



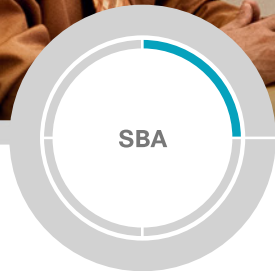
Newer Design Guide Available

Cisco Smart Business Architecture has become part of the Cisco Validated Designs program.

For up-to-date guidance on the designs described in this guide, see <http://cvddocs.com/fw/Aug13-315>

For information about the Cisco Validated Design program, go to <http://www.cisco.com/go/cvd>





Teleworking—Cisco OfficeExtend Deployment Guide

● ● ● SMART BUSINESS ARCHITECTURE

February 2013 Series

Preface

Who Should Read This Guide

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

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

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

Release Series

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

The Release Notes for a series provides a summary of additions and changes made in the series.

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

month year Series

For example, the series of guides that we released in February 2013 is the “February Series”.

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

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

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

How to Read Commands

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

Commands to enter at a CLI appear as follows:

```
configure terminal
```

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

```
ntp server 10.10.48.17
```

Commands with variables that you must define appear as follows:

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

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

```
Router# enable
```

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

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

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

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

Comments and Questions

If you would like to comment on a guide or ask questions, please use the [SBA feedback form](#).

If you would like to be notified when new comments are posted, an RSS feed is available from the SBA customer and partner pages.

Table of Contents

What's In This SBA Guide.....	1
Cisco SBA Solutions	1
Route to Success	1
About This Guide	1
Introduction.....	2
Business Overview.....	2
Technology Overview.....	2

Deployment Details.....	4
Configuring Cisco Secure ACS	4
Configuring Internet Edge	10
Configuring LAN Distribution Switch.....	15
Configuring WLC	16
Configuring Voice/Data Connectivity	25
Configuring AP Authentication.....	32
Configuring Cisco OfficeExtend AP.....	34
Enabling AP Radios	35
Configuring WLC Resiliency	36
Appendix A: Product List	38
Appendix B: Changes	40

What's In This SBA Guide

Cisco SBA Solutions

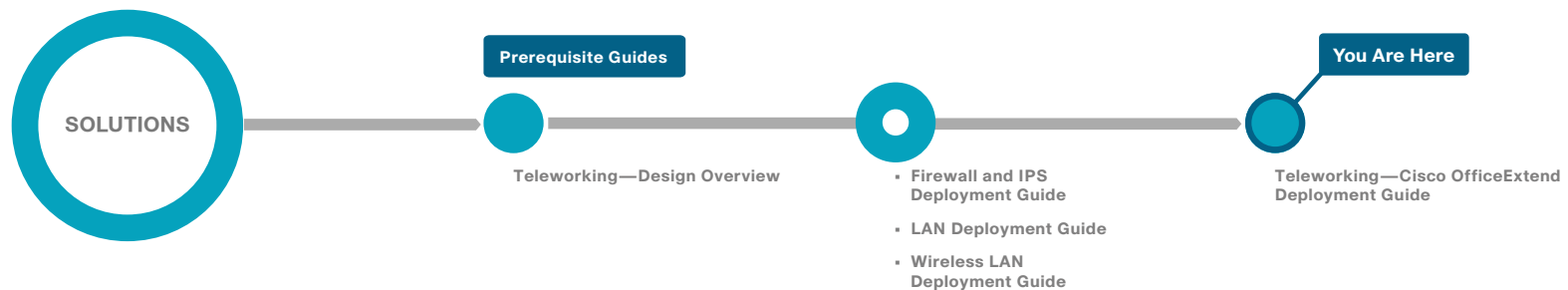
Cisco SBA helps you design and quickly deploy a full-service business network. A Cisco SBA deployment is prescriptive, out-of-the-box, scalable, and flexible.

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

Cisco SBA Solutions are designs for specific problems found within the most common technology trends. Often, Cisco SBA addresses more than one use case per solution because customers adopt new trends differently and deploy new technology based upon their needs.

Route to Success

To ensure your success when implementing the designs in this guide, you should first read any guides that this guide depends upon—shown to the left of this guide on the route below. As you read this guide, specific prerequisites are cited where they are applicable.



About This Guide

This *deployment guide* contains one or more deployment chapters, which each include the following sections:

- **Business Overview**—Describes the business use case for the design. Business decision makers may find this section especially useful.
- **Technology Overview**—Describes the technical design for the business use case, including an introduction to the Cisco products that make up the design. Technical decision makers can use this section to understand how the design works.
- **Deployment Details**—Provides step-by-step instructions for deploying and configuring the design. Systems engineers can use this section to get the design up and running quickly and reliably.

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

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

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

Introduction

Business Overview

Providing employees access to networked business services from a residential environment poses challenges for both the end user and IT operations. For the home-based teleworker, it is critical that access to business services be reliable and consistent, providing an experience that is as similar as sitting in a cubicle or office in the organization's facility. However, residential and urban environments tend to have many potential sources of congestion found on the commonly used 2.4-GHz wireless band. Potential sources of interference include cordless handsets, personal home laptops, iPhones or iPods, baby monitors, and many more. Additionally, solutions must support a wide range of teleworking employees who have varying skill sets, making it critical to have a streamlined and simplified way to implement devices that allow for access to the corporate environment.

IT operations have a different set of challenges when it comes to implementing a teleworking solution, including properly securing, maintaining, and managing the teleworker environment from a centralized location. Because operational expenses are a constant consideration, IT must implement a cost-effective solution that protects an organization's investment without sacrificing quality or functionality.

Technology Overview

The Cisco OfficeExtend solution is specifically designed for the teleworker who primarily uses wireless devices. The solution consists of the following components:

- Cisco Aironet 600 Series OfficeExtend Access Point
- Cisco 2500 Series or Cisco 5500 Series Wireless LAN Controller

Deployment Components

The Cisco Smart Business Architecture (SBA) OfficeExtend deployment is built around two main components: Cisco wireless LAN controllers and Cisco OfficeExtend Access Points.

Cisco Wireless LAN Controllers

Cisco wireless LAN controllers are responsible for system-wide WLAN functions, such as security policies, intrusion prevention, RF management, quality of service (QoS), and mobility. They work in conjunction with Cisco OfficeExtend Access Points to support business-critical wireless applications for teleworkers. Cisco wireless LAN controllers provide the control, scalability, security, and reliability that network managers need to build a secure, scalable teleworker environment.

Although a standalone controller can support up to 500 Cisco OfficeExtend sites, Cisco recommends deploying controllers in pairs for resiliency. There are many different ways to configure controller resiliency; the simplest is to use a primary/secondary model where all the access points at the site prefer to join the primary controller and only join the secondary controller during a failure event. However, even when configured as a pair, wireless LAN controllers do not share configuration information. Each wireless LAN controller must be configured separately.

The following controllers are included in this release of Cisco SBA.

- **Cisco 2500 Series Wireless LAN Controller**—Cisco 2504 Wireless Controllers support up to 75 Cisco OfficeExtend Access Points and 1000 clients. Cisco 2500 Series Wireless LAN Controllers are ideal for small OfficeExtend deployments.
- **Cisco 5500 Series Wireless LAN Controller**—Cisco 5508 Wireless Controllers support up to 500 Cisco OfficeExtend Access Points and 7000 clients, making them ideal for large OfficeExtend deployments.

Because software license flexibility allows you to add additional access points as business requirements change, you can choose the controller that will support your needs long-term, but only pay for what you need, when you need it.

To allow users to connect their endpoint devices to either the organization's on-site wireless network or their at-home teleworking wireless networks without reconfiguration, the Cisco OfficeExtend teleworking solution offers the same wireless Secure Set Identifiers (SSIDs) at teleworkers' homes as those that support data and voice inside the organization.

Cisco OfficeExtend Access Points

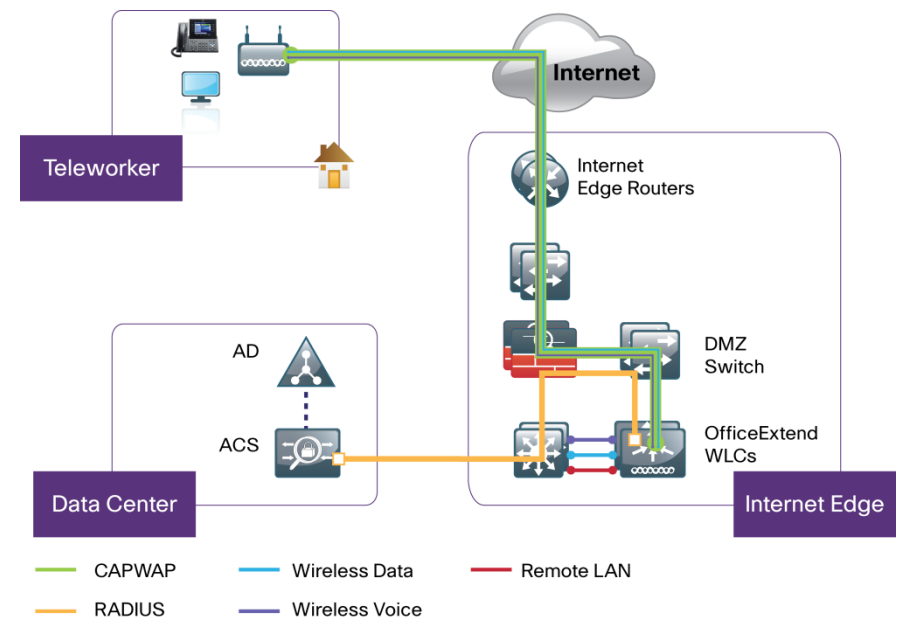
Cisco Aironet 600 Series OfficeExtend Access Points are lightweight. This means they cannot act independently of a wireless LAN controller (WLC). As the access point communicates with the WLC resources, it will download its configuration and synchronize its software/firmware image, if required. Cisco Aironet 600 Series establishes a secure Datagram Transport Layer Security (DTLS) connection between the access point and the controller to offer remote WLAN connectivity using the same profile as at the corporate office. Secure tunneling allows all traffic to be validated against centralized security policies and minimizes the management overhead associated with home-based firewalls.

Cisco OfficeExtend delivers full 802.11n wireless performance and avoids congestion caused by residential devices because it operates simultaneously in the 2.4-GHz and the 5-GHz radio frequency bands. The access point also provides wired Ethernet connectivity in addition to wireless. The Cisco OfficeExtend Access Point provides wired and wireless segmentation of home and corporate traffic, which allows for home device connectivity without introducing security risks to corporate policy.

Design Models

For the most flexible and secure deployment of Cisco OfficeExtend, deploy a dedicated controller pair for Cisco OfficeExtend using the Cisco 5500 or 2500 Series Wireless LAN Controllers. In the dedicated design model, the controller is directly connected to the Internet edge demilitarized zone (DMZ) and traffic from the Internet is terminated in the DMZ versus on the internal network, while client traffic is still directly connected to the internal network.

Figure 1 - Cisco OfficeExtend dedicated design model



In previous releases of this document, we presented a second design model where both internal and Cisco OfficeExtend access points were joined on the same controller pair. Because Cisco OfficeExtend and high availability using AP SSO is not supported concurrently on a controller, we have removed that option in this release.

Deployment Details

This deployment guide uses certain standard design parameters and references various network infrastructure services that are not located within the solution. These parameters are listed in the following table.

Table 1 - Universal design parameters

Network service	Cisco SBA values	Site specific values
Domain name	cisco.local	
Active Directory, Domain Name System (DNS) server, Dynamic Host Configuration Protocol (DHCP) server	10.4.48.10	
Network Time Protocol (NTP) server	10.4.48.17	
Simple Network Management Protocol (SNMP) read-only community	cisco	
SNMP read/write community	cisco123	

Process

Configuring Cisco Secure ACS

1. Create the wireless device group
2. Create the TACACS+ shell profile
3. Modify the device admin policy
4. Create the network access policy
5. Modify the network access policy
6. Create the network device

This guide assumes that you have already configured Cisco Secure Access Control System (ACS). This process includes only the procedures required to support the integration of wireless into the deployment. Full details on Cisco Secure ACS configuration are included in the *Cisco SBA—Borderless Networks Device Management Using ACS Deployment Guide*.

Procedure 1

Create the wireless device group

Step 1: Navigate to the Cisco Secure ACS Administration Page. (Example: <https://acs.cisco.local>)

Step 2: In **Network Resources > Network Device Groups > Device Type**, click **Create**.

Step 3: In the **Name** box, enter a name for the group. (Example: WLC)

Step 4: In the **Parent** box, select **All Device Types**, and then click **Submit**.

Network Resources > Network Device Groups > Device Type > Create

Device Group - General

Name: WLC

Description:

Parent: All Device Types Select

Required fields

Submit Cancel

Procedure 2 Create the TACACS+ shell profile

You must create a shell profile for the WLCs that contains a custom attribute that assigns the user full administrative rights when the user logs in to the WLC.

Step 1: In **Policy Elements > Authorization and Permissions > Device Administration > Shell Profiles**, click **Create**.

Step 2: Under the **General** tab, in the **Name** box, enter a name for the wireless shell profile. (Example: WLC Shell)

Step 3: On the **Custom Attributes** tab, in the **Attribute** box, enter **role1**.

Step 4: In the **Requirement** list, choose **Mandatory**.

Step 5: In the **Value** box, enter **ALL**, and then click **Add**.

Step 6: Click **Submit**.

Policy Elements > Authorization and Permissions > Device Administration > Shell Profiles > Create

General Common Tasks Custom Attributes

Common Tasks Attributes

Attribute	Requirement	Value
role1	Mandatory	All

Manually Entered

Attribute	Requirement	Value
role1	Mandatory	All

Add A Edit V Replace A Delete

Attribute:

Requirement: Mandatory

Attribute: Static

Value:

Required fields

Submit Cancel

Procedure 3 Modify the device admin policy

First, you must exclude WLCs from the existing authorization rule.

Step 1: In **Access Policies > Default Device Admin > Authorization**, click the **Network Admin** rule.

Step 2: Under **Conditions**, select **NDG:Device Type**, and from the **filter** list, choose **not in**.

Step 3: In the box to the right of the **filter** list, select **All Device Types:WLC**, and then click **OK**.

General
Name: Network Admin Status: Enabled

The Customize button in the lower right area of the policy rules screen controls which policy conditions and results are available here for use in policy rules.

Conditions

☒ Identity Group: in All Groups: Network Admins

☐ NDG:Location: -ANY-

☒ NDG:Device Type: not in All Device Types: WLC

☐ Time And Date: -ANY-

Results
Shell Profile: Level 15

Next, create a WLC authorization rule.

Step 4: In **Access Policies > Default Device Admin > Authorization**, click **Create**.

Step 5: In the **Name** box, enter a name for the WLC authorization rule. (Example: WLC Admin)

Step 6: Under **Conditions**, select **Identity Group** condition, and in the box, select **Network Admins**.

Step 7: Select **NDG:Device Type**, and then in the box, select **All Device Types:WLC**.

Step 8: In the **Shell Profile** box, select **WLC Shell**, and then click **OK**.

Step 9: Click **Save Changes**.

General
Name: WLC Admin Status: Enabled

The Customize button in the lower right area of the policy rules screen controls which policy conditions and results are available here for use in policy rules.

Conditions

☒ Identity Group: in All Groups: Network Admins

☐ NDG:Location: -ANY-

☒ NDG:Device Type: in All Device Types: WLC

☐ Time And Date: -ANY-

Results
Shell Profile: WLC Shell

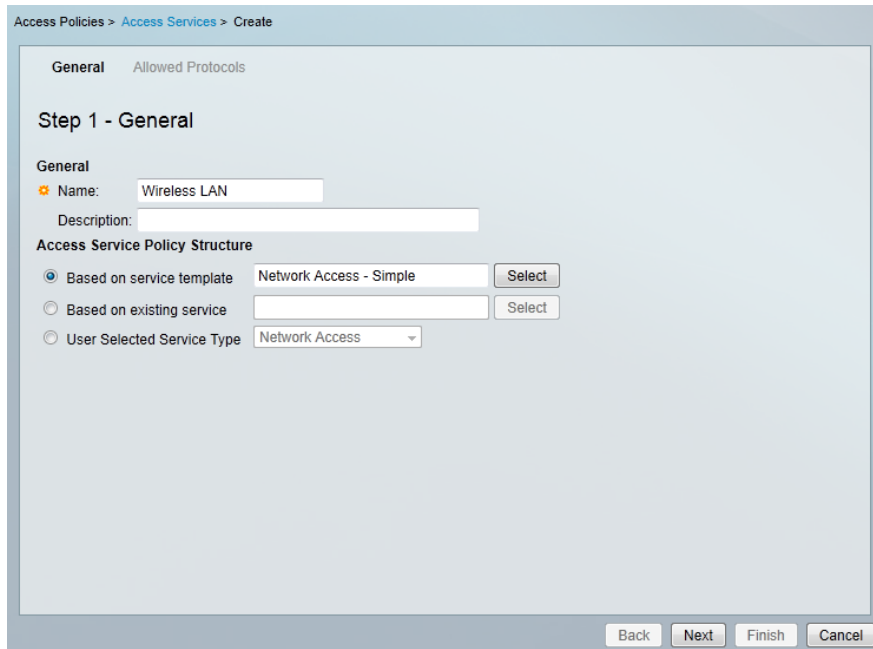
Procedure 4

Create the network access policy

Step 1: In **Access Policies > Access Services**, click **Create**.

Step 2: In the **Name** box, enter a name for the policy. (Example: Wireless LAN)

Step 3: To the right of Based on Service Template, select **Network Access - Simple**, and then click **Next**.



Step 4: On the Allowed Protocols pane, ensure **Allow PEAP** and **Allow EAP-Fast** are selected, and then click **Finish**.

Step 5: On the “Access Service created successfully. Would you like to modify the Service Selection policy to activate this service?” message, click **Yes**.

Step 6: On the Service Selection Policy pane, click **Customize**.

Step 7: Using the arrow buttons, move **Compound Condition** from the **Available** list to the **Selected** list, and then click **OK**.

Step 8: On the Service Selection Rules pane, select the default RADIUS rule.

<input checked="" type="checkbox"/>		Rule-1	match Radius	-ANY-
<input type="checkbox"/>		Rule-2	match Tacacs	-ANY-

Next, you create a new rule for wireless client authentication.

Step 9: Click **Create > Create Above**.

Step 10: In the **Name** box, enter a name for the rule. (Example: Rule Wireless RADIUS)

Step 11: Under Conditions, select **Compound Condition**.

Step 12: In the **Dictionary** list, choose **RADIUS-IETF**.

Step 13: In the **Attribute** box, select **Service-Type**.

Step 14: In the **Value** box, select **Framed**, and then click **Add V**.

Step 15: In the **Attribute** box, select **NAS-Port-Type**.

Step 16: In the **Value** box, select **Wireless - IEEE 802.11**.

Step 17: Under Current Condition Set, click **And > Insert**, and then click **Add V**.

Step 18: Under Results, in the **Service** list, choose **Wireless LAN**, and then click **OK**.

General
Name: Rule Wireless RADIUS Status: Enabled

The Customize button in the lower right area of the policy rules screen controls which policy conditions and results are available here for use in policy rules.

Conditions
☐ Protocol: -ANY-
☒ Compound Condition:
Condition:
Dictionary: RADIUS-IETF Attribute: NAS-Port-Type
Operator: match Value: Static
Current Condition Set:
Add V Edit A Replace V
And
---RADIUS-IETF:Service-Type match Framed
---RADIUS-IETF:NAS-Port-Type match Wireless - IEEE 802.11
Delete Preview
Results
Service: Wireless LAN

Step 19: On the Service Selection Rules pane, click **Save Changes**.

Procedure 5 Modify the network access policy

First you must, create an authorization rule to allow the WLCs to authenticate clients using RADIUS.

Step 1: Navigate to **Access Policies > Wireless LAN > Identity**.

Step 2: In the **Identity Source** box, select **AD then Local DB**, and then click **Save Changes**.

Access Policies > Access Services > Default Network Access > Identity
☒ Single result selection ☐ Rule based result selection
Identity Source: AD then Local DB Select
Advanced Options
Save Changes Discard Changes

Step 3: Navigate to **Access Policies > Wireless LAN > Authorization**.

Step 4: On the Network Access Authorization Policy pane, click **Customize**.

Step 5: Using the arrow buttons, move **NDG:Device Type** from the **Available** list to the **Selected** list, and then click **OK**.

Step 6: In **Access Policies > Wireless LAN > Authorization**, click **Create**.

Step 7: In the **Name** box, enter a name for the rule. (Example: WLC Access)

Step 8: Under **Conditions**, select **NDG:Device Type**, and in the box, select **All DeviceTypes:WLC**.

Step 9: In the **Authorization Profiles** box, select **Permit Access**, and then click **OK**.

General
Name: WLC Access Status: Enabled

The Customize button in the lower right area of the policy rules screen controls which policy conditions and results are available here for use in policy rules.

Conditions
☐ NDG:Location: -ANY-
☐ Time And Date: -ANY-
☒ NDG:Device Type: in All Device Types:WLC Select
☐ Identity Group: -ANY-

Results
Authorization Profiles:
Permit Access
You may select multiple authorization profiles. Attributes defined in multiple profiles will use the value from the first profile defined.
Select Deselect

OK Cancel Help

Step 10: Click **Save Changes**.

Procedure 6 Create the network device

The TACACS+ shell profile that is required when managing the controllers with AAA must be applied to the controllers. This requires that for each controller in the organization; you create a network device entry in Cisco Secure ACS.

Step 1: In **Network Resources > Network Devices and AAA Clients**, click **Create**.

Step 2: In the **Name** box, enter the device host name. (Example: WLC-OEAP-1)

Step 3: In the **Device Type** box, select **All Device Types:WLC**.

Step 4: In the **IP** box, enter the WLC's management interface IP address. (Example: 192.168.19.20)

Step 5: Select **TACACS+**.

Step 6: Enter the TACACS+ shared secret key. (Example: SecretKey)

Step 7: Select **RADIUS**.

Step 8: Enter the RADIUS shared secret key, and then click **Submit**. (Example: SecretKey)

Network Resources > Network Devices and AAA Clients > Create

Name: WLC-OEAP-1
Description:

Network Device Groups
Location: All Locations Select
Device Type: All Device Types:WLC Select

IP Address
☒ Single IP Address ☐ IP Range(s) By Mask ☐ IP Range(s)
IP: 192.168.19.20

Authentication Options
▼ TACACS+ ☒
Shared Secret: SecretKey Hide
☐ Single Connect Device
☒ Legacy TACACS+ Single Connect Support
☐ TACACS+ Draft Compliant Single Connect Support
▼ RADIUS ☒
Shared Secret: SecretKey Hide
CoA port: 1700
☐ Enable KeyWrap
Key Encryption Key:
Message Authenticator Code Key:
Key Input Format ☐ ASCII ☒ HEXADECIMAL

Submit Cancel

Process

Configuring Internet Edge

1. Configure the DMZ switch
2. Configure the DMZ interface
3. Configure address translation
4. Configure security policy

Procedure 1 Configure the DMZ switch

Step 1: On the DMZ switch, create the wireless VLANs.

```
vlan 1119
name WLAN_Mgmt
```

Step 2: Configure the interfaces that connect to the Internet firewalls as trunk ports, and add the wireless VLANs.

```
interface GigabitEthernet1/0/24
description IE-ASA5545Xa Gig0/1
!
interface GigabitEthernet2/0/24
description IE-ASA5545Xb Gig0/1
!
interface range GigabitEthernet1/0/24, GigabitEthernet2/0/24
switchport trunk encapsulation dot1q
switchport trunk allowed vlan add 1119
switchport mode trunk
macro apply EgressQoS
logging event link-status
logging event trunk-status
no shutdown
```

Step 3: Configure the interfaces that are connected to the primary and resilient WLCs' management port.

```
interface GigabitEthernet1/0/5
description DMZ OEAP WLC-1 Management Port
!
interface GigabitEthernet2/0/5
description DMZ OEAP WLC-2 Management Port
!
interface range GigabitEthernet 1/0/5, GigabitEthernet 2/0/5
switchport access vlan 1119
switchport host
macro apply EgressQoS
logging event link-status
no shutdown
```

Procedure 2 Configure the DMZ interface

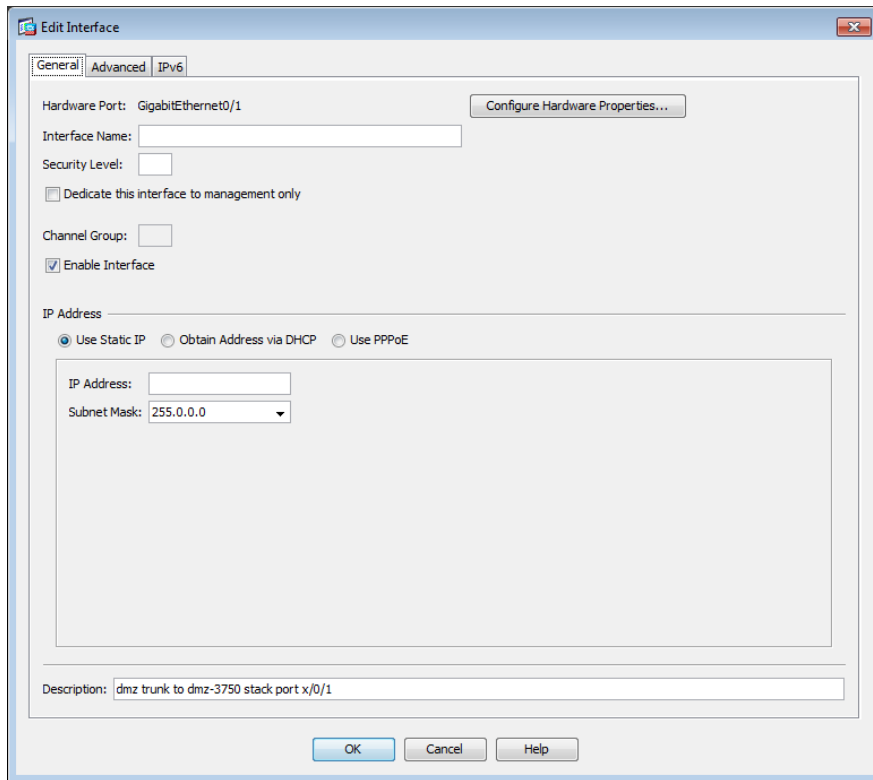
Typically, the firewall DMZ is a portion of the network where traffic to and from other parts of the network is tightly restricted. Organizations place network services in a DMZ for exposure to the Internet; these services are typically not allowed to initiate connections to the inside network, except for specific circumstances.

The various DMZ networks are connected to Cisco ASA on the appliance's GigabitEthernet interface via a VLAN trunk. The IP address assigned to the VLAN interface on the appliance is the default gateway for that DMZ subnet. The DMZ switch's VLAN interface does not have an IP address assigned for the DMZ VLAN.

Step 1: Log in to the Internet edge firewall using Cisco Adaptive Security Device Manager (ASDM).

Step 2: In **Configuration > Device Setup > Interfaces**, click the interface that is connected to the DMZ switch, and then click **Edit**. (Example: GigabitEthernet0/1)

Step 3: Select **Enable Interface**, and then click **OK**.



Step 4: On the Interface pane, click **Add > Interface**.

Step 5: In the **Hardware Port** list, choose the interface that you configured in Step 2. (Example: GigabitEthernet0/1)

Step 6: In the **VLAN ID** box, enter the VLAN number for the DMZ VLAN. (Example: 1119)

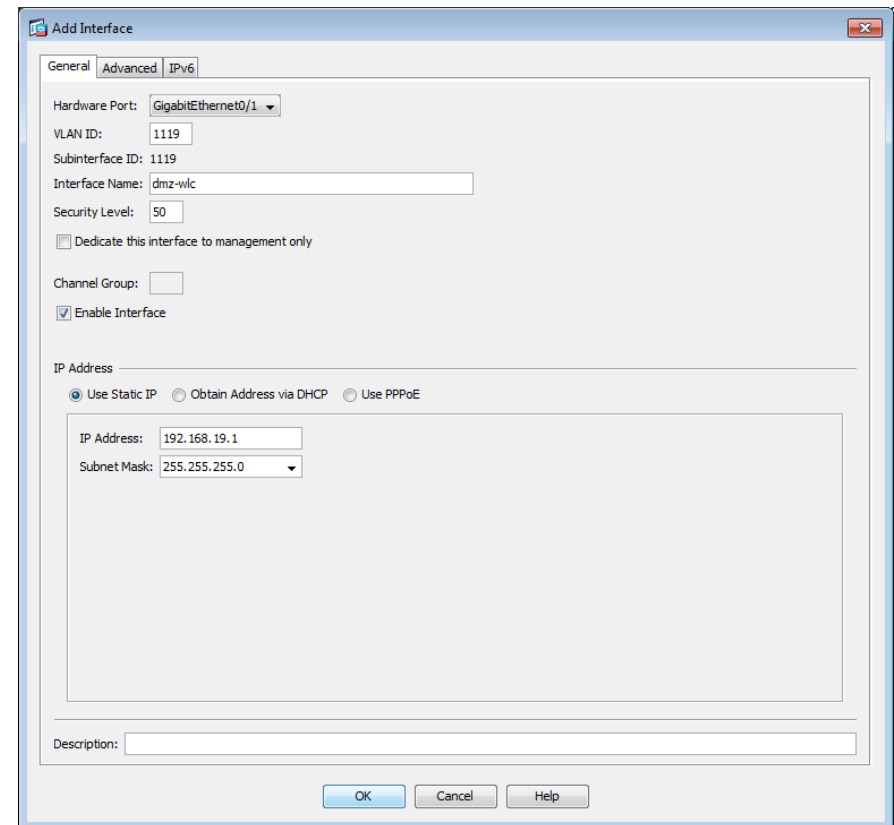
Step 7: In the **Subinterface ID** box, enter the VLAN number for the DMZ VLAN. (Example: 1119)

Step 8: Enter an **Interface Name**. (Example: dmz-wlc)

Step 9: In the **Security Level** box, enter a value of 50.

Step 10: Enter the interface **IP Address**. (Example: 192.168.19.1)

Step 11: Enter the interface **Subnet Mask**, and then click **OK**. (Example: 255.255.255.0)



Procedure 3 Configure address translation

The DMZ network uses private network (RFC 1918) addressing that is not Internet routable, so the firewall must translate the DMZ address of the WLC to an outside public address.

For resiliency in the case of a controller or Internet connection failure, translate the DMZ IP address of the primary controller to the primary Internet connection and the DMZ IP address of the resilient controller to the resilient Internet connection.

The example DMZ address-to-public IP address mapping is shown in the following table.

Table 2 - Address mapping from DMZ address to public IP address

Object information	Primary Internet connection translation	Secondary Internet connection translation
WLC DMZ address	192.168.19.20	192.168.19.21
DMZ object name	dmz-wlc-1	dmz-wlc-2
WLC public address	172.16.130.20	172.17.130.20
Outside object name	outside-wlc-ISP a	outside-wlc-ISP b

Step 1: Navigate to **Configuration > Firewall > Objects > Network Objects/Groups**.

First, you add a network object for the public address of the WLC.

Step 2: Click **Add > Network Object**.

Step 3: In the Add Network Object dialog box, in the **Name** box, enter a description for the primary WLC's public IP address. (Example: outside-wlc-ISP a)

Step 4: In the **IP Address** box, enter the primary WLC's public IP address, and then click **OK**. (Example: 172.16.130.20)

Next, you add a network object for the private DMZ address of the WLC.

Step 5: In the Add Network Object dialog box, in the **Name** box, enter a description for the primary WLC's private DMZ IP address. (Example: dmz-wlc-1)

Step 6: In the **IP Address** box, enter the primary WLC's private DMZ IP address. (Example: 192.168.19.20)

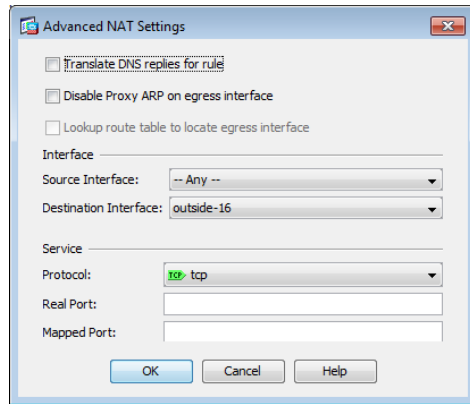
Step 7: Click the two down arrows. The NAT pane expands.

Step 8: Select **Add Automatic Address Translation Rules**.

Step 9: In the **Translated Addr** list, choose the network object created in Step 2, and then click **OK**.

Step 10: Click **Advanced**.

Step 11: In the **Destination Interface** list, choose the interface name for the primary Internet connection, and then click **OK**. (Example: outside-16)



Step 12: Repeat Step 1 through Step 11 for the resilient WLC.

Next, you create a network object group that contains the private DMZ address of every WLC in the DMZ. This makes it easier to configure security policy.

Step 13: Click **Add > Network Object Group**.

Step 14: In the Add Network Object Group dialog box, in the **Group Name** box, enter a name for the group. (Example: dmz-wlc-group)

Step 15: On the Existing Network Objects/Groups pane, select the primary WLC, and then click **Add >>**.

Step 16: On the Existing Network Objects/Groups pane, select the resilient WLC, click **Add >>**, and then click **OK**.

Next, you insert a new rule above the rule you selected that enables the WLCs in the DMZ to communicate with the AAA server in the data center for management and user authentication.

Step 3: Click **Add > Insert**.

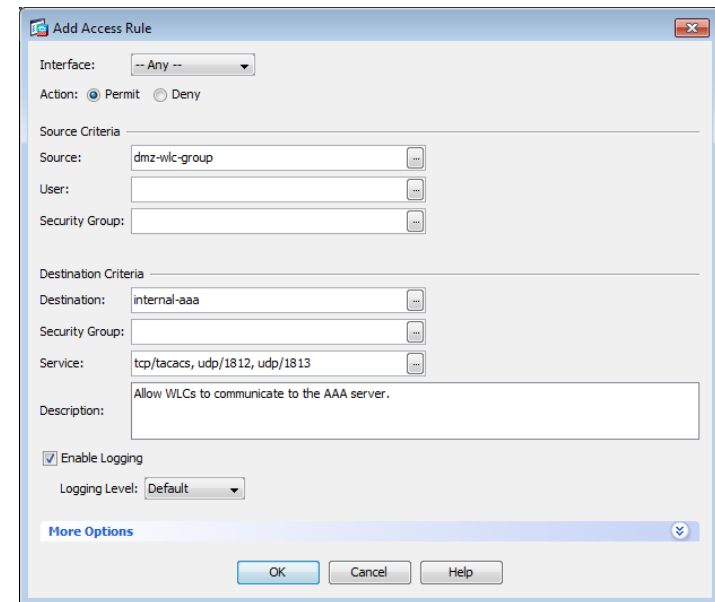
Step 4: In the Internet Access Rule dialog box, in the **Interface** list, select **—Any—**.

Step 5: To the right of Action, select **Permit**.

Step 6: In the **Source** list, choose the network object group created in Procedure 3, “Configure address translation,” Step 14. (Example: dmz-wlc-group)

Step 7: In the **Destination** list, choose the network object for the AAA server. (Example: internal-aaa)

Step 8: In the **Service** list, enter **tcp/tacacs, udp/1812, udp/1813**, and then click **OK**.



Next, you must enable the WLCs in the DMZ to synchronize their time with the NTP server in the data center.

Procedure 4 Configure security policy

Step 1: Navigate to **Configuration > Firewall > Access Rules**.

Step 2: Click the rule that denies traffic from the DMZ toward other networks.



Step 9: Click **Add > Insert**.

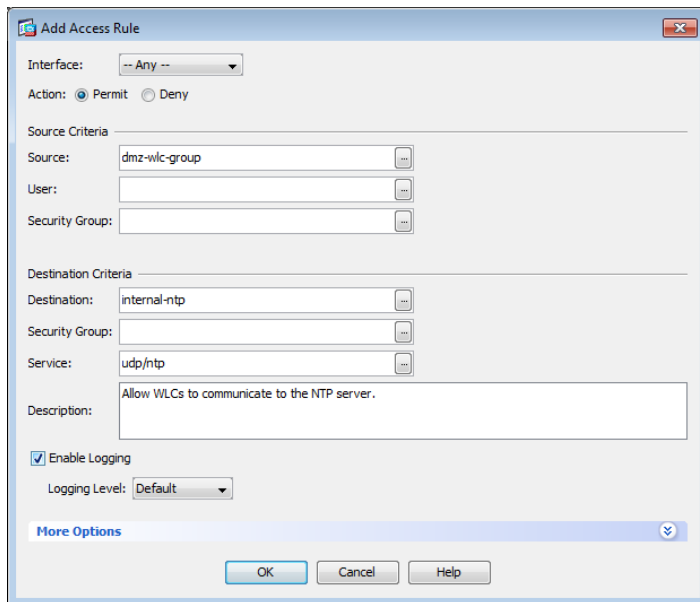
Step 10: In the Internet Access Rule dialog box, in the **Interface** list, select **—Any—**.

Step 11: To the right of Action, select **Permit**.

Step 12: In the **Source** list, choose the network object group created in Procedure 3, "Configure address translation," Step 14. (Example: dmz-wlc-group)

Step 13: In the **Destination** list, choose the network object for the NTP server. (Example: internal-ntp)

Step 14: In the **Service** list, enter **udp/ntp**, and then click **OK**.



Next, you enable the WLCs in the DMZ to be able to download new software via FTP.

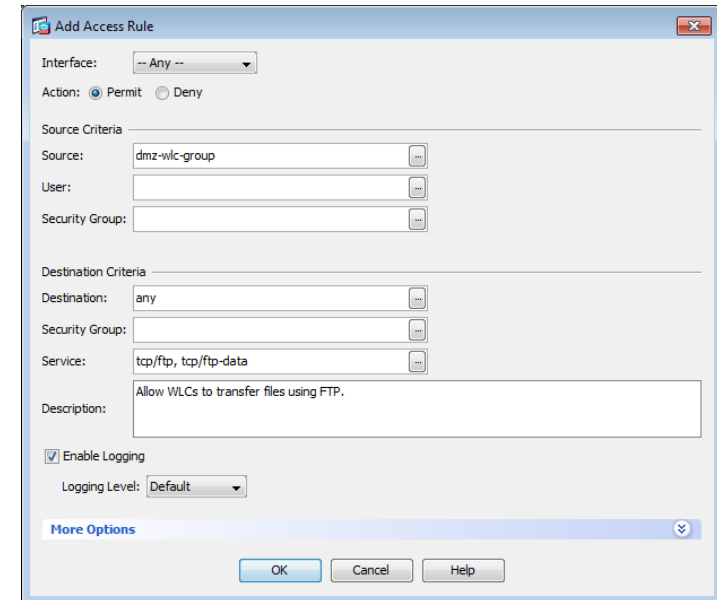
Step 15: Click **Add > Insert**.

Step 16: In the Internet Access Rule dialog box, in the **Interface** list, select **—Any—**.

Step 17: To the right of Action, select **Permit**.

Step 18: In the **Source** list, choose the network object group created in Procedure 3, "Configure address translation," Step 14. (Example: dmz-wlc-group)

Step 19: In the **Service** list, enter **tcp/ftp, tcp/ftp-data**, and then click **OK**.



Now you enable the Cisco OfficeExtend Access Points to communicate with the WLCs in the DMZ using Control and Provisioning of Wireless Access Points (CAPWAP).

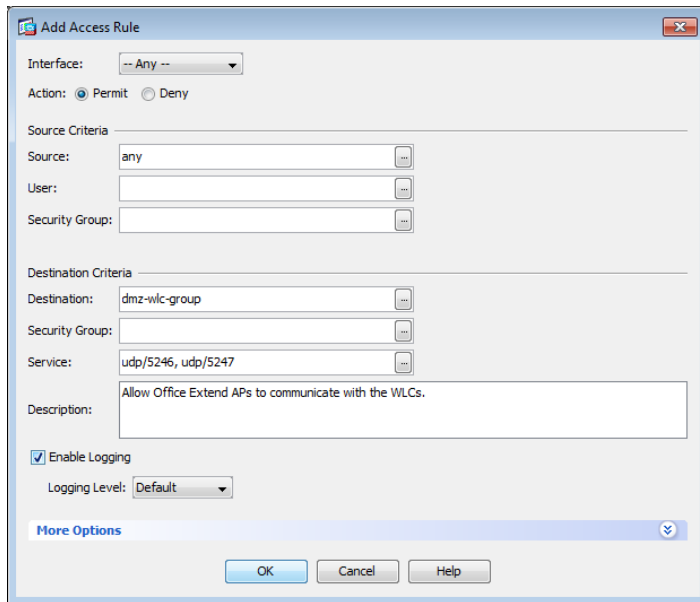
Step 20: Click **Add > Insert**.

Step 21: In the Internet Access Rule dialog box, in the **Interface** list, select **—Any—**.

Step 22: To the right of Action, select **Permit**.

Step 23: In the **Destination** list, choose the network object group created in Procedure 3, "Configure address translation," Step 14. (Example: dmz-wlc-group)

Step 24: In the **Service** list, enter **udp/5246, udp/5247**, and then click **OK**.



Step 25: Click **Apply**.

Process

Configuring LAN Distribution Switch

1. Configure the distribution switch

Step 1: On the LAN distribution switch, create the wireless VLANs that you are connecting to the distribution switch.

```
vlan 244
  name OEAP_Data
vlan 248
  name OEAP_Voice
vlan 252
  name OEAP_RemoteLAN
```

Step 2: Configure a VLAN interface (SVI) for each VLAN so devices in the VLAN can communicate with the rest of the network.

```
interface Vlan244
  description OEAP Wireless Data Network
  ip address 10.4.144.1 255.255.252.0
  no shutdown
!
interface Vlan248
  description OEAP Wireless Voice Network
  ip address 10.4.148.1 255.255.252.0
  no shutdown
!
interface Vlan252
  description OEAP Remote LAN Data Network
  ip address 10.4.152.1 255.255.252.0
  no shutdown
```

Procedure 1 Configure the distribution switch

The VLANs used in the following configuration examples are:

- Wireless data—**VLAN 244, IP: 10.4.144.0/22**
- Wireless voice—**VLAN 248, IP 10.4.148.0/22**
- Remote LAN—**VLAN 252, IP 10.4.152.0/24**

Step 3: For interface configuration, an 802.1Q trunk is used for the connection to the WLCs. This allows the distribution switch to provide the Layer 3 services to all the networks defined on the WLC. The VLANs allowed on the trunk are pruned to only the VLANs that are active on the WLC.

If you are deploying the Catalyst 6500 or 4500 LAN distribution switch, you do not need to use the **switchport trunk encapsulation dot1q** command in the following configurations.

```
interface GigabitEthernet [port 1]
  description OEAP WLC-1
interface GigabitEthernet [port 2]
  description OEAP WLC-2
!
interface range GigabitEthernet [port 1], GigabitEthernet
[port 2]
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 244,248,252
  switchport mode trunk
  macro apply EgressQoS
  logging event link-status
  logging event trunk-status
  no shutdown
```

Process

Configuring WLC

1. Configure the WLC platform
2. Configure the WLC for NAT
3. Configure the time zone
4. Configure SNMP
5. Limit what networks can manage the WLC
6. Configure wireless user authentication
7. Centralize management authentication

Procedure 1

Configure the WLC platform


After the WLC is physically installed and powered up, you will see the following on the console:

```
Welcome to the Cisco Wizard Configuration Tool
Use the '-' character to backup
Would you like to terminate autoinstall? [yes]: YES
```

Step 1: Enter a system name. (Example: WLC-OEAP-1)

```
System Name [Cisco_7e:8e:43] (31 characters max): WLC-OEAP-1
```

Step 2: Enter an administrator username and password.

**Tech Tip**

Use at least three of the following four classes in the password: lowercase letters, uppercase letters, digits, or special characters.

```
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 port interface address.

```
Service Interface IP address Configuration [none] [DHCP]: DHCP
```

Step 4: Disable link aggregation. This enables clients to attach directly to the LAN distribution switch and not have to traverse the firewall.

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

Step 5: Enter the IP address and subnet mask for the management interface.

```
Management Interface IP Address: 192.168.19.20
Management Interface Netmask: 255.255.255.0
Management interface Default Router: 192.168.19.1
Management Interface VLAN Identifier (0 = untagged): 0
Management Interface Port Num [1 to 8]: 1
```

Step 6: Enter the default DHCP server for clients. (Example: 10.4.48.10)

Management Interface DHCP Server IP Address: **10.4.48.10**

Step 7: If you are deploying a Cisco 5500 Series Wireless LAN Controller (WLC), disable high availability. High availability and Cisco OfficeExtend are not supported concurrently on the controller.

Enable HA [yes] [NO]: **NO**

Step 8: Configure the virtual interface the WLC uses for Mobility DHCP relay and inter-controller communication. (Example: 192.0.2.1)

Virtual Gateway IP Address: **192.0.2.1**

Step 9: If you are configuring a Cisco 2500 Series WLC, enter the multicast IP address for the communication of multicast traffic by using the multicast-multicast method.

Multicast IP Address: **239.40.40.40**

Step 10: Enter a name that will be used as the default mobility and RF group. (Example: OEAP-1)

Mobility/RF Group Name: **OEAP-1**

Step 11: Enter an SSID for the WLAN SSID that supports data traffic. You will be able to leverage this later in the deployment process.

Network Name (SSID): **WLAN-Data**

Configure DHCP Bridging Mode [yes] [NO]: **NO**

Step 12: Disable DHCP snooping. This increases resiliency during a WLC failure.

Allow Static IP Addresses {YES} [no]: **YES**

Step 13: Specify that the RADIUS Server will be configured later using the GUI.

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

Step 14: Enter the correct country code for the country where you are deploying the WLC.

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

Step 15: Enable all wireless networks.

Enable 802.11b network [YES] [no]: **YES**

Enable 802.11a network [YES] [no]: **YES**

Enable 802.11g network [YES] [no]: **YES**

Step 16: Enable the radio resource management (RRM) auto-RF feature. This helps you keep your network up and operational.

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

Step 17: Synchronize the WLC clock to your organization's NTP server.

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

Enter the NTP server's IP address: **10.4.48.17**

Enter a polling interval between 3600 and 604800 secs: **86400**

Step 18: Save the configuration. If you respond with **no**, the system will restart without saving the configuration and you will have to complete this procedure again.

Configuration correct? If yes, system will save it and reset.

[yes] [NO]: **YES**

Configuration saved!

Resetting system with new configuration

Step 19: After the WLC has reset, log in to the Cisco Wireless LAN Controller Administration page using the credentials defined in Step 2. (Example: <https://wlc-oeap-1.cisco.local/>)

Procedure 2

Configure the WLC for NAT

The Internet edge firewall translates the IP address of the WLC management interface in the DMZ to a publicly reachable IP address so Cisco OfficeExtend Access Points at teleworker locations can reach the WLC. However, in order for the Cisco OfficeExtend Access Points to be able to communicate with the WLC, the publicly reachable address must also be configured on the WLC management interface.

Step 1: In **Controller > Interfaces**, click the **management** interface.

Step 2: Select **Enable NAT Address**.

Step 3: In the **NAT IP Address** box, enter the publicly reachable IP address, and then click **Apply**. (Example: 172.16.130.20)

The screenshot shows the Cisco WLC configuration page for the 'management' interface. The 'NAT Address' section is highlighted, showing 'Enable NAT Address' checked and 'NAT IP Address' set to 172.16.130.20. Other sections like General Information, Configuration, Interface Address, Physical Information, DHCP Information, and Access Control List are also visible.

Step 3: Click **Set Timezone**.

The screenshot shows the Cisco WLC 'Set Time' page. The 'Set Timezone' button is highlighted. The 'Current Time' is Tue May 31 11:07:38 2011. The 'Date' section shows Month: May, Day: 31, Year: 2011. The 'Time' section shows Hour: 11, Minutes: 7, Seconds: 38. The 'Timezone' section shows Delta: 0 hours, 0 mins, and Location: (GMT -8:00) Pacific Time (US and Canada).

Procedure 4 Configure SNMP

Step 1: In **Management > SNMP > Communities**, click **New**.

Step 2: Enter the **Community Name**. (Example: cisco)

Step 3: Enter the **IP Address**. (Example: 10.4.48.0)

Step 4: Enter the **IP Mask**. (Example: 255.255.255.0)

Procedure 3 Configure the time zone

Step 1: Navigate to **Commands > Set Time**.

Step 2: In the **Location** list, choose the time zone that corresponds to the location of the WLC.

Step 5: In the **Status** list, choose **Enable**, and then click **Apply**.

The screenshot shows the Cisco Management interface with the 'MANAGEMENT' tab selected. The left sidebar lists various configuration categories, including 'SNMP'. The main content area is titled 'SNMP v1 / v2c Community > New'. It contains a form with the following fields: 'Community Name' (cisco), 'IP Address' (10.4.48.0), 'IP Mask' (255.255.255.0), 'Access Mode' (Read Only), and 'Status' (Enable). There are '< Back' and 'Apply' buttons at the top right of the form.

Step 6: In **Management > SNMP > Communities**, click **New**.

Step 7: Enter the **Community Name**. (Example: cisco123)

Step 8: Enter the **IP Address**. (Example: 10.4.48.0)

Step 9: Enter the **IP Mask**. (Example: 255.255.255.0)

Step 10: In the **Access Mode** list, choose **Read/Write**.

Step 11: In the **Status** list, choose **Enable**, and then click **Apply**.

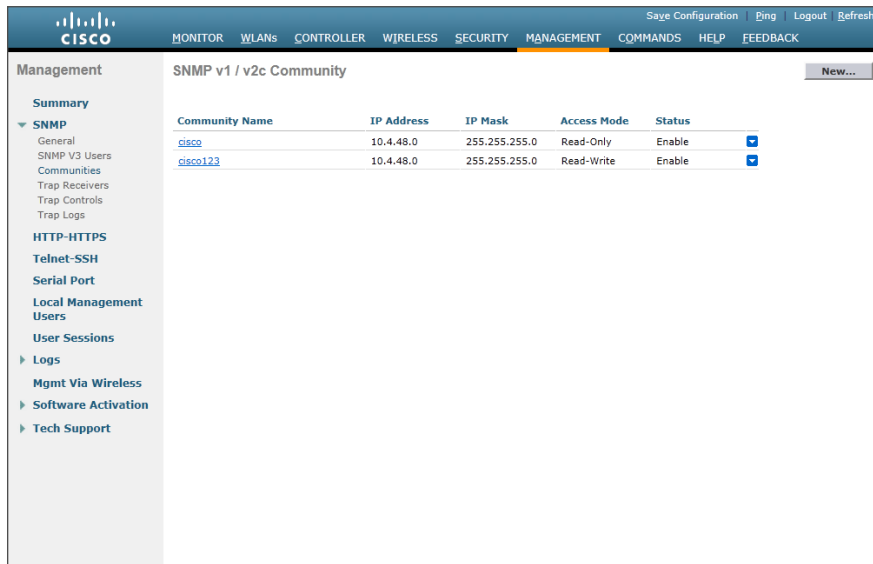
The screenshot shows the Cisco Management interface with the 'MANAGEMENT' tab selected. The left sidebar lists various configuration categories, including 'SNMP'. The main content area is titled 'SNMP v1 / v2c Community > New'. It contains a form with the following fields: 'Community Name' (cisco123), 'IP Address' (10.4.48.0), 'IP Mask' (255.255.255.0), 'Access Mode' (Read/Write), and 'Status' (Enable). There are '< Back' and 'Apply' buttons at the top right of the form.

Step 12: Navigate to **Management > SNMP > Communities**.

Step 13: Point to the blue box for the **public** community, and then click **Remove**.

Step 14: On the “Are you sure you want to delete?” message, click **OK**.

Step 15: Repeat Step 13 and Step 14 for the **private** community.



Procedure 5 Limit what networks can manage the WLC

(Optional)

In networks where network operational support is centralized, you can increase network security by using an access list to limit the networks that can access your controller. In this example, only devices on the 10.4.48.0/24 network will be able to access the controller via Secure Shell (SSH) Protocol or SNMP.

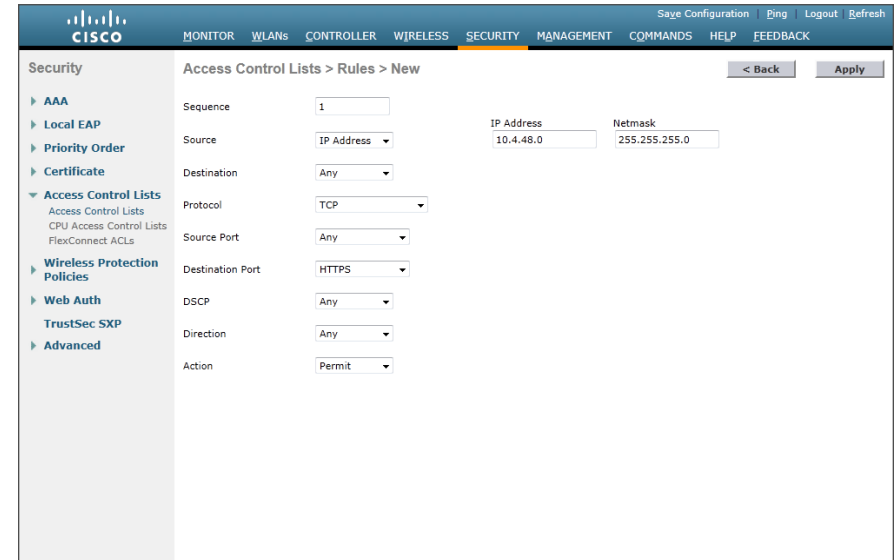
Step 1: In **Security > Access Control Lists > Access Control Lists**, click **New**.

Step 2: Enter an access list name, and then click **Apply**.

Step 3: In the list, choose the name of the access list you just created, and then click **Add New Rule**.

Step 4: In the window, enter the following configuration details, and then click **Apply**.

- Sequence—**1**
- Source—**10.4.48.0 / 255.255.255.0**
- Destination—**Any**
- Protocol—**TCP**
- Destination Port—**HTTPS**
- Action—**Permit**



Step 5: Repeat Step 3 through Step 4 four more times, using the configuration details in the following table.

Table 3 - Rule configuration values

Sequence	Source	Destination	Protocol	Destination port	Action
2	10.4.48.0/255.255.255.0	Any	TCP	Other/22	Permit
3	Any	Any	TCP	HTTPS	Deny
4	Any	Any	TCP	Other/22	Deny
5	Any	Any	Any	Any	Permit

Step 6: In **Security > Access Control Lists > CPU Access Control Lists**, select **Enable CPU ACL**.

Step 7: In the **ACL Name** list, choose the ACL you created in Step 2, and then click **Apply**.

Procedure 6 Configure wireless user authentication

Step 1: In **Security > AAA > Radius > Authentication**, click **New**.

Step 2: Enter the **Server IP Address**. (Example: 10.4.48.15)

Step 3: Enter and confirm the **Shared Secret**. (Example: SecretKey)

Step 4: To the right of **Management**, clear **Enable**, and then click **Apply**.

The screenshot shows the Cisco configuration interface for RADIUS Authentication Servers. The left sidebar lists the navigation menu: Security, AAA, RADIUS, Authentication, Accounting, Fallback, TACACS+, LDAP, Local Net Users, MAC Filtering, Disabled Clients, User Login Policies, AP Policies, Password Policies, Local EAP, Priority Order, Certificate, Access Control Lists, Wireless Protection Policies, Web Auth, TrustSec SXP, and Advanced. The main content area is titled "RADIUS Authentication Servers > New" and contains the following fields: Server Index (Priority) set to 1, Server IP Address set to 10.4.48.15, Shared Secret Format set to ASCII, Shared Secret and Confirm Shared Secret fields with masked text, Port Number set to 1812, Key Wrap checkbox (unchecked), Server Status set to Enabled, Support for RFC 3576 set to Enabled, Server Timeout set to 2 seconds, Network User checkbox (checked), Management checkbox (unchecked), and IPsec checkbox (unchecked). The "Apply" button is visible at the bottom right.

Step 5: In **Security > AAA > Radius > Accounting**, click **New**.

Step 6: Enter the **Server IP Address**. (Example: 10.4.48.15)

Step 7: Enter and confirm the **Shared Secret**, and then click **Apply**. (Example: SecretKey)

The screenshot shows the Cisco configuration interface for RADIUS Accounting Servers. The left sidebar lists the navigation menu: Security, AAA, RADIUS, Authentication, Accounting, Fallback, TACACS+, LDAP, Local Net Users, MAC Filtering, Disabled Clients, User Login Policies, AP Policies, Password Policies, Local EAP, Priority Order, Certificate, Access Control Lists, Wireless Protection Policies, Web Auth, TrustSec SXP, and Advanced. The main content area is titled "RADIUS Accounting Servers > New" and contains the following fields: Server Index (Priority) set to 1, Server IP Address set to 10.4.48.15, Shared Secret Format set to ASCII, Shared Secret and Confirm Shared Secret fields with masked text, Port Number set to 1813, Server Status set to Enabled, Server Timeout set to 2 seconds, Network User checkbox (checked), and IPsec checkbox (unchecked). The "Apply" button is visible at the bottom right.

Procedure 7 Centralize management authentication

(Optional)

You can use this procedure to deploy centralized management authentication by configuring the authentication, authorization, and accounting (AAA) service. If you prefer to use local management authentication, skip this procedure.

As networks scale in the number of devices to maintain, the operational burden to maintain local management accounts on every device also scales. A centralized AAA service reduces operational tasks per device and provides an audit log of user access for security compliance and root-cause analysis. When AAA is enabled for access control, all management access to the network infrastructure devices (SSH and HTTPS) is controlled by AAA.

Step 1: In **Security > AAA > TACACS+ > Authentication**, click **New**.

Step 2: Enter the **Server IP Address**. (Example: 10.4.48.15)

Step 3: Enter and confirm the **Shared Secret**, and then click **Apply**.
(Example: SecretKey)

The screenshot shows the Cisco IOS Security Configuration page for TACACS+ Authentication Servers. The left sidebar shows the navigation tree with 'TACACS+' expanded. The main content area is titled 'TACACS+ Authentication Servers > New'. It contains the following fields: 'Server Index (Priority)' set to 1, 'Server IP Address' set to 10.4.48.15, 'Shared Secret Format' set to ASCII, 'Shared Secret' and 'Confirm Shared Secret' both masked with asterisks, 'Port Number' set to 49, 'Server Status' set to Enabled, and 'Server Timeout' set to 5 seconds. There are '< Back' and 'Apply' buttons at the top right.

Step 4: In **Security > AAA > TACACS+ > Accounting**, click **New**.

Step 5: Enter the **Server IP Address**. (Example: 10.4.48.15)

Step 6: Enter and confirm the **Shared Secret**, and then click **Apply**.
(Example: SecretKey)

The screenshot shows the Cisco IOS Security Configuration page for TACACS+ Accounting Servers. The left sidebar shows the navigation tree with 'TACACS+' expanded. The main content area is titled 'TACACS+ Accounting Servers > New'. It contains the following fields: 'Server Index (Priority)' set to 1, 'Server IP Address' set to 10.4.48.15, 'Shared Secret Format' set to ASCII, 'Shared Secret' and 'Confirm Shared Secret' both masked with asterisks, 'Port Number' set to 49, 'Server Status' set to Enabled, and 'Server Timeout' set to 5 seconds. There are '< Back' and 'Apply' buttons at the top right.

Step 7: In **Security > AAA > TACACS+ > Authorization**, click **New**.

Step 8: Enter the **Server IP Address**. (Example: 10.4.48.15)

Step 9: Enter and confirm the **Shared Secret**, and then click **Apply**.
(Example: SecretKey)

The screenshot shows the Cisco IOS Security Configuration page for TACACS+ Authorization Servers. The left sidebar lists various security options, with TACACS+ selected. The main area is titled 'TACACS+ Authorization Servers > New'. It contains fields for: Server Index (Priority) set to 1, Server IP Address set to 10.4.48.15, Shared Secret Format set to ASCII, Shared Secret and Confirm Shared Secret both masked with dots, Port Number set to 49, Server Status set to Enabled, and Server Timeout set to 5 seconds. There are '< Back' and 'Apply' buttons at the top right.

Step 10: Navigate to **Security > Priority Order > Management User**.

Step 11: Using the arrow buttons, move **TACACS+** from the **Not Used** list to the **Used for Authentication** list.

Step 12: Using the **Up** and **Down** buttons, move **TACACS+** to be the first in the **Order Used for Authentication** list.

Step 13: Using the arrow buttons, move **RADIUS** to the **Not Used** list, and then click **Apply**.

The screenshot shows the Cisco IOS Security Configuration page for Priority Order > Management User. The left sidebar lists various security options, with Priority Order selected. The main area is titled 'Priority Order > Management User'. It contains two lists: 'Not Used' and 'Order Used for Authentication'. The 'Not Used' list contains RADIUS. The 'Order Used for Authentication' list contains TACACS+ and LOCAL. There are arrow buttons between the lists and Up/Down buttons for the 'Order Used for Authentication' list. A note at the bottom states: 'If LOCAL is selected as second priority then user will be authenticated against LOCAL only if first priority is unreachable.' There is an 'Apply' button at the top right.

Process

Configuring Voice/Data Connectivity

1. Create the wireless LAN data interface
2. Create the wireless LAN voice interface
3. Create the remote LAN interface
4. Configure the data wireless LAN
5. Configure voice wireless LAN
6. Configure the remote LAN

The Cisco OfficeExtend Access Point supports a maximum of two wireless LANs and one remote LAN. Configure the SSIDs to separate voice and data traffic, which is essential in any good network design in order to ensure proper treatment of the respective IP traffic, regardless of the medium it is traversing. In this procedure, you add an interface that allows devices on the wireless data network to communicate with the rest of your organization.

Procedure 1 Create the wireless LAN data interface

Step 1: In **Controller>Interfaces**, click **New**.

Step 2: Enter the **Interface Name**. (Example: Wireless-Data)

Step 3: Enter the **VLAN Id**, and then click **Apply**. (Example: 244)

The screenshot shows the Cisco OfficeExtend Controller web interface. The top navigation bar includes links for MONITOR, WLANs, CONTROLLER (selected), WIRELESS, SECURITY, MANAGEMENT, COMMANDS, HELP, and FEEDBACK. The left sidebar lists various configuration categories: General, Inventory, Interfaces (selected), Interface Groups, Multicast, Network Routes, Internal DHCP Server, Mobility Management, Ports, NTP, CDP, and Advanced. The main content area is titled 'Interfaces > New' and contains two input fields: 'Interface Name' with the value 'Wireless-Data' and 'VLAN Id' with the value '244'. At the top right of the main area are links for 'Save Configuration', 'Ping', 'Logout', and 'Refresh'. At the bottom right are '< Back' and 'Apply' buttons.

Step 4: In the **Port Number** box, enter the WLC interface that connects to the LAN distribution switch. (Example: 2)

Step 5: In the **IP Address** box, enter the IP address to assign to the WLC interface. (Example: 10.4.144.5)

Step 6: Enter the **Netmask**. (Example: 255.255.252.0)

Step 7: In the **Gateway** box, enter the IP address of the VLAN interface defined in Configuring LAN Distribution Switch, Procedure 1, "Configure the distribution switch," Step 2. (Example: 10.4.144.1)

Step 8: In the **Primary DHCP Server** box, enter the IP address of your organization's DHCP server, and then click **Apply**. (Example: 10.4.48.10)

The screenshot shows the Cisco Controller configuration page for a new interface. The left sidebar contains a navigation menu with options: General, Inventory, Interfaces, Interface Groups, Multicast, Network Routes, Internal DHCP Server, Mobility Management, Ports, NTP, CDP, and Advanced. The main content area is titled 'Interfaces > Edit' and includes a '< Back' button and an 'Apply' button. The configuration is organized into several sections: General Information (Interface Name: Wireless-Voice, MAC Address: d0:d0:fd:1f:59:e0), Configuration (Guest Lan, Quarantine, Quarantine Vlan Id), Physical Information (Port Number: 2, Backup Port: 0, Active Port: 0, Enable Dynamic AP Management), Interface Address (VLAN Identifier: 244, IP Address: 10.4.144.5, Netmask: 255.255.252.0, Gateway: 10.4.144.1), DHCP Information (Primary DHCP Server: 10.4.48.10, Secondary DHCP Server), and Access Control List (ACL Name: none). A note at the bottom states: '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: Enter the **VLAN Id**, and then click **Apply**. (Example: 248)

The screenshot shows the Cisco Controller configuration page for a new interface. The left sidebar contains a navigation menu with options: General, Inventory, Interfaces, Interface Groups, Multicast, Network Routes, Internal DHCP Server, Mobility Management, Ports, NTP, CDP, and Advanced. The main content area is titled 'Interfaces > New' and includes a '< Back' button and an 'Apply' button. The configuration is organized into several sections: General Information (Interface Name: Wireless-Voice, VLAN Id: 248), Configuration, Physical Information, Interface Address, DHCP Information, and Access Control List.

Step 4: In the **Port Number** box, enter the WLC interface that connects to the LAN distribution switch. (Example: 2)

Step 5: In the **IP Address** box, enter the IP address to assign to the WLC interface. (Example: 10.4.148.5)

Step 6: Enter the **Netmask**. (Example: 255.255.252.0)

Step 7: In the **Gateway** box, enter the IP address of the VLAN interface defined in Configuring LAN Distribution Switch, Procedure 1, "Configure the distribution switch," Step 2. (Example: 10.4.148.1)

Procedure 2 Create the wireless LAN voice interface

You must add an interface that allows devices on the wireless voice network to communicate with the rest of the organization.

Step 1: In **Controller>Interfaces**, click **New**.

Step 2: Enter the **Interface Name**. (Example: Wireless-Voice)

Step 8: In the **Primary DHCP Server** box, enter the IP address of your organization's DHCP server, and then click **Apply**. (Example: 10.4.48.10)

Step 3: Enter the **VLAN Id**, and then click **Apply**. (Example: 252)

Step 4: In the **Port Number** box, enter the WLC interface that connects to the LAN distribution switch. (Example: 2)

Step 5: In the **IP Address** box, enter the IP address to assign to the WLC interface. (Example: 10.4.152.5)

Step 6: Enter the **Netmask**. (Example: 255.255.252.0)

Step 7: In the **Gateway** box, enter the IP address of the VLAN interface defined in Configuring LAN Distribution Switch, Procedure 1, "Configure the distribution switch," Step 2. (Example: 10.4.152.1)

Procedure 3 Create the remote LAN interface

Next, you add an interface that allows devices on the remote LAN network to communicate with the rest of the organization.

Step 1: In **Controller>Interfaces**, click **New**.

Step 2: Enter the **Interface Name**. (Example: Remote-LAN)

Step 8: In the **Primary DHCP Server** box, enter the IP address of your organization's DHCP server, and then click **Apply**. (Example: 10.4.48.10)

Procedure 4 Configure the data wireless LAN

Wireless data traffic is different from voice traffic in that it can more efficiently handle delay and jitter as well as greater packet loss. For the data wireless LAN, keep the default QoS settings and segment the data traffic onto the data wired VLAN.

Step 1: Navigate to **WLANs**.

Step 2: Click the **WLAN ID** of the SSID created during platform setup.

Step 3: On the **General** tab, in the **Interface** list, choose the interface created in Procedure 1. (Example: Wireless-Data)

Step 4: On the Advanced tab, clear **Coverage Hole Detection**.

Step 5: Clear **Aironet IE**, and then click **Apply**.

The screenshot shows the 'WLANs > Edit 'WLAN-Data'' configuration page. The 'Advanced' tab is selected. The 'General' section has 'Allow AAA Override' and 'Coverage Hole Detection' disabled, 'Enable Session Timeout' checked with a value of 1800, 'Aironet IE' disabled, 'Diagnostic Channel' disabled, 'IPv6 Enable' checked, 'Override Interface ACL' set to 'None', 'P2P Blocking Action' set to 'Disabled', 'Client Exclusion' checked with a 'Timeout Value (secs)' of 60, 'Maximum Allowed Clients' set to 0, and 'Static IP Tunneling' disabled. The 'DHCP' section has 'DHCP Server' disabled and 'DHCP Addr. Assignment' set to 'Required'. The 'Management Frame Protection (MFP)' section has 'MFP Client Protection' set to 'Optional'. The 'DTIM Period (in beacon intervals)' section has '802.11a/n (1 - 255)' and '802.11b/g/n (1 - 255)' both set to 1. The 'NAC' section has 'NAC State' set to 'None'. The 'Load Balancing and Band Select' section has 'Client Load Balancing' and 'Client Band Select' both disabled. The 'Off Channel Scanning Defer' section has 'Scan Defer Priority' set to 0. The 'Foot Notes' section contains 13 numbered notes.

Step 2: In the drop-down list, choose **Create New**, and then click **Go**.

The screenshot shows the 'WLANs' configuration page. The 'WLANs' tab is selected. The 'WLANs' list shows one entry with ID 1, Type 'WLAN', Profile Name 'WLAN-Data', WLAN SSID 'WLAN-Data', Admin Status 'Enabled', and Security Policies '[WPA2][Auth(802.1X)]'. The 'Create New' button is visible.

Step 3: Enter the **Profile Name**. (Example: Voice)

Step 4: In the **SSID** box, enter the voice WLAN name, and then click **Apply**. (Example: WLAN-Voice)

The screenshot shows the 'WLANs > New' configuration page. The 'Type' is set to 'WLAN', the 'Profile Name' is 'Voice', the 'SSID' is 'WLAN-Voice', and the 'ID' is set to 2. The 'Apply' button is visible.

Procedure 5 Configure voice wireless LAN

Wireless voice traffic is different from data traffic in that it cannot effectively handle delay and jitter as well as packet loss. To configure the voice wireless LAN, change the default QoS settings to Platinum and segment the voice traffic onto the voice wired VLAN.

Step 1: Navigate to **WLANs**.

Step 5: On the General tab, to the right of **Status**, select **Enabled**.

Step 6: In the **Interface** list, choose the interface created in Procedure 2.
(Example: Wireless-Voice)

The screenshot shows the Cisco WLAN configuration page for a profile named 'Voice'. The 'General' tab is selected. The 'Status' is set to 'Enabled'. The 'Interface/Interface Group' is set to 'wireless-voice'. The 'Security Policies' are set to '[WPA2][Auth(802.1X)]'. The 'Radio Policy' is set to 'All'. The 'Multicast VLAN Feature' is set to 'Enabled'. The 'Broadcast SSID' is set to 'Enabled'. The 'Foot Notes' section at the bottom contains 13 numbered notes regarding configuration restrictions and warnings.

WLANs > Edit 'Voice'

General Security QoS Advanced

Profile Name: Voice
Type: WLAN
SSID: WLAN-Voice
Status: ☒ Enabled

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

Radio Policy: All
Interface/Interface Group(G): wireless-voice
Multicast VLAN Feature: ☐ Enabled
Broadcast SSID: ☒ Enabled

Foot Notes

- 1 Web Policy cannot be used in combination with IPsec
- 2 H-REAP Local Switching is not supported with IPsec, CRANITE authentication
- 3 When client exclusion is enabled, a Timeout Value of zero means infinity (will require administrative override to reset excluded clients)
- 4 Client MFP is not active unless WPA2 is configured
- 5 Learn Client IP is configurable only when HREAP Local Switching is enabled
- 6 WMM and open or AES security should be enabled to support higher 11n rates
- 7 Multicast Should Be Enabled For IPv6.
- 8 Band Select is configurable only when Radio Policy is set to 'All'.
- 9 Value zero implies there is no restriction on maximum clients allowed.
- 10 MAC Filtering is not supported with HREAP Local authentication
- 11 MAC Filtering should be enabled.
- 12 Guest tunneling, Local switching, DHCP Required should be disabled.
- 13 Max-associated-clients feature is not supported with HREAP Local Authentication.

Step 7: Click the **QoS** tab, and in the **Quality of Service (QoS)** list, choose **Platinum**.

The screenshot shows the Cisco WLAN configuration page for a profile named 'Voice'. The 'QoS' tab is selected. The 'Quality of Service (QoS)' is set to 'Platinum (voice)'. The 'WMM' section shows 'WMM Policy' set to 'Allowed', '7920 AP CAC' set to 'Enabled', and '7920 Client CAC' set to 'Enabled'. The 'Foot Notes' section at the bottom contains 13 numbered notes regarding configuration restrictions and warnings.

WLANs > Edit 'Voice'

General Security QoS Advanced

Quality of Service (QoS): Platinum (voice)

WMM

WMM Policy: Allowed
7920 AP CAC: ☐ Enabled
7920 Client CAC: ☐ Enabled

Foot Notes

- 1 Web Policy cannot be used in combination with IPsec
- 2 H-REAP Local Switching is not supported with IPsec, CRANITE authentication
- 3 When client exclusion is enabled, a Timeout Value of zero means infinity (will require administrative override to reset excluded clients)
- 4 Client MFP is not active unless WPA2 is configured
- 5 Learn Client IP is configurable only when HREAP Local Switching is enabled
- 6 WMM and open or AES security should be enabled to support higher 11n rates
- 7 Multicast Should Be Enabled For IPv6.
- 8 Band Select is configurable only when Radio Policy is set to 'All'.
- 9 Value zero implies there is no restriction on maximum clients allowed.
- 10 MAC Filtering is not supported with HREAP Local authentication
- 11 MAC Filtering should be enabled.
- 12 Guest tunneling, Local switching, DHCP Required should be disabled.
- 13 Max-associated-clients feature is not supported with HREAP Local Authentication.

Step 8: Click the **Advanced** tab, and then clear **Coverage Hole Detection**.

Step 9: Clear **Aironet IE**, and then click **Apply**.

The screenshot shows the 'WLANs > Edit 'Voice'' configuration page in the Cisco Prime interface. The 'Advanced' tab is selected. The 'General' section has 'Allow AAA Override' and 'Coverage Hole Detection' checked, 'Enable Session Timeout' set to 1800, 'Aironet IE' checked, 'Diagnostic Channel' checked, 'IPv6 Enable' checked, 'Override Interface ACL' set to 'None', 'P2P Blocking Action' set to 'Disabled', 'Client Exclusion' checked, 'Maximum Allowed Clients' set to 0, and 'Static IP Tunneling' checked. The 'QoS' section has 'DHCP' and 'DHCP Server' checked, 'DHCP Addr. Assignment' set to 'Required', 'Management Frame Protection (MFP)' set to 'Optional', and 'DTIM Period (in beacon intervals)' set to 1. The 'Foot Notes' section at the bottom contains 13 numbered notes.

Step 2: In the drop-down list, choose **Create New**, and then click **Go**.

The screenshot shows the 'WLANs' configuration page in the Cisco Prime interface. The 'WLANs' tab is selected. The 'WLANs' list shows two entries: '1' and '2'. Entry '1' is a 'WLAN' with 'Profile Name' 'WLAN-Data' and 'WLAN SSID' 'WLAN-Data'. Entry '2' is a 'WLAN' with 'Profile Name' 'Voice' and 'WLAN SSID' 'WLAN-Voice'. The 'Admin Status' is 'Enabled' for both, and the 'Security Policies' are '[WPA2][Auth(802.1X)]'.

Step 3: In the **Type** list, choose **Remote LAN**.

Step 4: Enter the **Profile Name**, and then click **Apply**. (Example: LAN)

The screenshot shows the 'WLANs > New' configuration page in the Cisco Prime interface. The 'Type' is set to 'Remote LAN', the 'Profile Name' is 'LAN', and the 'ID' is '3'. The 'Apply' button is visible.

Procedure 6 Configure the remote LAN

A remote LAN is similar to a WLAN except it is mapped to one of the Ethernet ports on the back of the Cisco OfficeExtend Access Point.

Step 1: Navigate to **WLANs**.

Step 5: On the General tab, to the right of **Status**, select **Enabled**.

Step 6: In the **Interface** list, choose the interface created in Procedure 3. (Example: Remote-LAN)

The screenshot shows the Cisco Secure ACS configuration page for a WLAN named 'LAN'. The 'General' tab is selected, displaying the following configuration:

Field	Value
Profile Name	LAN
Type	Remote LAN
SSID	LAN
Status	<input checked="" type="checkbox"/> Enabled
Egress Interface	remote-lan

Foot Notes:
3 When client exclusion is enabled, a Timeout Value of zero means infinity (will require administrative override to reset excluded clients)
9 Value zero implies there is no restriction on maximum clients allowed.

Step 7: Click the **Security** tab.

Step 8: On the Layer 2 tab, clear **MAC Filtering**, and then click **Apply**.

The screenshot shows the Cisco Secure ACS configuration page for a WLAN named 'LAN'. The 'Security' tab is selected, displaying the 'Layer 2' sub-tab. The 'MAC Filtering' checkbox is unchecked.

Foot Notes:
3 When client exclusion is enabled, a Timeout Value of zero means infinity (will require administrative override to reset excluded clients)
9 Value zero implies there is no restriction on maximum clients allowed.

Process

Configuring AP Authentication

1. Enable the default network device
2. Configure the access point account
3. Configure AP authentication in the WLC

Access point authentication ensures only authorized access points can connect to the controller.

If you want to control which access points can connect to the Cisco OfficeExtend controller, follow this process.

If you want to allow any access point to connect to the Cisco OfficeExtend controller, skip to the next process.

Cisco Secure ACS is used to store the list of access points authorized by the organization. Storing the list in Secure ACS eases the operational burden of keeping authorization lists on all the controllers in sync.

Procedure 1

Enable the default network device

Access point authentication is kept separate from user authentication by the use of access services in Cisco Secure ACS. The separation is important for security in order to ensure users do not use the well-known username and password format to gain access to the wireless network. Since access point authentication does not match the selection rule defined for wireless user authentication, an additional RADIUS access service must be enabled.

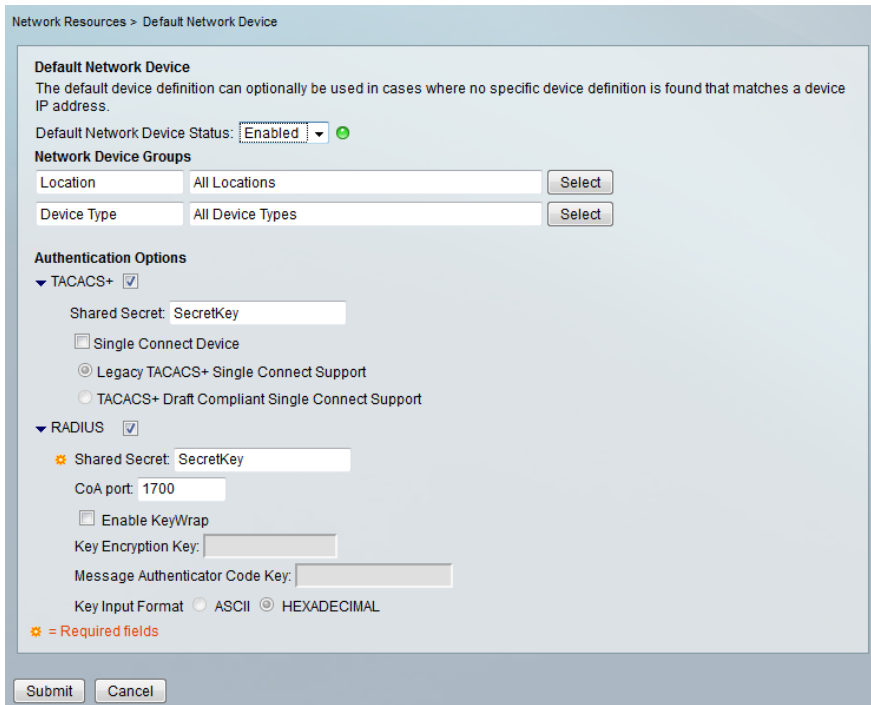
Step 1: Navigate to the Cisco Secure ACS Administration page. (Example: <https://acs.cisco.local>)

Step 2: Navigate to **Network Resources > Default Network Device**.

Step 3: In the **Default Network Device Status** list, choose **Enabled**.

Step 4: Select **RADIUS**.

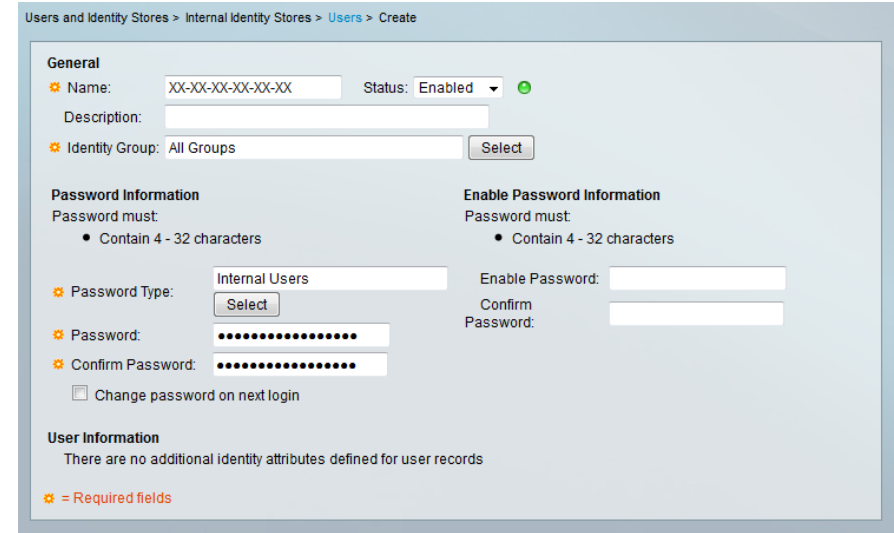
Step 5: Enter the RADIUS shared secret key, and then click **Submit**.
(Example SecretKey)



Step 3: In the **Name** box, enter the MAC address of the access point.
(Example: XX-XX-XX-XX-XX-XX)

Step 4: Enter and confirm a password.

Step 5: Click **Submit**. This applies the changes.



Procedure 2 Configure the access point account

Each access point is created as a user in the internal identity store of Cisco Secure ACS, and the username is set to the access point's MAC address. The password should also be set to the access point's MAC address, but because Secure ACS uses host lookup in order to authenticate the RADIUS request, it is not checked and can be set to anything you prefer. The access point's MAC address can be found on a label on the outside of the product packaging and on a label on the bottom of the access point.

Step 1: In Cisco Secure ACS, navigate to **Users and Identity Stores > Internal Identity Stores > Users**.

Step 2: Click **Create**.

Procedure 3 Configure AP authentication in the WLC

Step 1: Navigate to **Security > AAA > AP Policies**.

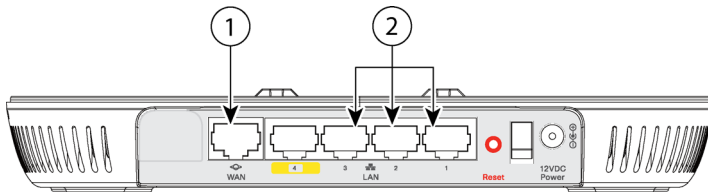
Step 2: Under Policy Configuration, select **Authorize MIC APs** against **auth-list** or **AAA**, and then click **Apply**.

Process

Configuring Cisco OfficeExtend AP

1. Configure the Cisco OfficeExtend AP

Procedure 1 Configure the Cisco OfficeExtend AP



Step 1: Connect the WAN port on the back of the Cisco OfficeExtend Access Point to your home router/gateway. The Cisco OfficeExtend Access Point gets an IP address from the home router/gateway.



Tech Tip

The Cisco OfficeExtend Access Point is not designed to replace the functionality of a home router, and it should not be connected directly to the service provider gateway.

Step 2: After the Cisco OfficeExtend Access Point has started, connect a computer to Ethernet port 1, 2, or 3. The computer gets an IP address from the default DHCP address pool of 10.0.0.0/24.

Step 3: Navigate to the Cisco OfficeExtend Access Point by using its default IP address: <http://10.0.0.1/>

Step 4: Log in to the Administration page by using the default credentials **admin/admin**.

Step 5: On the Cisco OfficeExtend Access Point Welcome page, click **Enter**. The Summary page appears.

Home: Summary					
General Information					
Ap Name	APE05F.B9DC.FC30				
AP IP Address	192.168.1.100				
AP Mode	Local				
AP MAC Address	E0:5F:B9:DC:FC:30				
AP Uptime	1 minutes, 28 seconds				
AP Software Version	7.0.112.53				
AP Statistics					
Radio	Admin Status	Freq/Chan	Tx Power	Pkts In/Out	Bytes In/Out
Radio-802.11G	up	2.4 GHz/6	18.50dBm	0/0	0/0
Radio-802.11A	up	5 GHz/36	12.50dBm	0/0	0/0
Association					
Client MAC	Association Time	Bytes In/Out	Duplicate/Retries	Decrypt Failed	
To edit 'Personal SSID' association and settings, click on Configuration					
©2010 Cisco Systems Inc. All rights reserved.					

Step 6: Navigate to **Configuration > WAN**.

Step 7: In the **Primary Controller IP Address** box, enter the outside IP address of the primary WLC, and then click **Apply**. (Example: 172.16.130.20)

The screenshot shows the 'Configuration' page with the 'WAN' tab selected. Under 'Primary Controller', the 'IP Address' is set to 172.16.130.20. Under 'Uplink IP Configuration', the 'Static IP' checkbox is checked, and the 'Domain Name' is set to cisco.com. Other fields include IP Address (192.168.1.100), Subnet Mask (255.255.255.0), Default Gateway (192.168.1.1), and DNS Server (171.68.226.120). An 'Apply' button is at the top right.

Step 8: On the verification screen that appears, click **Continue**.

The Cisco OfficeExtend Access Point connects to the controller and downloads the current software image. Allow 5 minutes for the device to download and reboot with the new code and configuration.



Tech Tip

After the access point makes a connection to the WLC, the Status LED on the top of the access point flashes. The Status LED continues flashing until the download is complete. When the download is complete, your access point restarts. After the access point connects to the controller again, the Status LED is displayed as solid blue or purple.

Process

Enabling AP Radios

1. Configure the WLC

After a new Cisco OfficeExtend Access Point joins the controller, the radios are automatically disabled. Before clients can use the access point, you must enable the 5-GHz and 2.4 GHz radios.

Procedure 1

Configure the WLC

First, enable the 5-GHz radio.

Step 1: On the primary WLC, navigate to **Wireless > Access Points > Radios > 802.11a/n**.

Access points that have their radios disabled have an Admin Status of Disable and an Operational Status of DOWN.

Step 2: Point to the blue box for the Cisco OfficeExtend Access Point that you want to enable, and then click **Configure**.

The screenshot shows the 'Wireless' configuration page with the '802.11a/n Radios' tab selected. A table lists three radios with their respective configurations. The third radio, APECC8.8266.2858, has its Admin Status set to 'Disable' and Operational Status set to 'DOWN', both highlighted with red boxes. A blue box with a 'C' icon is visible in the bottom right corner of the table.

AP Name	Radio Slot	Base Radio MAC	Sub Band	Admin Status	Operational Status	Channel	CleanAir Admin Status	CleanAir Oper Status	Radio Role	Power Level	Antenna
AP000.f045.4ae1	1	d0:57:4c:09:c0:80	-	Enable	UP	157 *	NA	NA	N/A	1 *	External
AP000.f0db.b85c	1	58:bc:27:0e:1c:80	-	Enable	UP	64 *	NA	NA	N/A	6 *	Internal
AP442b.039a.9c3a	1	3c:0e:73:1b:43:50	-	Enable	UP	161 *	Enable	DOWN	N/A	1 *	Internal
APECC8.8266.2858	1	ec:db:82:c0:ad:30	-	Disable	DOWN	36 *	NA	NA	N/A	1 *	Internal

Step 3: Under General, in the **Admin Status** list, choose **Enable**, and then click **Apply**.

The screenshot shows the Cisco WLC configuration interface. The left sidebar lists various configuration categories like Access Points, Radios, and Advanced. The main content area is titled '802.11a/n Cisco APs > Configure'. It has tabs for General, RF Channel Assignment, 11n Parameters, and Tx Power Level Assignment. In the General tab, the 'Admin Status' is set to 'Enable' (highlighted with a red box). Other settings include AP Name (APEC8.8288.2858), Operational Status (DOWN), Slot # (1), and 11n Supported (Yes).

Next, enable the 2.4-GHz radio.

Step 4: Navigate to **Wireless > Access Points > Radios > 802.11b/g/n**.

Step 5: Point to the blue box for the Cisco OfficeExtend Access Point that you want to enable, and then click **Configure**.

Step 6: Under General, in the **Admin Status** list, choose **Enable**, and then click **Apply**.

Process

Configuring WLC Resiliency

1. Configure the resilient WLC
2. Configure APs for resiliency

This design uses two WLCs. The first is the primary controller, and in the previous process, you configured all of the Cisco OfficeExtend Access Points to register to it.

The secondary controller, also called the *resilient controller*, provides resiliency in case the primary controller or Internet connection fails. Under

normal operation, there will not be any Cisco OfficeExtend Access Points registered to the resilient controller.

Procedure 1

Configure the resilient WLC

On the resilient WLC, repeat the procedures in the “Configuring WLC” process.

Procedure 2


Configure APs for resiliency

Step 1: On the primary WLC, navigate to **Wireless**, and then select the desired Cisco OfficeExtend Access Point.

Step 2: Click the **High Availability** tab.

Step 3: In the **Primary Controller** box, enter the name and management IP address of the primary WLC. (Example: WLC-OEAP-1 / 172.16.130.20)

Step 4: In the **Secondary Controller** box, enter the name and management IP address of the resilient WLC, and then click **Apply**. (Example: WLC-OEAP-2 / 172.17.130.20)



[MONITOR](#)
[WLANS](#)
[CONTROLLER](#)
[WIRELESS](#)
[SECURITY](#)
[MANAGEMENT](#)
[COMMANDS](#)
[HELP](#)
[FEEDBACK](#)

[Save Configuration](#)
[Ping](#)
[Logout](#)
[Refresh](#)

Wireless

Access Points

All APs

Radios

802.11a/n

802.11b/g/n

Global Configuration

Advanced

Mesh

HREAP Groups

802.11a/n

802.11b/g/n

Media Stream

Country

Timers

QoS

All APs > Details for APE05F.B9DC.FC30

< Back

Apply

General

Interfaces

High Availability

Inventory

Advanced

	Name	Management IP Address
Primary Controller	WLC-OEAP-1	172.16.130.20
Secondary Controller	WLC-OEAP-2	172.17.130.20
Tertiary Controller		

AP Failover Priority

Low

Foot Notes

1 DNS server IP Address and the Domain name can be set only after a valid static IP is pushed to the AP.

Notes

Appendix A: Product List

Wireless LAN OfficeExtend Access Points

Functional Area	Product Description	Part Numbers	Software
Teleworker AP	Cisco Aironet 600 OfficeExtend Series Access Point: Dual-band Controller-based 802.11a/g/n	AIR-OEAP602I-x-K9	7.4.100.0

Wireless LAN Controllers

Functional Area	Product Description	Part Numbers	Software
OfficeExtend Controller	Cisco 5500 Series Wireless Controller for up to 500 Cisco access points	AIR-CT5508-500-K9	7.4.100.0
	Cisco 5500 Series Wireless Controller for up to 250 Cisco access points	AIR-CT5508-250-K9	
	Cisco 5500 Series Wireless Controller for up to 100 Cisco access points	AIR-CT5508-100-K9	
	Cisco 5500 Series Wireless Controller for up to 50 Cisco access points	AIR-CT5508-50-K9	
	Cisco 5500 Series Wireless Controller for up to 25 Cisco access points	AIR-CT5508-25-K9	
	Cisco 5500 Series Wireless Controller for up to 12 Cisco access points	AIR-CT5508-12-K9	
	Cisco 2500 Series Wireless Controller for up to 50 Cisco access points	AIR-CT2504-50-K9	
	Cisco 2500 Series Wireless Controller for up to 25 Cisco access points	AIR-CT2504-25-K9	
	Cisco 2500 Series Wireless Controller for up to 15 Cisco access points	AIR-CT2504-15-K9	
	Cisco 2500 Series Wireless Controller for up to 5 Cisco access points	AIR-CT2504-5-K9	

Access Control

Functional Area	Product Description	Part Numbers	Software
Authentication Services	ACS 5.3 VMware Software and Base License	CSACS-5.3-VM-K9	5.3

Internet Edge

Functional Area	Product Description	Part Numbers	Software
Firewall	Cisco ASA 5545-X IPS Edition - security appliance	ASA5545-IPS-K9	ASA 9.0(1) IPS 7.1(6)E4
	Cisco ASA 5525-X IPS Edition - security appliance	ASA5525-IPS-K9	
	Cisco ASA 5515-X IPS Edition - security appliance	ASA5515-IPS-K9	
	Cisco ASA 5512-X IPS Edition - security appliance	ASA5512-IPS-K9	
	Cisco ASA5512-X Security Plus license	ASA5512-SEC-PL	
	Firewall Management	ASDM	7.0(2)

Internet Edge LAN

Functional Area	Product Description	Part Numbers	Software
DMZ Switch	Cisco Catalyst 3750-X Series Stackable 24 Ethernet 10/100/1000 ports	WS-C3750X-24T-S	15.0(2)SE IP Base license

LAN Distribution Layer

Functional Area	Product Description	Part Numbers	Software
Modular Distribution Layer Virtual Switch Pair	Cisco Catalyst 6500 E-Series 6-Slot Chassis	WS-C6506-E	15.0(1)SY1 IP Services license
	Cisco Catalyst 6500 VSS Supervisor 2T with 2 ports 10GbE and PFC4	VS-S2T-10G	
	Cisco Catalyst 6500 16-port 10GbE Fiber Module w/DFC4	WS-X6816-10G-2T	
	Cisco Catalyst 6500 24-port GbE SFP Fiber Module w/DFC4	WS-X6824-SFP-2T	
	Cisco Catalyst 6500 4-port 40GbE/16-port 10GbE Fiber Module w/DFC4	WS-X6904-40G-2T	
	Cisco Catalyst 6500 4-port 10GbE SFP+ adapter for WX-X6904-40G module	CVR-CFP-4SFP10G	
Modular Distribution Layer Switch	Cisco Catalyst 4507R+E 7-slot Chassis with 48Gbps per slot	WS-C4507R+E	3.3.0.SG(15.1-1SG) Enterprise Services license
	Cisco Catalyst 4500 E-Series Supervisor Engine 7-E, 848Gbps	WS-X45-SUP7-E	
	Cisco Catalyst 4500 E-Series 24-port GbE SFP Fiber Module	WS-X4624-SFP-E	
	Cisco Catalyst 4500 E-Series 12-port 10GbE SFP+ Fiber Module	WS-X4712-SFP+E	
Stackable Distribution Layer Switch	Cisco Catalyst 3750-X Series Stackable 12 GbE SFP ports	WS-C3750X-12S-E	15.0(2)SE IP Services license
	Cisco Catalyst 3750-X Series Two 10GbE SFP+ and Two GbE SFP ports network module	C3KX-NM-10G	
	Cisco Catalyst 3750-X Series Four GbE SFP ports network module	C3KX-NM-1G	

Appendix B: Changes

This appendix summarizes the changes to this guide since the previous Cisco SBA series.

- In previous releases of this document, we presented a second design model where both internal and Cisco OfficeExtend access points were joined on the same controller pair. Because Cisco OfficeExtend and high availability using AP SSO is not supported concurrently on a controller, we have removed that option in this release.
- We upgraded the Cisco ASA software to 9.0(1).
- We upgraded the Cisco Wireless Controller software to 7.4.
- We made minor changes to improve the readability of this guide.

Notes

Feedback

Please use the [feedback form](#) to send comments and suggestions about this guide.



SMART BUSINESS ARCHITECTURE



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.

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.

© 2013 Cisco Systems, Inc. All rights reserved.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)