deny  ip any any
```

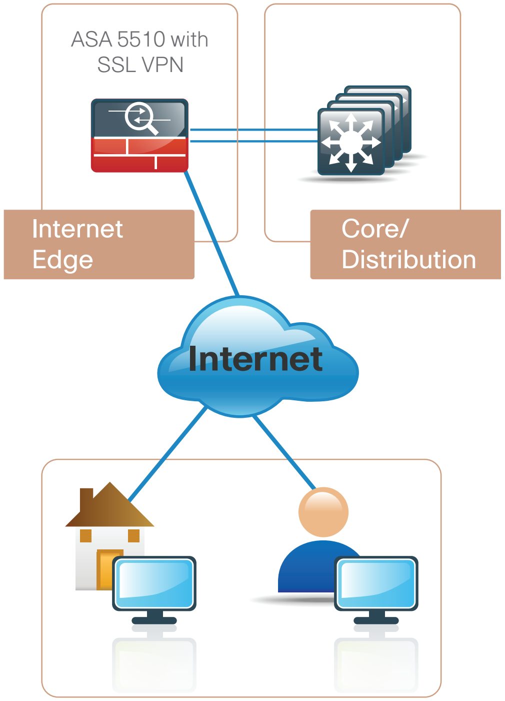
If you wanted to forego inspecting HTTPS traffic, the ACL would look like this:

```
access-list 199 permit tcp any any eq 443
access-list 199 deny ip any any
```

IPS 4200 Connecting to IOS Switch

The IPS 4255 is connected to port Gigabit Ethernet 1/0/9, and the monitor session sends all traffic from VLANs 1-31 to the interface for inspection.

```
monitor session 1 source vlan 1 - 31
monitor session 1 destination interface
Gi1/0/9
```



The Cisco ASA supports IPsec, web portal, and full tunnel SSL VPNs for client-based remote access and IPsec for hardware client or site-to-site VPN. This section describes the basic configuration of remote access IPsec, web portal, and SSL VPNs for basic remote access, plus the configuration of Cisco EZVPN for hardware client (ASA 5505) access.

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 configured on their machine in order to connect and works best with corporate-owned machines such as laptops. SSL VPN access can use a web browser for portal access or the Cisco AnyConnect as a client. SSL access is more flexible and is likely to be accessible from more locations than IPsec, as few companies block HTTPS access out of their networks. With SSL, a restricted level of service can be offered when the user connects from unknown machines, thus providing greater security for the corporate network.

A hardware client is a physical device like a small appliance or router that can provide an “always on” connection back to the corporate network. They are typically used in situations where the user connects regularly, for long periods of time, from a static location, such as a home office user.

Remote Access VPN (SSL and IPsec) Setup

The ASA was configured for remote VPN access by adding a baseline configuration to the default configuration on the appliance. Users are authenticated to the local Windows Domain Controller.

```
group-policy DfltGrpPolicy attributes
 dns-server value 192.168.28.10
 vpn-tunnel-protocol IPSec svc webvpn
 split-tunnel-policy tunnelspecified
 split-tunnel-network-list value RA_
SplitTunnelACL
 address-pools value VPN-Pool
```

This split tunneling access list tunnels all traffic with a destination address of 192.168.0.0/16, to the internal network.

```
access-list RA_SplitTunnelACL standard permit
192.168.0.0 255.255.0.0
```

Remote access clients are assigned an address from the pool VPN-Pool.

```
ip local pool VPN-Pool 192.168.30.129-
192.168.30.254 mask 255.255.255.128

tunnel-group DefaultRAGroup general-
attributes
 address-pool VPN-Pool
```

Web and IPsec VPN clients are authenticated to an AAA server called “AD” and, then, if the server is unreachable, the ASA falls back to local authentication.

```
 authentication-server-group AD LOCAL
tunnel-group DefaultRAGroup ipsec-attributes
 pre-shared-key [password]
tunnel-group DefaultWEBVPNGroup general-
attributes

address-pool VPN-Pool
 authentication-server-group AD LOCAL
```

Here is the config for the AAA server AD. The ASA supports several native authentication protocols and does not require an intermediate RADIUS server to authenticate users via protocols such as LDAP, NT domain, Kerberos, etc.:

```
aaa-server AD protocol nt
aaa-server AD (inside) host 192.168.28.10
 nt-auth-domain-controller 192.168.28.10
```

The last part of the configuration is critical if the internal addresses are being NATed to the outside, which is commonly the case. The configuration below prevents the VPN clients’ return traffic from being NATed and lost when it is sent back from the corporate network. This creates a NAT 0 or NAT exempt rule going out of the Firewall that keeps traffic sourced from the inside from being translated if the destination is the VPN-Pool of addresses. This is one of the most common errors; if left out, the consequence is that a VPN client is connected, but cannot pass traffic.

```
nat (inside) 0 access-list inside_nat0_
outbound
access-list inside_nat0_outbound extended 

permit ip 192.168.0.0 255.255.0.0 
192.168.30.128 255.255.255.128
```

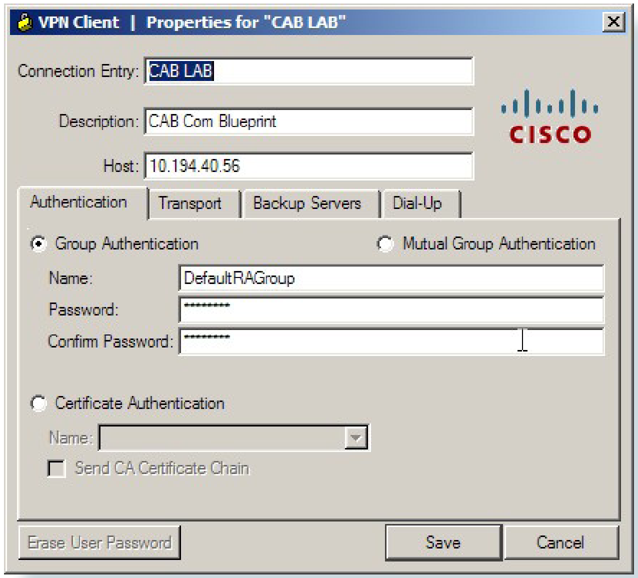
If the web portal is being used, it is important to include the command:

```
http redirect outside 80
```

This will redirect any access to the outside interface on port 80 (HTTP) to port 443 (HTTPS). This also keeps users from having to type HTTPS://ssl.company.com to gain access to the portal.

Software Client Setup

On the client side for IPsec, the user needs the IP address or DNS name of the headend, the group name and password, and a username and password. For SSL VPN access, the user needs the IP address or DNS name of the headend and a username and password.



VPN Client | Properties for "CAB LAB"

Connection Entry: CAB LAB

Description: CAB Com Blueprint

Host: 10.194.40.56

● Group Authentication ○ Mutual Group Authentication

Name: DefaultRAGroup

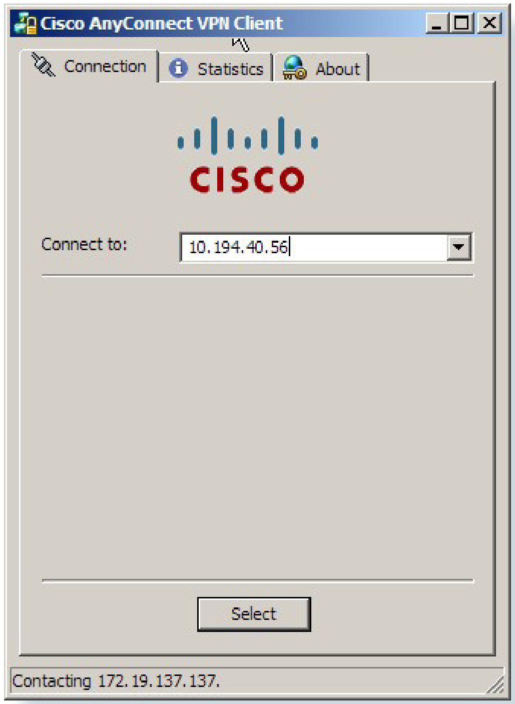
Password: *********

Confirm Password: *********

○ Certificate Authentication

Name:

□ Send CA Certificate Chain



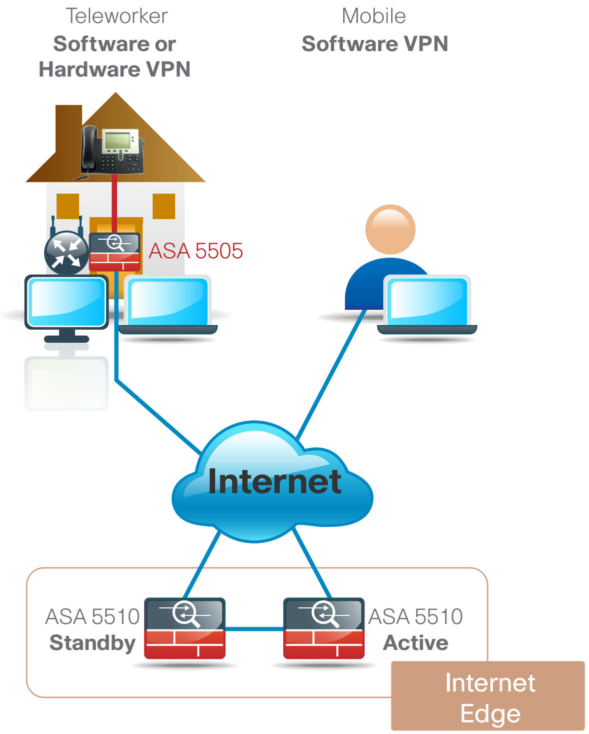
Cisco AnyConnect VPN Client

Connect to: 10.194.40.56

Contacting 172.19.137.137.

VPN Hardware Client Setup

The ASA will support a wide variety of routers as VPN hardware remote clients as well as the ASA 5505. In this example, we are using the ASA 5505 for the remote hardware client.



Headend Configuration

The ASA 5510 headend configuration:

IPsec encryption set to AES-128 and SHA-1. The ASA supports a wide range of transform sets including DES, 3DES, AES 128-256, and MD5 and SHA algorithms. We are using AES-128 because it provides a good balance of security and performance.

```
crypto ipsec transform-set 5505SET  esp-aes esp-sha-hmac
```

Associate the 5505 dynamic crypto map to the 5505SET encryption algorithm:

```
crypto dynamic-map 5505DYN-MAP 5 set transform-set 5505SET
```

Set the lifetime in seconds and bytes so that the connection will rekey the IPsec tunnels after the specified period.

```
crypto dynamic-map 5505DYN-MAP 5 set security-association lifetime 
seconds 28800

crypto dynamic-map 5505DYN-MAP 5 set security-association lifetime 
kilobytes 4608000
```

This configures the headend to advertise a route into the corporate network so that the remote network is reachable.

```
crypto dynamic-map 5505DYN-MAP 5 set reverse-route
```

This associates the crypto map with the outside interface where the ASA 5505 remotes will connect.

```
crypto map 5505MAP 60 ipsec-isakmp dynamic 5505DYN-MAP
crypto map 5505MAP interface outside

group-policy 5505Group internal

group-policy 5505Group attributes
 vpn-tunnel-protocol IPSec
 ip-comp enable
 split-tunnel-policy tunnelspecified
```

We are re-using the same split tunnel policy from the client remote access configuration.

```
 split-tunnel-network-list value RA_SplitTunnelACL
 user-authentication-idle-timeout 480
 nem enable

username 5505site1 password [password]
username 5505site1 attributes
 vpn-group-policy 5505Group

tunnel-group RA5505 type remote-access
tunnel-group RA5505 general-attributes
 default-group-policy 5505Group
tunnel-group RA5505 ipsec-attributes
 pre-shared-key [password]
```

This NAT 0 or NAT exempt rule prevents the return traffic to the VPN remote from being translated.

```
nat (inside) 0 access-list inside_nat0_outbound
access-list inside_nat0_outbound extended permit ip 192.168.0.0 
255.255.0.0 192.168.192.0 255.255.255.0
```

Remote Configuration

Here is the configuration for the remote ASA 5505.

NOTE: The pre-shared-key password and vpn client vpn group password need to match.

```
vpnclient server 10.194.40.56
vpnclient mode network-extension-mode
vpnclient nem-st-autoconnect
vpnclient vpngroup RA5505 password [password]
vpnclient username 5505site1 password [password]
vpnclient enable
```

Technology Overview

The Unified Communication (UC) deployment is greatly simplified by the products and configurations in other modules. For example, access switches provide Power over Ethernet (PoE) for phone deployments without the need for a local power outlet. The entire network is preconfigured with quality of service (QoS) to support high-quality voice and video traffic. The choice of Headquarters (HQ) router in the wide-area network (WAN) module supports the public switched telephone network (PSTN) gateway function, as well as the conference bridge resources with the addition of packet voice digital signal processing (DSP) modules (PVDM) and the required interface card specific to the PSTN connectivity requirements, although at the HQ site, this is very likely to be a T1 or E1 PRI interface. In addition to the other hardware modules added to the router, the IOS code needs to include the "Voice" feature set. Beyond the wired network, the wireless network is also preconfigured for wireless UC devices, providing IP telephony over 802.11 Wi-Fi (referred to as mobility), not only at the HQ, but also within the branches. The security and mobility module is also ready to provide soft phones via VPN, but also regular "hard" phones, which can be plugged into the Cisco ASA 5505, which provides PoE on two ports and connectivity back to the Cisco ASA 5510 at the HQ site. Although not part of the foundation configuration, the HQ Cisco ASA 5510 can also support a phone proxy, allowing the deployment of phones across the Internet in home offices without the Cisco ASA 5505 hardware VPN. Building upon this platform, we add three appliances to provide a highly available and scalable communications manager and a voicemail system capable of email client integration.

The Cisco Unified Communications Manager (Unified CM) was chosen to provide the "PBX" functionality for all users within the HQ, as well as the branch locations. Using two Cisco MCS 7835s for the platform and connecting each to a different switch within the server farm, there is a high level of availability designed in should a switch or MCS platform fail. The selection of the Cisco MCS 7835 was a balance between flexibility for future services and cost. By selecting this platform, there is sufficient capacity for multiple devices for each user. For example, you can enable a desk phone and a soft phone with enough computer telephony integration (CTI) to allow a high percentage of users to also have applications such as click-to-call or other applications remote control their phones. For phones not assigned to a specific user, such as public areas, meeting room phones, storage and break rooms, there is additional capacity available. Beyond the built-in capabilities, the platform can be extended to support other services including presence and instant messaging, advanced conferencing and collaboration, and contact center and video conferencing. The platform hardware includes redundant disk arrays (RAID) and dual power supplies to provide further high availability. For the branch sites, the ISR-based router also includes the capability of providing phone services during a WAN outage or loss of connectivity to the HQ site. Survivable Remote Site Telephony (SRST) is configured within the router and automatically takes over during a failure.

Voicemail is considered part of the UC foundation and is provided by a Cisco Unity Connection deployed on a Cisco MCS 7835 platform, allowing all 1000 users to have a voice mailbox accessible through the phone or integrated into their email client. Unity Connection is deployed as a simple voicemail system, however, with additional configuration, will provide calendar-based call handling integration with Microsoft Exchange, Cisco MeetingPlace® Express, and other networkable voicemail systems as just a few options of this powerful application.

Unity Connection is deployed in the architecture as nonredundant, although the option can be added as required. The Unity Connection configuration is covered in the Rapid Deployment Method using the link provided at the end of this section.

Cisco Unified IP Phones

The choice of phone model depends on the user needs, the environment, and also price. Support for phone services and video would require at least Cisco 7942G or Cisco 7962G phones, with Cisco 7945G and Cisco 7965G providing high-resolution color backlit screens and Gigabit Ethernet capabilities. The Cisco 7931G and Cisco 7911G phones provide less functionality and, hence, are a lower-cost option. The Cisco 7921 and 7925 wireless phones provide mobility, with the Cisco 7937 conference station for conference room and IP Communicator software client providing a desktop computer solution. These are only a selection of the possible phones that can be deployed, although highly recommended options.

Whichever phone is required, the use of Skinny Client Control Protocol (SCCP) is chosen as the signaling protocol, as this also provides video and expansion module capabilities. The wired phones use Cisco Discovery Protocol to acquire the voice VLAN configured in the access switch and then Dynamic Host Configuration Protocol (DHCP) to obtain an IP address, subnet mask, default gateway, domain name, domain name server address(es), and Option 150 information, which provides the two IP addresses of the Unified CMs, which allows the phones to download their configuration files and firmware. Option 150 is added to the voice DHCP scopes and uses the "Publisher" Unified CM as the primary and Subscriber as the secondary option.

The following configuration provides DHCP for one of the voice subnets, where 192.168.28.20 is the IP address of the Publisher and 192.168.29.20 is the IP address of the "Subscriber" Unified CM:

```
ip dhcp pool voice
   network 192.168.12.0 255.255.255.0
   default-router 192.168.12.1
   dns-server 192.168.28.10
   option 150 ip 192.168.28.20 192.168.29.20
   domain-name cisco.com
```

The access layer will automatically negotiate PoE for the phone and also trust the QoS classification used by the phone for the various sessions, including signaling, media, and other services.

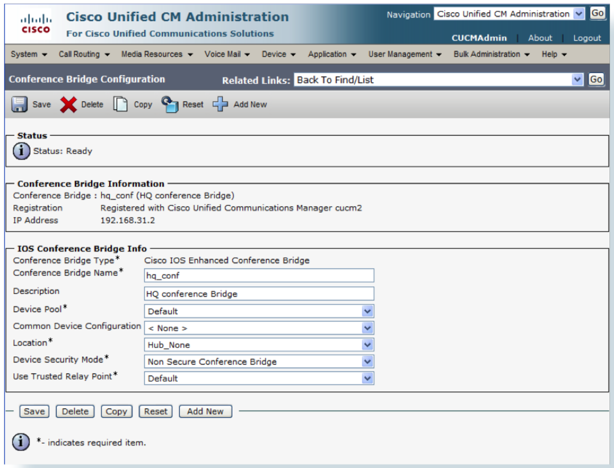
Cisco Unified Communications Manager

The first Unified CM appliance installed is known as the "Publisher," as this contains the master database that all other Unified CMs within the same cluster will subscribe and are hence known as "Subscribers." After the Unified CMs are installed and required service enabled, the configuration can begin. The following are some of main recommendations on how to simplify the deployment of UC.

Media Resources

Media resources such as conference bridges, the Annunciator (system voice messages), and music on hold (MoH) need to be configured as required at each location. They need to be assigned to Media Resource groups and then to the Media Resource List that are then assigned to devices such as phones and gateways to use when needed. In this deployment, the conference bridges were deployed at each site to minimize the use of bandwidth over the WAN for calls with more than two parties. The Annunciator and MoH service are centrally located and use Unicast media by default. Another option that may be considered is Multicast MoH and either deploying centrally or utilizing the branch routers. This option however is not covered in the UC foundation.

An example conference bridge configuration for the Unified CM is:



Conference Bridge Configuration **Related Links:** Back To Find/List

Status

Status: Ready

Conference Bridge Information

Conference Bridge : hq_conf (HQ conference Bridge)
Registration Registered with Cisco Unified Communications Manager cucm2
IP Address 192.168.31.2

IOS Conference Bridge Info

Conference Bridge Type* Cisco IOS Enhanced Conference Bridge
Conference Bridge Name* hq_conf
Description HQ conference Bridge
Device Pool* Default
Common Device Configuration < None >
Location* Hub_None
Device Security Mode* Non Secure Conference Bridge
Use Trusted Relay Point* Default

*- indicates required item.

The corresponding configuration in the HQ router that follows registers 10 conference bridge resources with the subscriber as the highest priority and the publisher as the second priority.

```
voice-card 0
 dsp services dspfarm

voice-port 0/0/1:23
ccm-manager sccp local Port-channel1
sccp local Port-channel1.31
sccp ccm 192.168.29.20 identifier 2 priority
1 version 7.0
sccp ccm 192.168.28.20 identifier 1 priority
2 version 7.0
sccp
```

```
sccp ccm group 1
 bind interface Port-channel1.31
 associate ccm 2 priority 1
 associate ccm 1 priority 2
 associate profile 1 register hq_conf
 switchback method graceful
 switchback interval 60

dspfarm profile 1 conference
 description HQ Conference Bridges
 codec g711ulaw
 codec g711alaw
 codec g729ar8
 codec g729abr8
 codec g729r8
 codec g729br8
 codec g722-64
 codec ilbc
 maximum sessions 10
 associate application SCCP
```

Unified CM can, after some initial configuration, provide auto configuration for many of the device parameters as it moves from site to site, and also provides more rapid and less error-prone deployment mechanisms for static devices. The basis for this deployment method is a feature called device mobility. This works in Unified CM using the IP address of the device to apply a profile, therefore, dynamically assigning site-specific dial plan, media resources groups, local route groups, codec control (regions), and call admission control (locations) configuration. This reduces the number of parameters needed to configure a device when it is added to the system, and also ensures the correct site-specific configuration is applied to a device, as it cannot be incorrectly configured. Should a device be sent to the wrong site, it will dynamically be configured with the correct configuration for the site it is located at.

Combining device mobility with extension mobility, it is possible to provide a mechanism where phones can be shipped directly to site, and all that needs to occur is to deploy the correct model of phone at the user's desk. The user then logs in, and after authentication, Unified CM applies a preconfigured user profile to the phone. The alternative is to configure each user's device specifically and ensure the correct phone is shipped not only to site, but also to the correct user's desk. The rapid deployment method provides a simplified replacement of change of phone. Device mobility benefits wireless and soft clients that roam from one site to another by ensuring the correct resources, regions, and locations are assigned automatically.

Dial Plan

The goal of any dial plan is to provide a simple method for users to dial each other within a site, between sites, and to the PSTN. In addition, some restrictions on where a user may call may be required, and these are implemented as class of restrictions (CoRs). To achieve this, we will use various techniques that, when combined, provide a structured foundation to be customized and expanded by other applications.

Fixed Length Dial Plan

The DNs assigned to the lines are all the same length and consist of an 8, a site code of 2 digits, and then a 4-digit extension number. The number is then masked on the phone using the "text label" to indicate only the 4-digit extension number and, optionally, the user's name. Configuring the external phone number mask allows the direct inward dialing (DID) or PSTN to be displayed on the "black stripe" at the top of the phones with full displays. So that users within a site can dial each other by the use of only the 4-digit extension, a site-specific translation pattern is used that translates a 4-digit number to the 8 + [Site Code] + extension number. Between sites, the users will dial the full 7 digits of 8 + [Site Code] + extension. For calls via the PSTN, they will dial either 9 or 0, based on the local country requirements.

Local Route Groups

The local route group feature introduced in Unified CM version 7.0 simplifies the dial plan configuration required for each branch site. The feature allows Route Lists to contain Route Groups that are dynamically allocated based on the location of the device. Prior to the introduction of this feature, there would be a route list and route group per site. Now, most of the dial plan is global, with only a small portion being required on a per-site basis.

PSTN Gateways

The gateways used for connectivity to the PSTN utilize the router platforms already deployed for the WAN in this architecture. The specific interface and protocol used for connectivity to the PSTN service provider will depend on the country, provider, and cost. Whichever option is used, the recommended protocol to connect the gateway to Unified CM at the HQ site is MGCP, as it combines simple configuration with a large feature set.

As most of the MGCP gateways configuration is downloaded from the Unified CM, it requires only a minimal set of commands to make it operational. The rest is configured using the Unified CM Administrative Interface.

The branch gateways could also utilize MGCP, however, this protocol cannot be utilized when there is no connectivity to the Unified CM servers or in the event of a WAN failure. Under these conditions, there would normally be a fallback protocol configured, such as Session Initiation Protocol (SIP) or H.323 for SRST to use for routing inbound and outbound calls via the PSTN. To further simplify the configuration, SIP is configured for use by Unified CM and is also available for SRST during a WAN failure. This avoids configuring the branch gateway twice, once for MGCP and again for SIP.

All of the techniques discussed above are more fully documented in the Unified Communications SRND, along with additional guidelines for deploying Unified Communications.

The UC Rapid Installation Guide, a step-by-step process for deploying Cisco Unified Communications Manager and Unity, can be found at **Cisco.com**

Notes

Technology Overview

WAN Optimization comes in many forms. Cisco Wide-Area Application Services (WAAS) is specifically designed to accelerate and optimize application traffic over a company WAN. **WAAS has multiple technologies for minimizing the transmission of traffic** between the remote location and the main office, thus reducing bandwidth cost and operating commitment. One technology employed in WAAS is **standard compression**. Standard LZ compression saves 10 to 20 percent. But WAAS provides much more. Another feature is *Data Redundancy Elimination (DRE)*, a caching technology that only sends the delta of a file rather than the whole file back to the main office. Depending on the application, DRE can reduce the traffic between the remote location and main office by 40 percent to 80 percent. DRE technology enables enough bandwidth savings so that you may add other nondata applications such as voice and video over your existing network without upgrading or incurring additional WAN charges. Another feature of WAAS is that while access to files appears to be local, they are actually stored at the main office/campus. This ensures **proper backup and archival** procedures can be applied along with the rest of the corporate data, removing the need for someone at the remote location to perform backup and archiving functions. In summary, the highlights of WAAS include:

- Significantly reduces the bandwidth needed between the remote locations and the main office
- Increases the application performance to LAN-like speeds in those remote locations
- Reduces the OpEx needed to support remote locations by centralizing files and data in the main office

For this deployment, we have modeled a single remote location (remote WAE-NM in branch router), a headquarters headend point (WAE Application Acceleration Appliance) to which all remote locations connect to as a data store, and a Central Manager (WAE Appliance) for managing and monitoring the WAAS network. As you add more branch locations, number of users, or the application type changes in the branches, you may need to modify the design.

Setup Configuration

The following steps summarize the tasks required to perform a basic configuration of a WAAS using the Setup Utility. For additional installation help and configuration options, refer to ***Cisco Wide-Area Application Services Quick Configuration Guide and Configuring Cisco WAAS Network Modules for Cisco Access Routers*** (with respective sections noted below).

Fill out checklist with appropriate values first. This will ensure proper configuration of the devices.

1. Use the Setup Utility and the WAAS CLI, beginning with the WAAS Central Manager, to configure the basic network settings and define the primary interface and device mode for each of the WAEs. See the “Configuring the WAAS Central Manager” later in this section.

2. The Setup Utility includes choosing and enabling an interception method. For our design, we use the WCCP method, but there are other methods that may suit your environment better. We recommend that you discuss the options with an authorized Cisco representative who is a WAAS specialist.

3. The Setup Utility prompts you for a list of intercepting routers and enables TCP promiscuous mode on the WAEs.

4. Using WCCP interception, configure WCCP Version 2 on the routers as described in the “Configuring WCCP” section.

5. Configure the Application Acceleration Appliances using their respective CLI. The CLI configuration for the Application Acceleration Appliances is very similar to the WAAS CM configuration. Use the values in the checklist to help guide you through the process. Access the WAAS Central Manager GUI to manage and monitor your WAAS network. See the “Accessing the WAAS Central Manager GUI and registering WAE devices” section.

6. Register the WAE devices with the CM. Verify that the WAAS application acceleration is working properly.

For further help in this guide, refer to the “Checklist for Configuring a WAAS Network” at the end of this section.

Device Configuration

Configuring the WAAS Central Manager

Connect a serial cable to the console port on the WAAS device and power up the device.

Configure WAAS Settings from the command-line interface.

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

The configuration prompt waits several seconds before proceeding with the WAE setup sequence.

If you want to quit the setup utility, you can press Esc at any time. Enter n at the first prompt to change the default settings. You must change the defaults to configure a WAAS Central Manager.

------------------------

Select device mode:

1. application-accelerator

2. central-manager

Enter your choice [1]: 2

This configuration takes effect after a reload.

Enable CMS automatically after reload? (y/n) [y]: y

------------------------

Select interface to configure as management interface:

NO INTERFACE NAME STATUS IP ADDRESS NETMASK

1. GigabitEthernet 1/0 UP unassigned unassigned

2. GigabitEthernet 2/0 DOWN unassigned unassigned

Enter choice [1]: 1

Continue to answer the questions displayed in the setup utility. You can accept the default choice [shown in brackets] at a prompt by pressing Enter.

If you have Dynamic Host Configuration Protocol (DHCP) enabled in your network, enable DHCP on the WAAS device interface by answering yes (y) to the following question. If you do not have DHCP enabled in your network, answer no (n). No is the default.

Step 4: Enable DHCP on this interface? (y/n) [n]:

Continue to answer the questions displayed in the setup utility.

When you see the prompt to configure a Network Time Protocol (NTP) server, we recommend that you enter the IP address of an NTP server, because clock synchronization between the WAEs in a WAAS network is important.

Step 11: Configure NTP [none]:(Your NTP IP Address)

Configure the time zone of the device. Enter the time zone abbreviation, the number of hours offset from UTC (rounded down to the nearest whole number), and the number of minutes of any partial hour of offset. For example, if your time zone offset is -3:30, then you would set -3 for the hours offset and 30 for the minutes offset.

Step 12: Enter timezone [UTC 0 0] :EST - 5 0

You will then see a summary of the information that you entered. Write down the IP address for future reference. You will need the IP address of the WAAS Central Manager device to launch the WAAS Central Manager GUI.

Accept the configuration when prompted. If you answer no (n), you can reenter and change any values (previous answers are used as the defaults).

Based on the input, the following configurations will be done:

```
device mode central-manager
no central-manager address
no wccp version 2
interface GigabitEthernet 1/0
ip address 10.10.10.10 255.255.255.0
autosense
exit
ip default-gateway 10.10.10.1
ip name-server 172.19.228.233
ip domain-name  example.com
primary-interface GigabitEthernet 1/0
hostname waas-cm
clock timezone EST -5 0
```

Do you accept these configurations? (y/n) [y]: y

Apply the configuration when prompted. Once you apply the configuration, the device is visible on the network and it can be pinged.

Would you like to apply the configurations? (y/n) [y]: y

After specifying the basic network parameters for the designated WAAS Central Manager, save the configuration, and then reload the system so that the new configuration will take effect.

```
waas-cm# copy running-config startup-config
waas-cm# reload
Proceed with reload?[confirm] y
Shutting down all services, will Reload
requested by CLI@ttyS0.
Restarting system.
```

The system reboots. The WAAS Central Manager configuration that you just configured is loaded on the WAAS device named waas-cm, which has now been designated as a WAAS Central Manager.

When prompted, enter the administrator username (admin) and password (default) and press Enter.

Username: admin

Password:

System Initialization Finished.

CLI configuration of Application Acceleration Appliances using the values from your worksheet (see worksheet the end of this section), refer to the Cisco Wide-Area Application Services Quick Configuration Guide for your specific configuration requirements.

Previous answers are used as the defaults.

Configuring WCCP

HQ and BRANCH Router WAAS Commands

Enable the WCCP protocol on the headquarters and branch router.

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

NOTE: IP wccp version 2 will not show in configuration file.

HQ Router WAAS Commands

On the internal or LAN interface (server farm facing) of the HQ router (3845), add the following commands. We are applying the commands to the port channel, which is applied to the ports connected to the network core.

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

On the external router interface (WAN facing) of the HQ router (3845) add the following:

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

BRANCH Router WAAS Commands

WCCP redirection commands on the LAN or client interface:

```
interface FastEthernet0/0.64
 description Access Subnet
 encapsulation dot1Q 64
 ip address 192.168.64.1 255.255.255.0
 ip wccp 61 redirect in
```

WCCP redirection commands on the WAN interface:

```
interface Serial0/0/0:0
ip address 10.0.1.2 255.255.255.252
ip wccp 62 redirect in
```

Here are the steps for adding the WAE headend and branch devices to your WAAS CM:

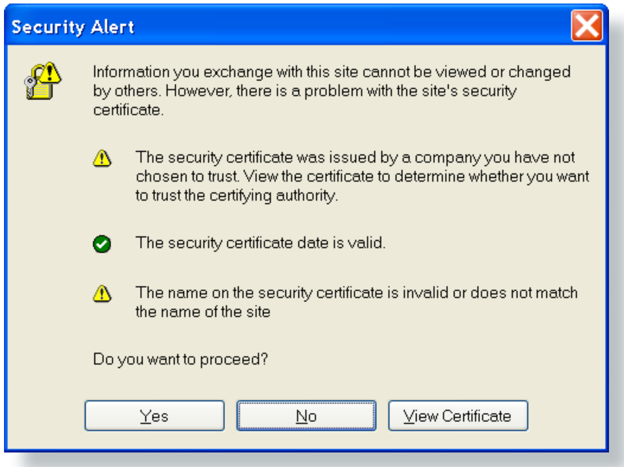
Accessing the WAAS Central Manager GUI and Registering WAE Devices

Step 1: Log in to the web interface for your CM. At your browser, enter the IP address with the following:

https://xxx.xxx.xxx.xxx:8443

So if the IP address for the CM, which we entered in the configuration, is 192.168.28.100, an example of what we would enter is https://192.168.28.100:8443.

Click yes on the security screen and you will be presented with the following:



Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

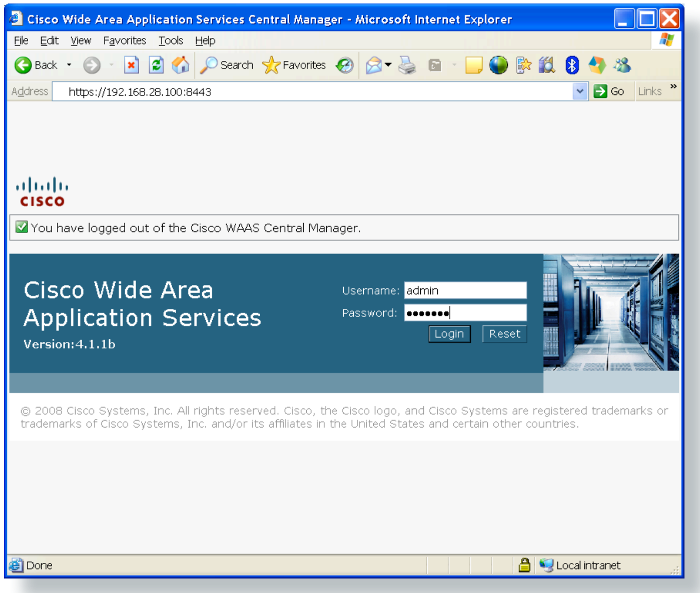
⚠ The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.

✓ The security certificate date is valid.

⚠ The name on the security certificate is invalid or does not match the name of the site

Do you want to proceed?

Notes



Cisco Wide Area Application Services Central Manager - Microsoft Internet Explorer

Address: https://192.168.28.100:8443

☑ You have logged out of the Cisco WAAS Central Manager.

Cisco Wide Area Application Services

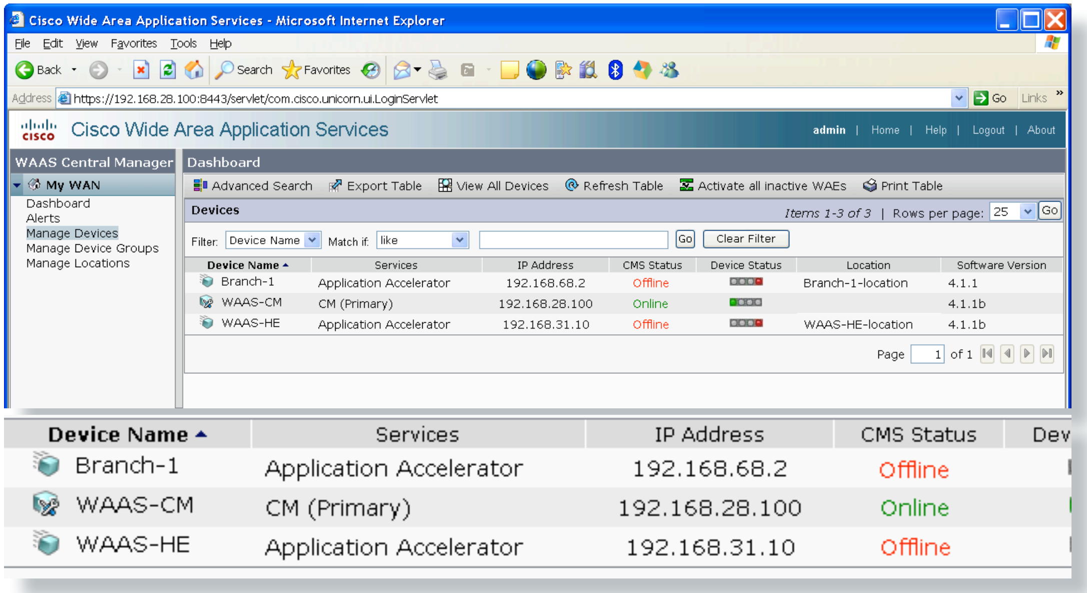
Version:4.1.1b

Username: admin

Password: •••••••

© 2008 Cisco Systems, Inc. All rights reserved. Cisco, the Cisco logo, and Cisco Systems are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

Type in default username: admin, default password: default or username and password you defined and click on the Login button.



Cisco Wide Area Application Services - Microsoft Internet Explorer

Address: https://192.168.28.100:8443/servlet/com.cisco.unicorn.ui.LoginServlet

Cisco Wide Area Application Services

Devices — Items 1-3 of 3 | Rows per page: 25

Filter: Device Name Match if: like

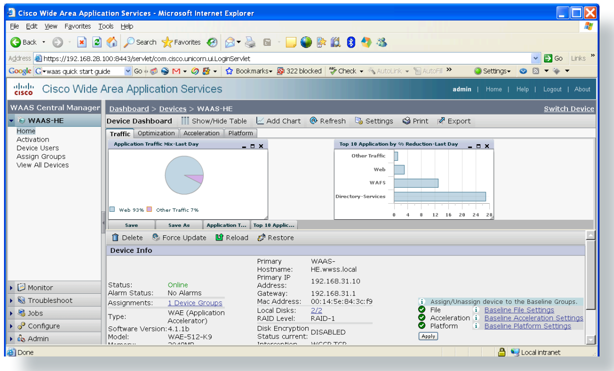
Device Name ▲	Services	IP Address	CMS Status	Device Status	Location	Software Version
Branch-1	Application Accelerator	192.168.68.2	Offline	■■■	Branch-1-location	4.1.1
WAAS-CM	CM (Primary)	192.168.28.100	Online	■■■		4.1.1b
WAAS-HE	Application Accelerator	192.168.31.10	Offline	■■■	WAAS-HE-location	4.1.1b

Page 1 of 1

Device Name ▲	Services	IP Address	CMS Status	Dev
Branch-1	Application Accelerator	192.168.68.2	Offline	
WAAS-CM	CM (Primary)	192.168.28.100	Online	
WAAS-HE	Application Accelerator	192.168.31.10	Offline	

Step 2: Log on to remote WAE devices and register with CM.

Enter the IP address of the WAE device you want to register in the same format as you did with the CM. https://xxx.xxx.xxx.xxx:8443



Cisco Wide Area Application Services - Microsoft Internet Explorer

Address: https://192.168.28.100:8443/servlet/com.cisco.unicorn.ui.LoginServlet

Dashboard > Devices > WAAS-HE

Device Info

Status: Online

Alarm Status: No Alarms

Assignments: 1 Device Groups

Type: WAE (Application Accelerator)

Software Version: 4.1.1b

Model: WAE-512-K9

Primary Hostname: WAAS-HE.wwss.local

Primary IP Address: 192.168.31.10

Gateway: 192.168.31.1

Mac Address: 00:14:5e:84:3c:f9

Local Disks: 2/2

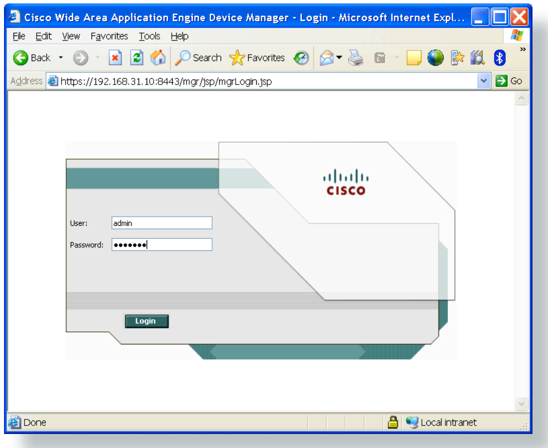
RAID Level: RAID-1

Disk Encryption Status current: DISABLED

Assign/Unassign device to the Baseline Groups.

- File — Baseline File Settings
- Acceleration — Baseline Acceleration Settings
- Platform — Baseline Platform Settings

You should be at the dashboard view. Click on View All Devices. The CM will see the devices, but their status will be red until you register them with the CM.



Cisco Wide Area Application Engine Device Manager - Login - Microsoft Internet Expl...

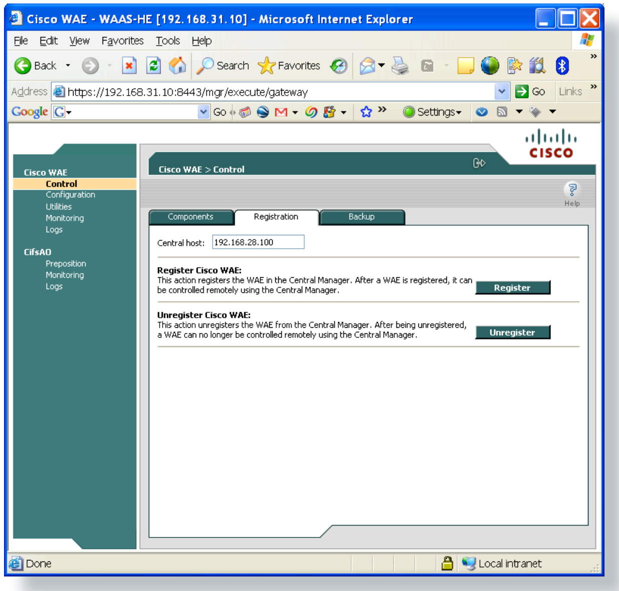
Address: https://192.168.31.10:8443/mgr/jsp/mgrLogin.jsp

User: admin

Password: •••••••

Type in default username: admin, default password: default or username and password you defined.

Click on registration tab.



Central host: 192.168.28.100

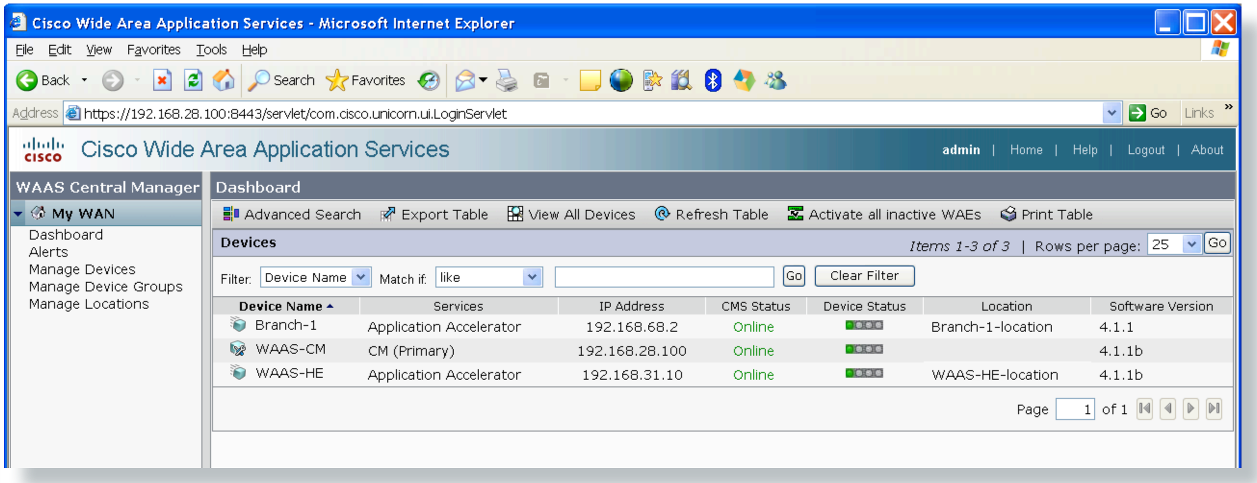
Register Cisco WAE:
This action registers the WAE in the Central Manager. After a WAE is registered, it can be controlled remotely using the Central Manager. Register

Unregister Cisco WAE:
This action unregisters the WAE from the Central Manager. After being unregistered, a WAE can no longer be controlled remotely using the Central Manager. Unregister

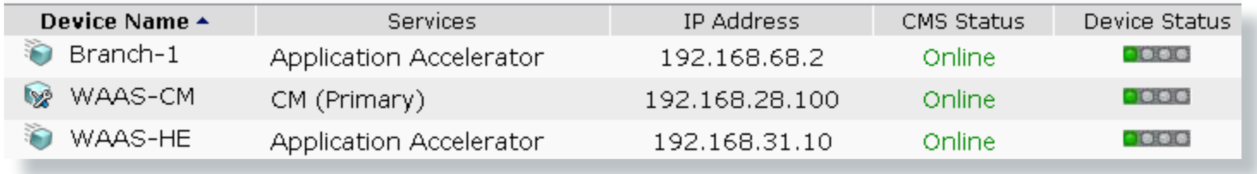
Step 3: Enter IP address of the WAAS CM and click on Register.

Repeat Steps 2 and 3 for other WAE devices.

Go back to CM and view the devices from the dashboard. Click on the refresh button ⟳ and the status for the devices should change to green.


Cisco Wide Area Application Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address https://192.168.28.100:8443/servlet/com.cisco.unicorn.ui.LoginServlet
Go Links
CISCO
Cisco Wide Area Application Services
admin | Home | Help | Logout | About
WAAS Central Manager
My WAN
Dashboard
Alerts
Manage Devices
Manage Device Groups
Manage Locations
Dashboard
Advanced Search
Export Table
View All Devices
Refresh Table
Activate all inactive WAEs
Print Table
Devices
Items 1-3 of 3 | Rows per page: 25 Go
Filter: Device Name Match if: like Go Clear Filter
Page 1 of 1

Device Name ▲	Services	IP Address	CMS Status	Device Status	Location	Software Version
Branch-1	Application Accelerator	192.168.68.2	Online	🟩⬜⬜⬜	Branch-1-location	4.1.1
WAAS-CM	CM (Primary)	192.168.28.100	Online	🟩⬜⬜⬜		4.1.1b
WAAS-HE	Application Accelerator	192.168.31.10	Online	🟩⬜⬜⬜	WAAS-HE-location	4.1.1b



Device Name ▲	Services	IP Address	CMS Status	Device Status
Branch-1	Application Accelerator	192.168.68.2	Online	🟩⬜⬜⬜
WAAS-CM	CM (Primary)	192.168.28.100	Online	🟩⬜⬜⬜
WAAS-HE	Application Accelerator	192.168.31.10	Online	🟩⬜⬜⬜

The lights should all be green and the WAAS network is now optimizing traffic across your WAN. You will need to generate traffic and view some of the graphics on the CM to confirm.

Checklist for Configuring a WAAS Network

Table 1 specifies the different parameters and data needed to set up and configure the WAAS network. For your convenience, you can enter your values in the table and refer back to it when configuring the WAAS network. The values you enter will differ from those in this example; these are for demonstration purposes only.

Table 1. Checklist of WAAS Network System Parameters

Parameter	WAAS Central Manager Values	Main Office WAE Values	Branch Office WAE Values – You will need one Branch column for each branch
Interface Speed	Default	Default	Default
Duplex Mode			
IP Address	192.168.28.100	192.168.31.10	192.168.68.2
Subnet Mask	255.255.255.0	255.255.255.0	255.255.255.0
Default Gateway	192.168.28.1	192.168.31.1	192.168.68.1
DNS Server 1	192.168.28.10	192.168.28.10	192.168.28.10
DNS Server 2			
DNS Domain	cisco.com	cisco.com	cisco.com
WAAS Device (Hostname)	WAAS-CM	WAAS-HE	Branch-1
Windows Domain			
IP Addresses of Routers Intercepting Traffic with WCCP			
NTP Server (Optional)			
Time Zone (Optional)			

Medium Business Deployment Product List

Functional Area	Product	Part Numbers	Software Version
250-600 Network Core	Catalyst 3750G Stackable 12 Port SFP	WS-C3750G-12S-S Catalyst 3750 12 SFP + IPB Image	12.2-40.SE
500-1000 Network Core	Catalyst 4507R Dual Supervisors Dual Power Supplies	WS-C4507R-E Cat4500 E-Series 7-Slot Chassis, fan, no ps, Red Sup Capable WS-X4624-SFP-E Catalyst 4500 E-Series 24-Port GE (SFP) WS-X45-SUP6-E Catalyst 4500 E-Series Sup 6-E, 2x10GE(X2) with Twin Gig	12.2-46.SG
Headquarter access for PC, phones, APs, other devices	Catalyst 3750G Stackable 24 Ethernet 10/100/1000 ports with PoE and 4 SFP ports Cisco Catalyst 3560G 24 & 48 Ethernet 10/100/1000 ports with PoE and 4 SFP ports	WS-C3750G-24PS-S Catalyst 3750 24 10/100/1000T PoE + 4 SFP + IPB Image WS-C3750G-48PS-S Catalyst 3750 48 10/100/1000T PoE + 4 SFP + IPB Image WS-C3560G-24PS-S Catalyst 3560 24 10/100/1000T PoE + 4 SFP + IPB Image WS-C3560G-48PS-S Catalyst 3560 48 10/100/1000T PoE + 4 SFP + IPB Image	12.2-40.SE
Server room switch	Catalyst 3750G 24 & 48 Ethernet 10/100/1000 ports and 4 SFP ports Catalyst 3560G 24 & 48 Ethernet 10/100/1000 ports and 4 SFP ports	WS-C3750G-24TS-S1U Catalyst 3750 24 10/100/1000 + 4 SFP + IPB Image; 1RU WS-C3750G-48TS-S1 Catalyst 3750 48 10/100/1000 + 4 SFP + IPB Image WS-C3560G-24TS-S Catalyst 3560 24 10/100/1000T + 4 SFP + IPB Image WS-C3560G-48TS-S Catalyst 3560 48 10/100/1000T + 4 SFP + IPB Image	12.2-40.SE
Headquarters WAN router	Cisco Integrated Services Router ISR 3845	CISCO3845 HWIC-2CE1T1-PRI	12.4.22T
Branch WAN router	Cisco Integrated Services Router ISR 2811	C2811-VSEC-SRST/K9 HWIC-2CE1T1-PRI	12.4.22T
Branch router modules	Wide Area Acceleration Module Intrusion Prevention Module	NME-WAE-502-K9 AIM-IPS-K9	4.1.1 6.1

Medium Business Deployment Product List

Functional Area	Product	Part Numbers	Software Version
Branch Switch	Catalyst 3750G Stackable 24 & 48 Ethernet 10/100/1000 ports with PoE and 4 SFP ports Cisco Catalyst 3560G 24 & 48 Ethernet 10/100/1000 ports with PoE and 4 SFP ports	WS-C3750G-24PS-S Catalyst 3750 24 10/100/1000T PoE + 4 SFP + IPB Image WS-C3750G-48PS-S Catalyst 3750 48 10/100/1000T PoE + 4 SFP + IPB Image WS-C3560G-24PS-S Catalyst 3560 24 10/100/1000T PoE + 4 SFP + IPB Image WS-C3560G-48PS-S Catalyst 3560 48 10/100/1000T PoE + 4 SFP + IPB Image	12.2-40.SE
Internet Edge Firewall	Adaptive Security Appliance ASA 5510 with the SSM-10 IPS Module	ASA5510-AIP10-K9	8.0.4.ED
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)	6.1
Application Acceleration Headquarters CM Headquarters endpoint	WAE 512 -1 WAE 512 -1	WAE-512-K9 Wide-Area Application Engine 512, 1GB MEM, No HDD Incl.	WAAS 4.1.1
Wireless Access Points	1140 Fixed with Internal Antennas 1250 Ruggedized, External Ant.	AIR-LAP1142N (Country-specific) AIR-AP1252AG (Country-specific)	
Wireless LAN Controller	WLC 4402	AIR-WLC4402-25-K9	5.1
Unified Communications	Cisco Unified Communications Manager—MCS 7835 CMC1 Cisco Unity Connections MCS 7825 UCB1	MCS7835I2-K9-CMC1 (2 required) MCS7825I3-K9-UCB1 Hardware Only	7.0 7.0

Medium Business Deployment Product List

Functional Area	Product	Part Numbers	Software Version
Phones	CP-7921G Wireless Phone CP-7925G Wireless Phone CP-7931G Multibutton Phone CP-7937G Conference Phone CP-7942G B&W Display Phone CP-7962G B&W Display Phone CP-7945G Color Display Phone CP-7965G Color Display Phone CP-7975G Color Executive Phone IPCOMM7-SW Soft Phone	A wide variety of phone models are available that meet specific needs of the user and the country they are deployed in.	
Teleworker	Adaptive Security Appliance ASA 5505	ASA5505-BUN-K9 ASA 5505 Appliance with SW, 10 Users, 8 ports, 3DES/AES	8.0.4

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

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

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

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

C07-542268-00 05/09