



# Cisco OfficeExtend

## Technology Design Guide

August 2014 Series



# Table of Contents

---

<b>Preface</b> .....	<b>1</b>
<b>CVD Navigator</b> .....	<b>2</b>
Use Cases .....	2
Scope .....	2
Proficiency.....	2
<b>Introduction</b> .....	<b>3</b>
Technology Use Case .....	3
Use Case: Teleworker with Wireless Devices .....	3
Design Overview.....	3
Deployment Components.....	3
Design Models .....	4
<b>Deployment Details</b> .....	<b>6</b>
Configuring Cisco Secure ACS .....	7
Configuring Internet Edge.....	15
Configuring LAN Distribution Switch.....	25
Configuring WLC.....	27
Configuring Voice/Data WLAN Connectivity .....	40
Configuring AP Authentication.....	52
Configuring Cisco OfficeExtend AP.....	55
Enabling AP Radios .....	57
Configuring WLC Resiliency .....	59
Enable Fast SSID Change.....	61
<b>Appendix A: Product List</b> .....	<b>62</b>
<b>Appendix B: Changes</b> .....	<b>65</b>

# Preface

---

Cisco Validated Designs (CVDs) present systems that are based on common use cases or engineering priorities. CVDs incorporate a broad set of technologies, features, and applications that address customer needs. Cisco engineers have comprehensively tested and documented each design in order to ensure faster, more reliable, and fully predictable deployment.

CVDs include two guide types that provide tested design details:

- **Technology design guides** provide deployment details, information about validated products and software, and best practices for specific types of technology.
- **Solution design guides** integrate existing CVDs but also include product features and functionality across Cisco products and sometimes include information about third-party integration.

Both CVD types provide a tested starting point for Cisco partners or customers to begin designing and deploying systems.

## CVD Foundation Series

This CVD Foundation guide is a part of the *August 2014 Series*. As Cisco develops a CVD Foundation series, the guides themselves are tested together, in the same network lab. This approach assures that the guides in a series are fully compatible with one another. Each series describes a lab-validated, complete system.

The CVD Foundation series incorporates wired and wireless LAN, WAN, data center, security, and network management technologies. Using the CVD Foundation simplifies system integration, allowing you to select solutions that solve an organization's problems—without worrying about the technical complexity.

To ensure the compatibility of designs in the CVD Foundation, you should use guides that belong to the same release. For the most recent CVD Foundation guides, please visit [the CVD Foundation web site](#).

## Comments and Questions

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

# CVD Navigator

The CVD Navigator helps you determine the applicability of this guide by summarizing its key elements: the use cases, the scope or breadth of the technology covered, the proficiency or experience recommended, and CVDs related to this guide. This section is a quick reference only. For more details, see the Introduction.

## Use Cases

This guide addresses the following technology use cases:

- **Teleworker with Wireless Devices**—Teleworkers require always-on secure access to networked business services from the remote home office. Wireless access provides easy mobility and setup within the home office, and consistent device configuration allows for easy mobility between the home office and on site at the main location.

For more information, see the “Use Cases” section in this guide.

## Scope

This guide covers the following areas of technology and products:

- Remote-site teleworking using the Cisco Aironet 600 Series OfficeExtend Access Point
- OfficeExtend termination on Cisco 2500 Series or Cisco 5500 Series Wireless LAN Controllers

For more information, see the “Design Overview” section in this guide.

## Proficiency

This guide is for people with the following technical proficiencies—or equivalent experience:

- **CCNA Wireless**—1 to 3 years installing, operating, and troubleshooting wireless LANs

## Related CVD Guides



Campus Wireless LAN  
Technology Design Guide

To view the related CVD guides, click the titles or visit [the CVD Foundation web site](#).

# Introduction

---

## Technology Use Case

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.

### Use Case: Teleworker with Wireless Devices

Teleworkers require always-on secure access to networked business services from the remote home office. Wireless access provides easy mobility and setup within the home office, and consistent device configuration allows for easy mobility between the home office and on site at the main location.

This design guide enables the following network capabilities:

- Common wireless device configuration for onsite and teleworker wireless access
- Authentication through IEEE 802.1x for employees and encryption for all information sent and received to the organization's main location
- Simplified IT provisioning for the home office, which reduces setup time and supports varying levels of end-user skills
- Mobility and flexibility for voice endpoints at the teleworker location

## Design 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 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 guide.

- **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

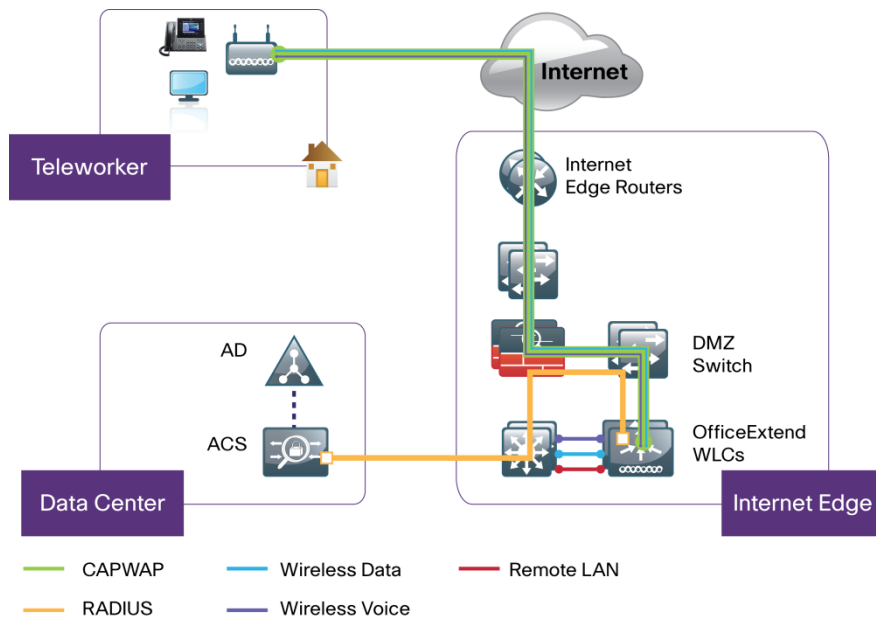
Cisco Aironet 600 Series OfficeExtend Access Points are lightweight. This means they cannot act independently of a wireless LAN controller (WLC). As the access point communicates with the WLC resources, it will download its configuration and synchronize its software/firmware image, if required. Cisco 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 option where both internal wireless users and remote OfficeExtend access points were registered to the same controller pair. Because Cisco OfficeExtend and high availability using stateful switchover (SSO) is not supported concurrently on a controller, we have removed that design option.

# Deployment Details

## How to Read Commands

This guide uses the following conventions for commands that you enter at the command-line interface (CLI).

Commands to enter at a CLI prompt:

```
configure terminal
```

Commands that specify a value for a variable:

```
ntp server 10.10.48.17
```

Commands with variables that you must define:

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

Commands at a CLI or script prompt:

```
Router# enable
```

Long commands that line wrap are underlined.

Enter them as one command:

```
police rate 10000 pps burst 10000  
packets conform-action
```

Noteworthy parts of system output (or of device configuration files) are highlighted:

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

This design 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	CVD 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	



## 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 WLAN 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 [Device Management Using ACS Design 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

\* = Required fields

### 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
-----------	-------------	-------

Manually Entered

Attribute	Requirement	Value
role1	Mandatory	All

Add A Edit V Replace A Delete

Attribute:

Requirement: Mandatory

Attribute Value: Static

\* = 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    **Select**

NDG:Location: -ANY-

NDG:Device Type: not in    All Device Types:WLC    **Select**

Time And Date: -ANY-

**Results**  
Shell Profile: Level 15    **Select**

**OK**    **Cancel**    **Help**

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.

The screenshot shows a configuration window for a policy named "WLC Admin". The "General" section shows the name "WLC Admin" and the status "Enabled" with a green checkmark. Below this is an information icon and a note: "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." The "Conditions" section has four items: "Identity Group" (checked, dropdown "in", "All Groups: Network Admins", "Select" button), "NDG: Location" (unchecked, "-ANY-"), "NDG: Device Type" (checked, dropdown "in", "All Device Types: WLC", "Select" button), and "Time And Date" (unchecked, "-ANY-"). The "Results" section has "Shell Profile" (dropdown "WLC Shell", "Select" button). At the bottom are "OK", "Cancel", and "Help" buttons.

## Procedure 4 Create the WLAN 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.

The screenshot shows the "Create" dialog for a policy. The breadcrumb is "Access Policies > Access Services > Create". The "General" tab is active. Under "Step 1 - General", the "Name" field contains "Wireless LAN" and the "Description" field is empty. The "Access Service Policy Structure" section has three radio buttons: "Based on service template" (selected), "Based on existing service", and "User Selected Service Type". The "Based on service template" option has a dropdown menu showing "Network Access - Simple" and a "Select" button. The "Based on existing service" option has an empty dropdown and a "Select" button. The "User Selected Service Type" option has a dropdown menu showing "Network Access". At the bottom are "Back", "Next", "Finish", and "Cancel" buttons.

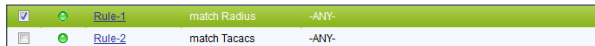
**Step 4:** On the Allowed Protocols pane, ensure **Allow PEAP** and **Allow EAP-Fast** are selected, and then click **Finish**.





**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.



		Rule-1	match Radius	-ANY-
		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 >  
Or >  
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. The ACS RADIUS server will check Active Directory (AD), followed by the ACS local database if not found in AD. Each of the Office Extend AP's will have an entry in the local ACS database based on their MAC address.

**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  
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**.

The screenshot shows the 'General' tab of a policy rule configuration window. The 'Name' field is 'WLC Access' and the 'Status' is 'Enabled'. A help icon and text explain that 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
- 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.

**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:   
Description:

**Network Device Groups**  
Location:    
Device Type:

**IP Address**  
 Single IP Address  IP Range(s) By Mask  IP Range(s)  
IP:

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

= Required fields



## Configuring Internet Edge

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

### Procedure 1 Configure the DMZ switch

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

```
vlan 1119
 name dmz-mgmt-wlan
```

**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 GigabitEthernet1/0/3
 description DMZ OEAP WLC-1 Management Port
 !
interface GigabitEthernet2/0/3
 description DMZ OEAP WLC-2 Management Port
 !
interface range GigabitEthernet 1/0/3, GigabitEthernet 2/0/3
 switchport access vlan 1119
 switchport host
 macro apply EgressQoS
 logging event link-status
 no shutdown
```

## Procedure 2 Configure the DMZ interface

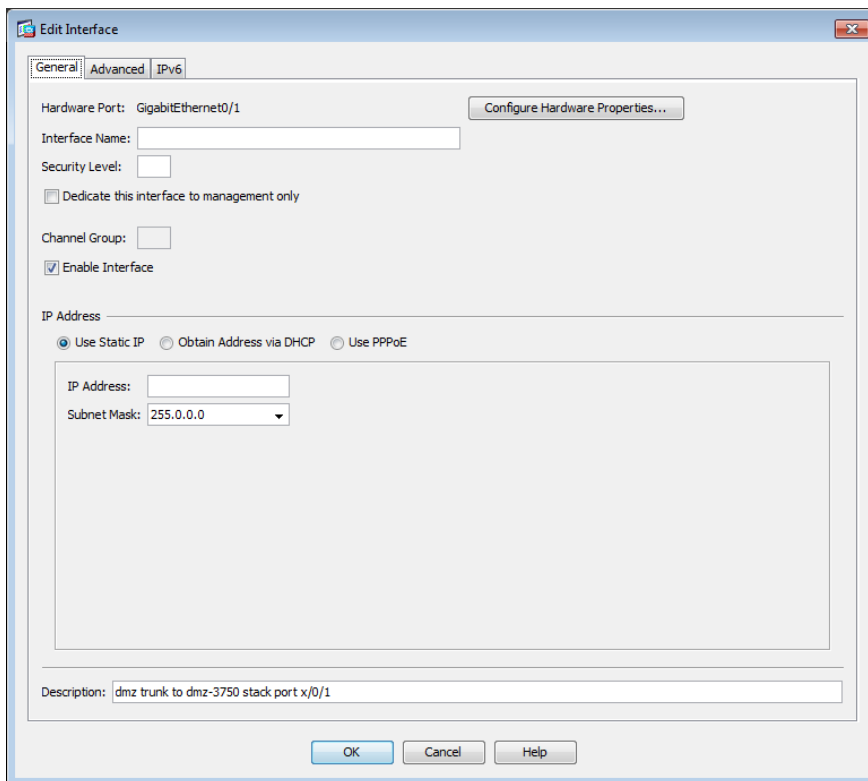
Typically, the firewall DMZ is a portion of the network where traffic to and from other parts of the network is tightly restricted. Organizations place network services in a DMZ for exposure to the Internet; these services are typically not allowed to initiate connections to the inside network, except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

**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)

The screenshot shows the 'Edit Interface' dialog box with the following configuration:

- Hardware Port: GigabitEthernet0/1.1119
- VLAN ID: 1119
- Subinterface ID: 1119
- Interface Name: dmz-mgmt-wlan
- Security Level: 50
- Dedicate this interface to management only
- Channel Group: (empty)
- Enable Interface
- IP Address: (radio buttons for Use Static IP, Obtain Address via DHCP, Use PPPoE)
- IP Address: 192.168.19.1
- Subnet Mask: 255.255.255.0
- Description: WLC DMZ Management Interface to DMZ Switch

### Procedure 3 Configure address translation

The DMZ network uses private network addressing (RFC 1918) 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-OEAP-1	dmz-wlc-OEAP-2
WLC public address	172.16.130.20	172.17.130.20
Outside object name	outside-wlc-ISPa	outside-wlc-ISPb

The use of objects and group objects in Cisco ASA make the configuration of the ASA appliance more easily understood. The following steps create a series of objects that represent the WLCs in your environment.



### Reader Tip

The numbers and type of Wireless LAN Controllers in your environment will vary. The list below is inclusive of the WLCs in the test environment used to produce this CVD.

Table 3 - OEAP and AAA network objects

Network object name	Object type	IP address
outside-wlc-ISPa	Host	172.16.130.20
outside-wlc-ISPb	Host	172.17.130.20
dmz-wlc-OEAP-1	Host	192.168.19.20
dmz-wlc-OEAP-2	Host	192.168.19.21
internal-aaa	Host	10.4.48.15

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

**Step 2:** Repeat Step 3 through Step 6 for all objects listed in Table 3. If the object already exists, then skip to the next object in the table.

**Step 3:** Click **Add > Network Object**.

The Add Network Object dialog box appears.

**Step 4:** In the **Name** box, enter a description of the WLC. (Examples: outside-wlc-ISPa)

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

**Step 6:** In the **IP Address** box, enter the WLC management interface IP address, and then click **OK**. (Example: 172.16.130.20)

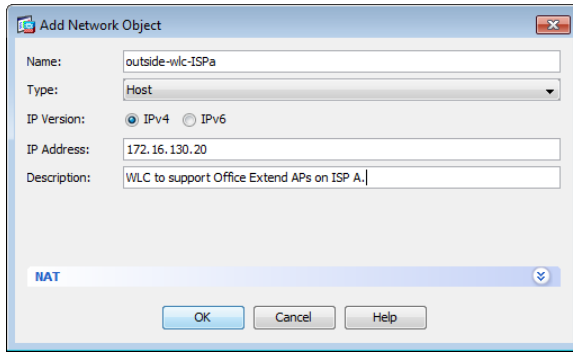


Table 4 - OEAP WLC network objects

Network object name	Object type	IP address	NAT Address	NAT Destination Interface
dmz-wlc-OEAP-1	Host	192.168.19.20	outside-wlc-ISPa	outside-16
dmz-wlc-OEAP-2	Host	192.168.19.21	outside-wlc-ISPb	outside-17

**Step 7:** Navigate to **Configuration > Firewall > Objects > Network Objects/Groups**.

**Step 8:** Repeat Step 9 through Step 17 for all objects listed in Table 4. If the object already exists, then skip to the next object in the table.

**Step 9:** Click **Add > Network Object**.

The Add Network Object dialog box appears.

**Step 10:** In the **Name** box, enter a description of the WLC. (Example: dmz-wlc-OEAP-1)

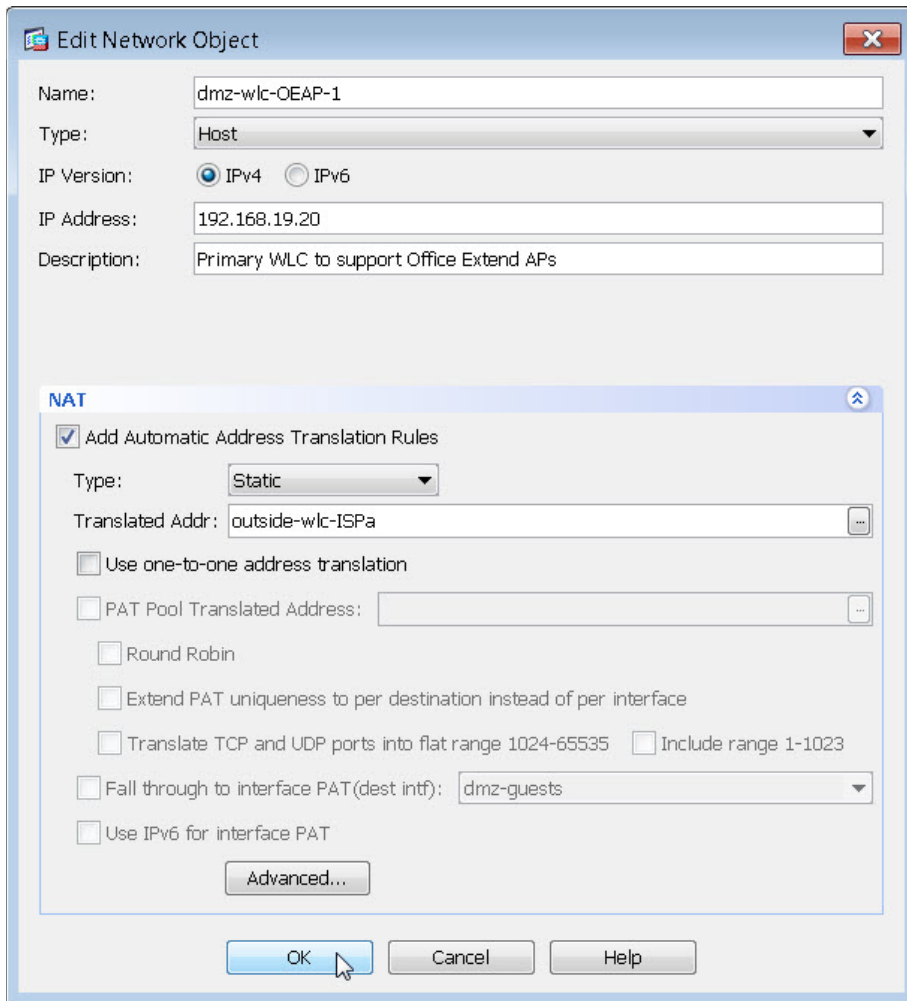
**Step 11:** In the **Type** list, choose **Host**.

**Step 12:** In the **IP Address** box, enter the WLC's management interface IP address, and then click **OK**. (Example: 192.168.19.20)

**Step 13:** Click the two down arrows. The NAT pane expands.

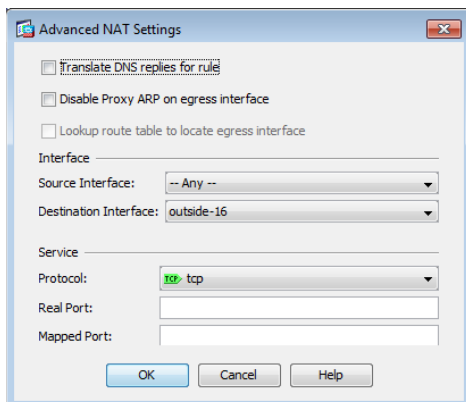
**Step 14:** Select **Add Automatic Address Translation Rules**.

**Step 15:** In the **Translated Addr** list, choose the network object created in Step 4, and then click **OK**. (Example: outside-wlc-ISPa)



**Step 16:** Click **Advanced**.

**Step 17:** In the **Destination Interface** list, choose the interface name for the primary or secondary Internet connection, and then click **OK**. (Example: outside-16, outside-17)

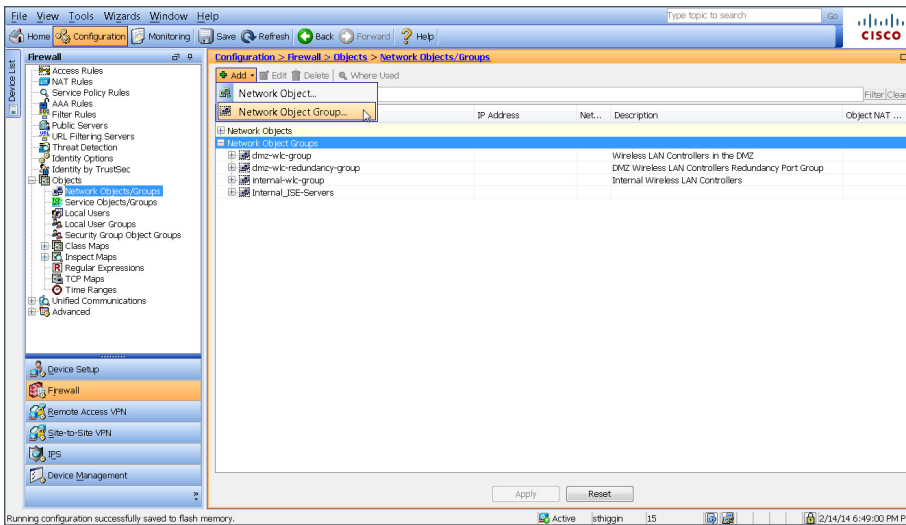


Next, to simplify the security policy configuration for similar network objects, create a network object group that will contain each of the OEAP WLCs.

Table 5 - OEAP WLC Object Groups

Network object group name	Network objects	Group description
dmz-OEAP-wlc-group	dmz-wlc-OEAP-1 dmz-wlc-OEAP-2	Wireless LAN OEAP WLCs in the DMZ.

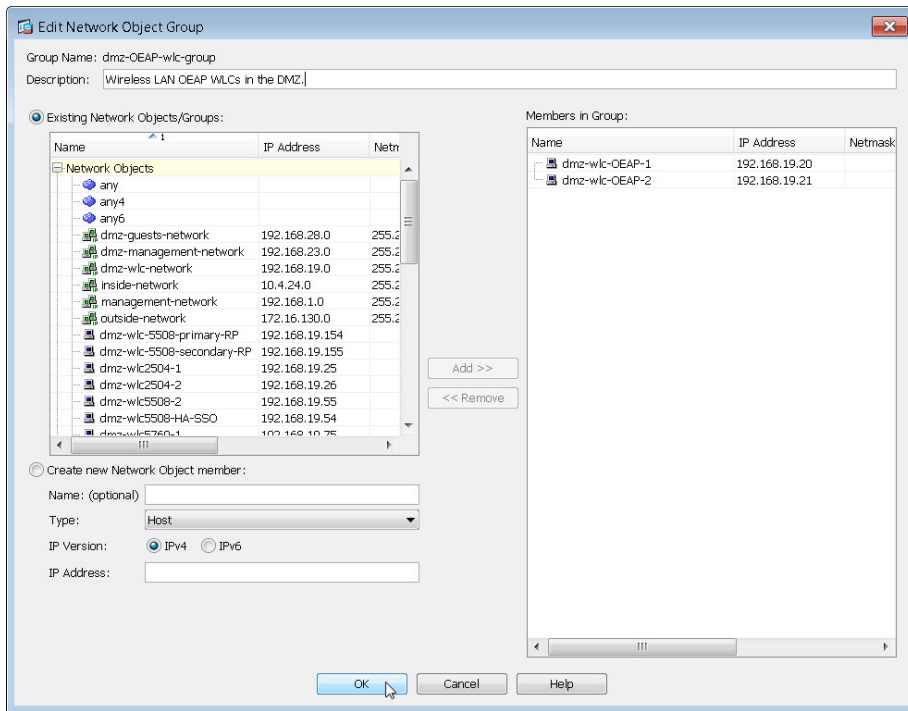
**Step 18:** Click **Add > Network Object Group**.



**Step 19:** In the Add Network Object Group dialog box, in the **Group Name** box, enter a name for the group (Example: dmz-OEAP-wlc-group).

**Step 20:** In the Existing Network Objects/Groups pane, select every OEAP WLC in your environment, and then click **Add** to move each Network Object into the Network Object Group.

**Step 21:** For each network object listed in Table 5, select the network object in the **Existing Network Objects/Groups** list, and then click **Add** to move each network object into the Members in Group list.



**Step 22:** Review the configured network object groups for completeness, click **OK**, and then **Apply**.



## Procedure 4 Configure OEAP security policy

The OEAP controllers located in the DMZ need to communicate using a number of services such as RADIUS, TACACS+, NTP, FTP and CAPWAP. This procedure provides connectivity from the dmz-mgmt-wlan (VLAN 1119) to the internal network and to the Internet using CAPWAP. On the Internet edge Cisco ASA appliance, navigate to **Configuration > Firewall > Access Rules**.

Table 6 - Firewall policy rules for DMZ WLC management interface

Interface	Action	Source	Destination	Service	Description	Logging Enable / Level
Any	Permit	dmz-OEAP-wlc-group	internal-aaa	tcp/tacacs, udp/1812, udp/1813	Allow OEAP based WLCs to communicate with the AAA/ACS server on the internal network	Selected / Default
Any	Permit	dmz-OEAP-wlc-group	internal-ntp	udp/ntp	Allow OEAP WLCs to communicate with the NTP server on the internal network	Selected / Default
Any	Permit	dmz-OEAP-wlc-group	any	tcp/ftp, tcp/ftp-data	Allow the OEAP WLCs to communicate with any FTP server	Selected / Default
Any	Permit	any	dmz-OEAP-wlc-group	udp/5246, udp/5247	Allow OEAP WLCs to communicate to external OEAP 600 A's on the Internet by using CAPWAP	Selected / Default

**Step 1:** Repeat Step 3 through Step 11 for each rule listed in Table 6.

**Step 2:** In order to position the new rule above the deny rule, click the rule that denies traffic from the **dmz-guest-wlan-networks** toward other internal networks.

30	<input checked="" type="checkbox"/>	dmz-guest-wlan-network/22	dmz-networks internal-network	ip	Deny	0	Deny traffic from the wireless guest network to the internal and dmz resources
----	-------------------------------------	---------------------------	----------------------------------	----	------	---	--

### Tech Tip

Be sure to perform this step for *every* rule listed in Table 6. Inserting the rules above the DMZ-to-any rule keeps the added rules in the same order as listed, which is essential for the proper execution of the security policy.

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

The Edit Access Rule dialog box appears.

**Step 4:** For **Interface**, select the interface. (Example: Any)

**Step 5:** Under **Action**, select the action listed. (Example: permit)

**Step 6:** In the **Source** list, choose the source. (Example: dmz-OEAP-wlc-group)

**Step 7:** In the **Destination** list, select the destination. (Example: internal-aaa)

**Step 8:** In the **Service list**, enter the service. (Example: tcp/tacacs, udp/1812, udp/1813)

**Step 9:** In the **Description** box, enter a useful description.

**Step 10:** Select or clear **Enable Logging**. (Example: Selected)

**Step 11:** In the **Logging Level** list, choose the logging level value, and then click **OK**. (Example: Default)

**Step 12:** After adding all of the rules in Table 6, in the order listed, in the Access Rules pane, click **Apply**.

30	<input checked="" type="checkbox"/>	dmz-OEAP-wlc-group	internal-aaa	tcp tacacs udp 1812 udp 1813	Permit	0	Allow OEAP based WLC's to communicate with the AAA/ACS server on the internal network.
31	<input checked="" type="checkbox"/>	dmz-OEAP-wlc-group	internal-ntp	ntp	Permit	0	Allow OEAP WLC's to communicate with the NTP server on the internal network.
32	<input checked="" type="checkbox"/>	dmz-OEAP-wlc-group	any	ftp ftp-data	Permit	0	Allow the OEAP WLC's to communicate with any FTP server.
33	<input checked="" type="checkbox"/>	any	dmz-OEAP-wlc-...	5246 5247	Permit	0	Allow OEAP WLC's to communicate to external OEAP 600 AP's on the Internet using CAPWAP.
34	<input checked="" type="checkbox"/>	dmz-guest-wlan-network/22	dmz-networks internal-network	ip	Deny	0	Deny traffic from the wireless guest network to the internal and dmz resources

## Configuring LAN Distribution Switch

1. Configure the distribution switch

### 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 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
```

**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
  switchport nonegotiate
  macro apply EgressQoSOneGig
  logging event link-status
  logging event trunk-status
  no shutdown
```

## 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 (Dedicated Redundancy Port is used by Default) [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)



## Tech Tip

The NAT IP Address must be the external, globally unique IP address that the Wireless LAN Controller displays on the Internet. This allows the WLC to place this IP address into the CAPWAP discovery response packet prior to encryption. The address shown here is an RFC-1918, private IP address and is used in this guide only for documentation purposes.

The screenshot shows the Cisco WLC configuration page for the 'management' interface. The page is titled 'Interfaces > Edit' and includes a navigation menu on the left with categories like General, Inventory, Interfaces, and Network Routes. The main content area is divided into several sections:

- General Information:** Interface Name: management, MAC Address: d0:d0:fd:1f:59:e0
- Configuration:** Quarantine: , Quarantine Vlan Id: 0
- NAT Address:** Enable NAT Address: , NAT IP Address: 172.16.130.20
- Interface Address:** VLAN Identifier: 0, IP Address: 192.168.19.20, Netmask: 255.255.255.0, Gateway: 192.168.19.1
- Physical Information:** Port Number: 1, Backup Port: 0, Active Port: 1, Enable Dynamic AP Management:
- DHCP Information:** Primary DHCP Server: 10.4.48.10, Secondary DHCP Server: 0.0.0.0
- 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.'

## 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 3: Click Set Timezone.

The screenshot shows the Cisco configuration interface for the 'Set Time' page. The page has a navigation bar at the top with 'COMMANDS' highlighted. On the left is a sidebar with various configuration options, including 'Set Time'. The main content area is titled 'Set Time' and contains two tabs: 'Set Date and Time' and 'Set Timezone'. The 'Set Timezone' tab is active. It displays the 'Current Time' as 'Tue May 31 11:07:38 2011'. Below this, there are sections for 'Date' (Month: May, Day: 31, Year: 2011), 'Time' (Hour: 11, Minutes: 7, Seconds: 38), and 'Timezone' (Delta: hours 0, mins 0, Location: (GMT -8:00) Pacific Time (US and Canada)). At the bottom, there is a 'Foot Notes' section with a note: '1. Automatically sets daylight savings time where used.'

## 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)

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

The screenshot shows the Cisco configuration interface for the 'SNMP v1 / v2c Community > New' page. The page has a navigation bar at the top with 'MANAGEMENT' highlighted. On the left is a sidebar with various configuration options, including 'SNMP'. The main content area is titled 'SNMP v1 / v2c Community > New' and 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 console interface. The top navigation bar includes links for Save Configuration, Ping, Logout, and Refresh. The main navigation menu on the left lists various management categories such as SNMP, HTTP-HTTPS, Telnet-SSH, Serial Port, Local Management, Users, User Sessions, Logs, Mgmt Via Wireless, Software Activation, and Tech Support. The main content area is titled 'SNMP v1 / v2c Community > New' and contains a form with the following fields:

Community Name	<input type="text" value="cisco123"/>
IP Address	<input type="text" value="10.4.48.0"/>
IP Mask	<input type="text" value="255.255.255.0"/>
Access Mode	<input type="text" value="Read/Write"/>
Status	<input type="text" value="Enable"/>

Buttons for '< Back' and 'Apply' are located at the top right of the form area.

**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.

Management > SNMP v1 / v2c Community

Community Name	IP Address	IP Mask	Access Mode	Status
<a href="#">cisco</a>	10.4.48.0	255.255.255.0	Read-Only	Enable
<a href="#">cisco123</a>	10.4.48.0	255.255.255.0	Read-Write	Enable

Step 16: Navigate to **Management > SNMP > General** and disable SNMP v3 Mode, and then press **Apply**.

Management > SNMP System Summary

Name: WLC-OEAP-1

Location: [ ]

Contact: [ ]

System Description: Cisco Controller

System Object ID: 1.3.6.1.4.1.9.1.1069

SNMP Port Number: 161

Trap Port Number: 162

SNMP v1 Mode: Disable

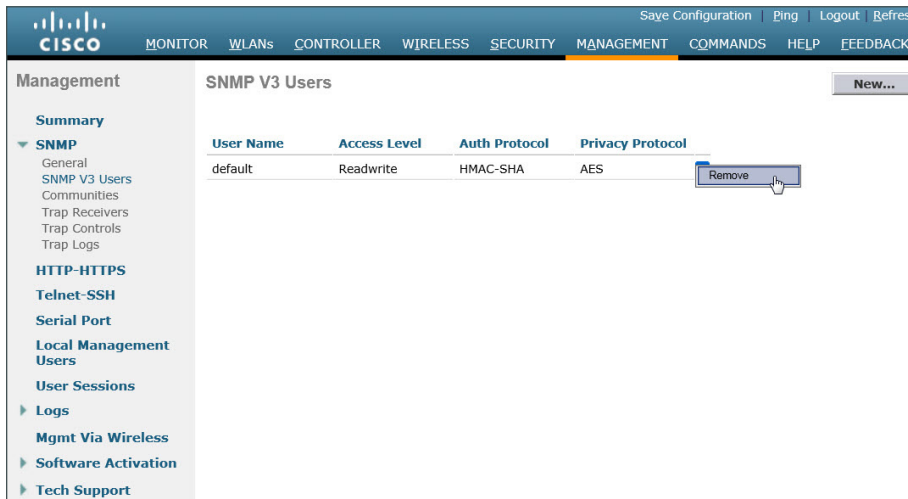
SNMP v2c Mode: Enable

SNMP v3 Mode: Disable

Apply

Step 17: Navigate to **Management > SNMP Communities > SNMP V3 Users**

**Step 18:** On the right side of the **default** User Name, point and click the blue down arrow, and then click **Remove**

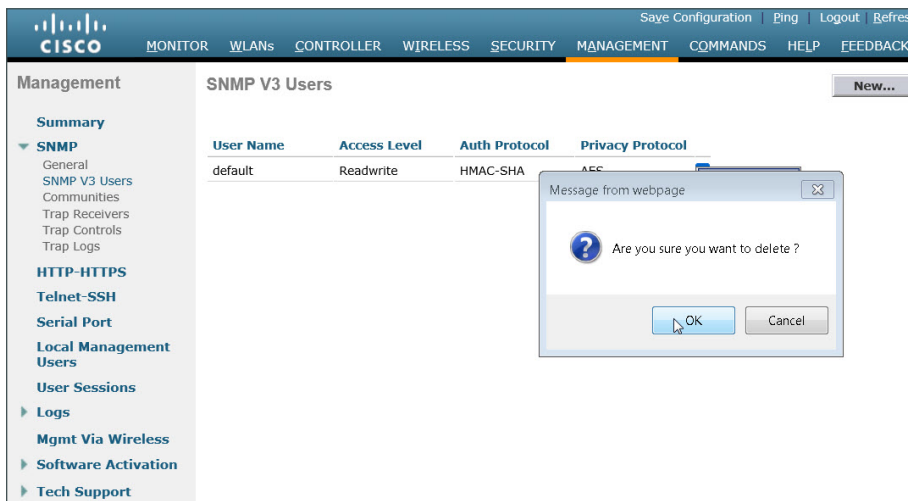


The screenshot shows the Cisco Management console interface. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', 'HELP', and 'FEEDBACK'. The 'MANAGEMENT' tab is active. On the left, a sidebar menu shows 'Management' expanded to 'SNMP'. The main content area is titled 'SNMP V3 Users' and contains a table with the following data:

User Name	Access Level	Auth Protocol	Privacy Protocol
default	Readwrite	HMAC-SHA	AES

A dropdown menu is open for the 'default' user, showing a 'Remove' button. A 'New...' button is located in the top right corner of the table area.

**Step 19:** Press **OK** to confirm that you are sure you want to delete, then press **Save Configuration**



The screenshot shows the same Cisco Management console interface as in Step 18. A confirmation dialog box is overlaid on the table, titled 'Message from webpage'. The dialog contains a question mark icon and the text 'Are you sure you want to delete?'. There are 'OK' and 'Cancel' buttons at the bottom of the dialog.

### Tech Tip

Changes to the SNMP configuration may sometimes require that the WLC be rebooted.

## 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**

The screenshot shows the Cisco WLC configuration interface for creating a new rule. The page title is "Access Control Lists > Rules > New". The configuration fields are as follows:

Field	Value
Sequence	1
Source	IP Address dropdown, 10.4.48.0, Netmask 255.255.255.0
Destination	Any dropdown
Protocol	TCP dropdown
Source Port	Any dropdown
Destination Port	HTTPS dropdown
DSCP	Any dropdown
Direction	Any dropdown
Action	Permit dropdown

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

Table 7 - Rule configuration values

Sequence	Source	Destination	Protocol	Source Port	Destination port	Action
1	10.4.48.0/255.255.255.0	Any	TCP	Any	HTTPS	Permit
2	10.4.48.0/255.255.255.0	Any	TCP	Any	Other/22	Permit
3	Any	Any	TCP	Any	HTTPS	Deny
4	Any	Any	TCP	Any	Other/22	Deny
5	Any	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**.

**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 contains a navigation tree with categories like AAA, RADIUS, TACACS+, 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): 1
- Server IP Address: 10.4.48.15
- Shared Secret Format: ASCII
- Shared Secret: [Redacted]
- Confirm Shared Secret: [Redacted]
- Port Number: 1813
- Server Status: Enabled
- Server Timeout: 2 seconds
- Network User:  Enable
- IPSec:  Enable

Buttons for "< Back" and "Apply" are visible at the top right of the configuration area.

## 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 Security configuration interface for TACACS+ Authentication Servers. The page title is "TACACS+ Authentication Servers > New". The left sidebar shows the navigation menu with "TACACS+" expanded. The main content area contains the following fields:

Server Index (Priority)	1
Server IP Address	10.4.48.15
Shared Secret Format	ASCII
Shared Secret	SecretKey
Confirm Shared Secret	SecretKey
Port Number	49
Server Status	Enabled
Server Timeout	5 seconds

Buttons for "< Back" and "Apply" are visible at the top right of the form.

**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 Security configuration interface for TACACS+ Accounting Servers. The page title is "TACACS+ Accounting Servers > New". The left sidebar shows the navigation menu with "TACACS+" expanded. The main content area contains the following fields:

Server Index (Priority)	1
Server IP Address	10.4.48.15
Shared Secret Format	ASCII
Shared Secret	SecretKey
Confirm Shared Secret	SecretKey
Port Number	49
Server Status	Enabled
Server Timeout	5 seconds

Buttons for "< Back" and "Apply" are visible at the top right of the form.

**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 configuration page for TACACS+ Authorization Servers. The left sidebar contains a navigation tree with categories like AAA, RADIUS, TACACS+, LDAP, Local EAP, Priority Order, Certificate, Access Control Lists, Wireless Protection Policies, Web Auth, TrustSec SXP, and Advanced. The main content area is titled "TACACS+ Authorization Servers > New" and includes 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 fields filled with masked characters, 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 "Priority Order > Management User" configuration page. It features two columns: "Not Used" and "Order Used for Authentication". In the "Not Used" column, "RADIUS" is selected in a dropdown menu. In the "Order Used for Authentication" column, "TACACS+" and "LOCAL" are listed in a dropdown menu, with "TACACS+" at the top. "Up" and "Down" arrow buttons are positioned to the right of the dropdown. Below the columns, a note states: "If LOCAL is selected as second priority then user will be authenticated against LOCAL only if first priority is unreachable." An "Apply" button is located at the top right.

## Configuring Voice/Data WLAN 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 Controller configuration interface. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', 'HELP', and 'FEEDBACK'. The 'CONTROLLER' tab is active. On the left, a sidebar menu lists various configuration categories: 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 contains two input fields: 'Interface Name' with the value 'Wireless-Data' and 'VLAN Id' with the value '244'. There are '< Back' and 'Apply' buttons at the top right of the form.

**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 the 'Wireless-Data' interface. The page is divided into several sections:

- General Information:** Interface Name: Wireless-Data, MAC Address: d0:d0:fd:1f:59:e0
- Configuration:** Guest Lan, Quarantine, and Quarantine Vlan Id (0) checkboxes.
- Physical Information:** Port Number (2), Backup Port (0), Active Port (0), and Enable Dynamic AP Management checkbox.
- Interface Address:** VLAN Identifier (244), IP Address (10.4.144.5), Netmask (255.255.252.0), and Gateway (10.4.144.1).
- DHCP Information:** Primary DHCP Server (10.4.48.10) and Secondary DHCP Server (empty).
- Access Control List:** ACL Name (none).

A note at the bottom states: "Note: Changing the Interface parameters causes the VLANs to be temporarily disabled and thus may result in loss of connectivity for some clients."

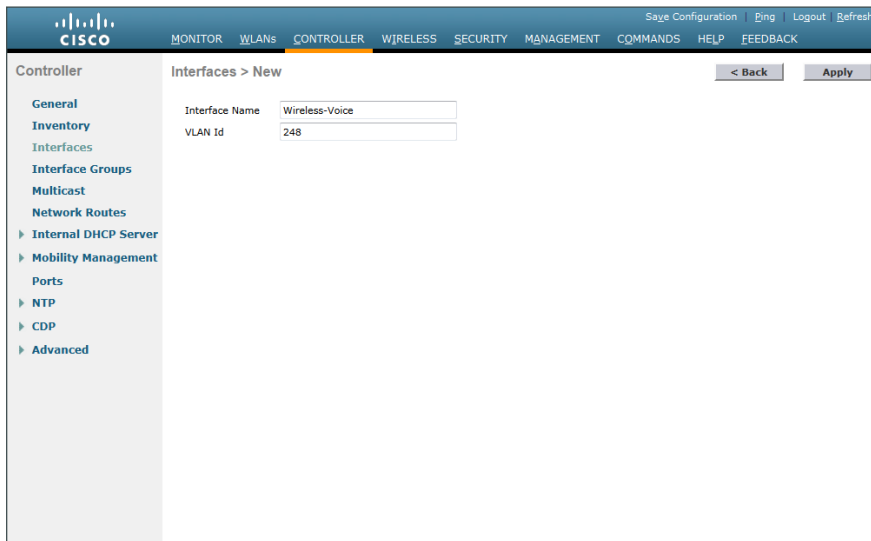
## Procedure 2 Create the wireless LAN voice interface

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 3:** Enter the **VLAN Id**, and then click **Apply**. (Example: 248)



The screenshot shows the Cisco Controller configuration interface. The top navigation bar includes 'MONITOR', 'WLANS', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', 'HELP', and 'FEEDBACK'. The 'CONTROLLER' tab is active. On the left, a sidebar menu lists various configuration categories: 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 contains two input fields: 'Interface Name' with the value 'Wireless-Voice' and 'VLAN Id' with the value '248'. There are '< Back' and 'Apply' buttons at the top right of the configuration area.

**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)

**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 an interface named 'wireless-voice'. The page is titled 'Interfaces > Edit' and has a navigation bar at the top with options like 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', 'HELP', and 'FEEDBACK'. The left sidebar contains a menu with categories like 'General', 'Inventory', 'Interfaces', 'Interface Groups', 'Multicast', 'Network Routes', 'Internal DHCP Server', 'Mobility Management', 'Ports', 'NTP', 'CDP', and 'Advanced'. The main content area is divided 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: 248, IP Address: 10.4.148.5, Netmask: 255.255.252.0, Gateway: 10.4.148.1), '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.'

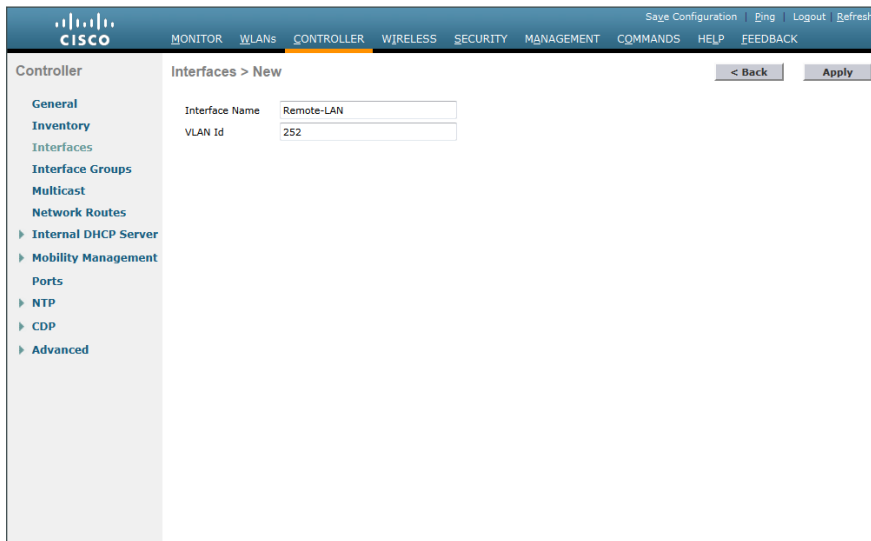
### Procedure 3 Create the remote LAN interface

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



The screenshot shows the Cisco Controller configuration interface. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', 'HELP', and 'FEEDBACK'. The 'CONTROLLER' tab is active. The left sidebar lists various configuration categories: 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 contains two input fields: 'Interface Name' with the value 'Remote-LAN' and 'VLAN Id' with the value '252'. There are '< Back' and 'Apply' buttons at the top right of the configuration area.

**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)

**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 an interface named 'Remote-LAN'. The configuration is as follows:

- General Information:** Interface Name: Remote-LAN, MAC Address: d0:d0:fd:1f:59:e0
- Configuration:** Guest Lan: , Quarantine: , Quarantine Vlan Id: 0
- Physical Information:** Port Number: 2, Backup Port: 0, Active Port: 0, Enable Dynamic AP Management:
- Interface Address:** VLAN Identifier: 252, IP Address: 10.4.152.5, Netmask: 255.255.252.0, Gateway: 10.4.152.1
- DHCP Information:** Primary DHCP Server: 10.4.48.10, Secondary DHCP Server: (empty)
- 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.

## 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.

The screenshot shows the Cisco Controller configuration page for WLANs. The table below lists the WLAN entries:

WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies
1	WLAN	WLAN-Data	WLAN-Data	Enabled	[WPA2][Auth(802.1X)]

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

The screenshot shows the Cisco configuration interface for a WLAN named 'WLAN-Data'. The 'General' tab is selected. The configuration includes:

- Profile Name: WLAN-Data
- Type: WLAN
- SSID: WLAN-Data
- Status:  Enabled
- Security Policies: [WPA2][Auth(802.1X)]
- Radio Policy: All
- Interface/Interface Group(G): wireless-data
- 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.

Next, enable Application Visibility and Control (AVC).

**Step 4:** Navigate to the QoS tab, select **Application Visibility**, click **Apply**, and then click **Save Configuration**, and agree to confirmation questions.

The screenshot shows the Cisco configuration interface for a WLAN named 'WLAN-Data', now on the 'QoS' tab. The configuration includes:

- Quality of Service (QoS): Silver (best effort)
- Application Visibility:  Enabled
- AVC Profile: none
- Netflow Monitor: none

Override Per-User Bandwidth Contracts (kbps):

	DownStream	UpStream
Average Data Rate	0	0
Burst Data Rate	0	0
Average Real-Time Rate	0	0
Burst Real-Time Rate	0	0

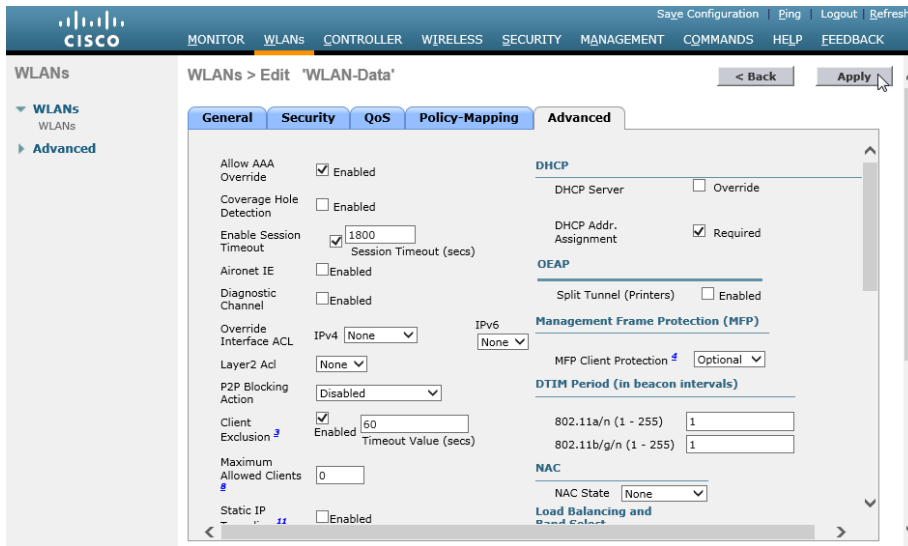
Clear

Override Per-SSID Bandwidth Contracts (kbps):

	DownStream	UpStream
Average Data Rate	0	0
Burst Data Rate	0	0



**Step 5:** On the Advanced tab, clear **Coverage Hole Detection**, enable **DHCP Addr. Assignment Required**, clear **Aironet IE**, enable **Allow AAA Override**, and then click **Apply**.

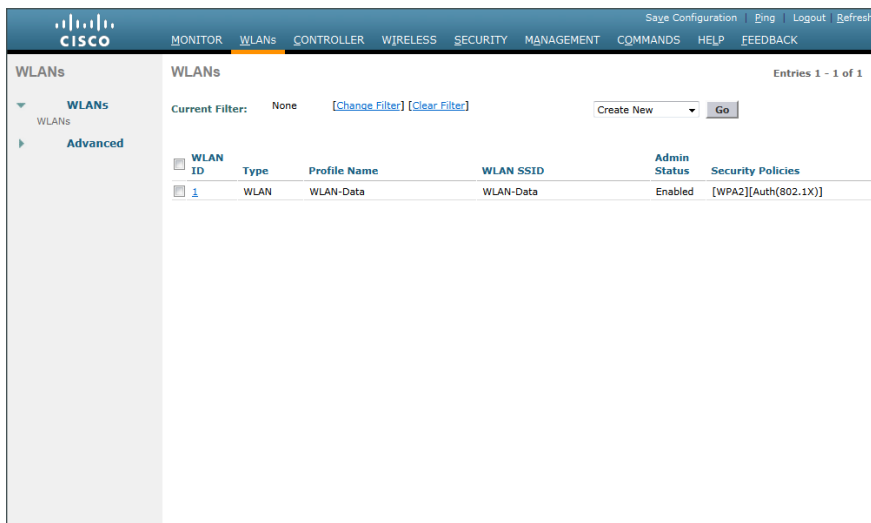


## Procedure 5 Configure voice wireless LAN

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.

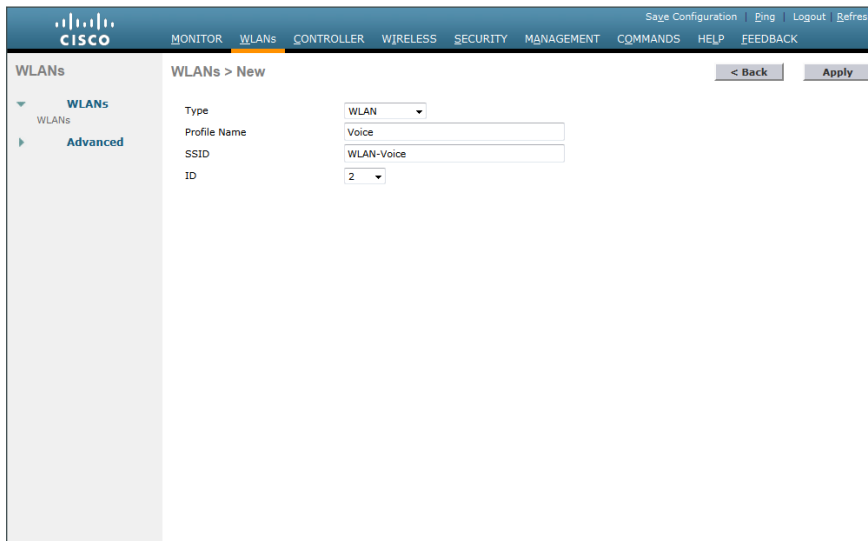
**Step 1:** Navigate to **WLANs**.

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



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

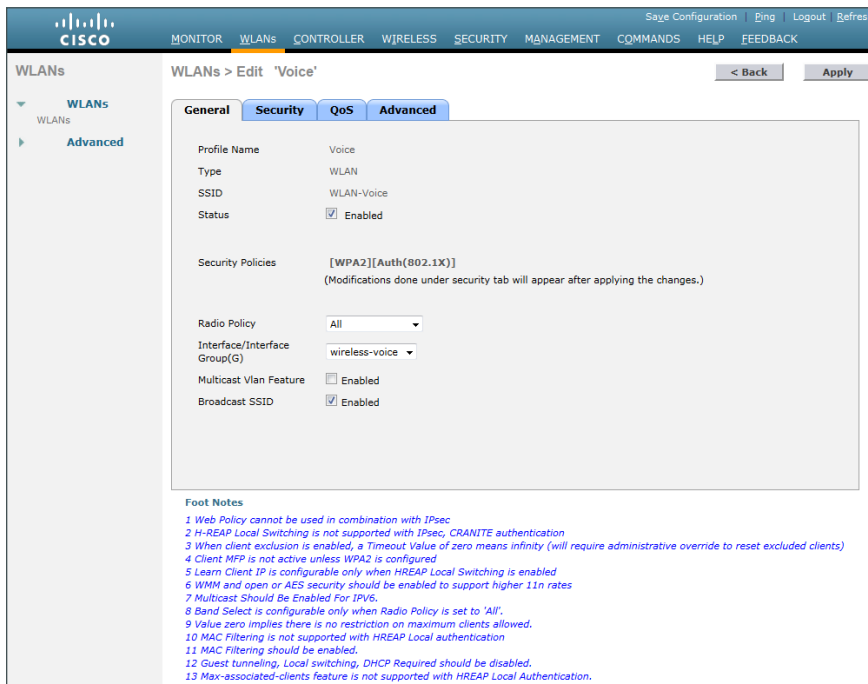
**Step 4:** In the SSID box, enter the voice WLAN name, and then click **Apply**. (Example: WLAN-Voice)



The screenshot shows the Cisco configuration interface for creating a new WLAN. The page title is 'WLANs > New'. The 'Type' is set to 'WLAN', 'Profile Name' is 'Voice', 'SSID' is 'WLAN-Voice', and 'ID' is '2'. There are 'Back' and 'Apply' buttons at the top right.

**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 configuration interface for editing an existing WLAN named 'Voice'. The 'General' tab is selected. The 'Status' is checked and set to 'Enabled'. The 'Interface/Interface Group(G)' is set to 'wireless-voice'. The 'Security Policies' are set to '[WPA2][Auth(802.1X)]'. There are 'Back' and 'Apply' buttons at the top right.

**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 and enable AVC.

The screenshot shows the Cisco configuration interface for a WLAN named 'Voice'. The 'QoS' tab is selected. Under the 'Quality of Service (QoS)' section, the dropdown menu is set to 'Platinum (voice)'. The 'Application Visibility' checkbox is checked and labeled 'Enabled'. The 'AVC Profile' dropdown is set to 'none', and the 'Netflow Monitor' dropdown is also set to 'none'. Below this, there are sections for 'Override Per-User Bandwidth Contracts (kbps)' and 'Override Per-SSID Bandwidth Contracts (kbps)', each with input fields for Average Data Rate and Burst Data Rate for both DownStream and UpStream directions.

**Step 8:** Click the Advanced tab, and then clear Coverage Hole Detection, clear Aironet IE, enable Allow AAA Override, and then click Apply.

The screenshot shows the Cisco configuration interface for a WLAN named 'Voice', with the 'Advanced' tab selected. In the 'Allow AAA Override' section, the checkbox is checked and labeled 'Enabled'. Under 'Coverage Hole Detection', the checkbox is unchecked. In the 'Aironet IE' section, the checkbox is unchecked. The 'Enable Session Timeout' checkbox is checked, with a value of '1800' entered in the 'Session Timeout (secs)' field. Other settings include 'Diagnostic Channel' (unchecked), 'Override Interface ACL' (set to 'None' for both IPv4 and IPv6), 'Layer2 Acl' (set to 'None'), 'P2P Blocking Action' (set to 'Disabled'), and 'Client Exclusion' (checked, with a 'Timeout Value (secs)' of '60'). On the right side, 'DHCP' settings show 'DHCP Server' (unchecked) and 'DHCP Addr. Assignment' (unchecked). 'OEAP' settings show 'Split Tunnel (Printers)' (unchecked). 'Management Frame Protection (MFP)' settings show 'MFP Client Protection' set to 'Optional'. 'DTIM Period (in beacon intervals)' shows values of '1' for both 802.11a/n and 802.11b/g/n. 'NAC' settings show 'NAC State' set to 'None'.

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

The screenshot shows the Cisco configuration interface for WLANs. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', 'HELP', and 'FEEDBACK'. The 'WLANs' section is active, showing a table of existing WLANs. The table has columns for 'WLAN ID', 'Type', 'Profile Name', 'WLAN SSID', 'Admin Status', and 'Security Policies'. Two entries are listed: ID 1 (WLAN, WLAN-Data, WLAN-Data, Enabled, [WPA2][Auth(802.1X)]) and ID 2 (WLAN, Voice, WLAN-Voice, Enabled, [WPA2][Auth(802.1X)]). A 'Create New' button is visible in the top right of the table area.

WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies
1	WLAN	WLAN-Data	WLAN-Data	Enabled	[WPA2][Auth(802.1X)]
2	WLAN	Voice	WLAN-Voice	Enabled	[WPA2][Auth(802.1X)]

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

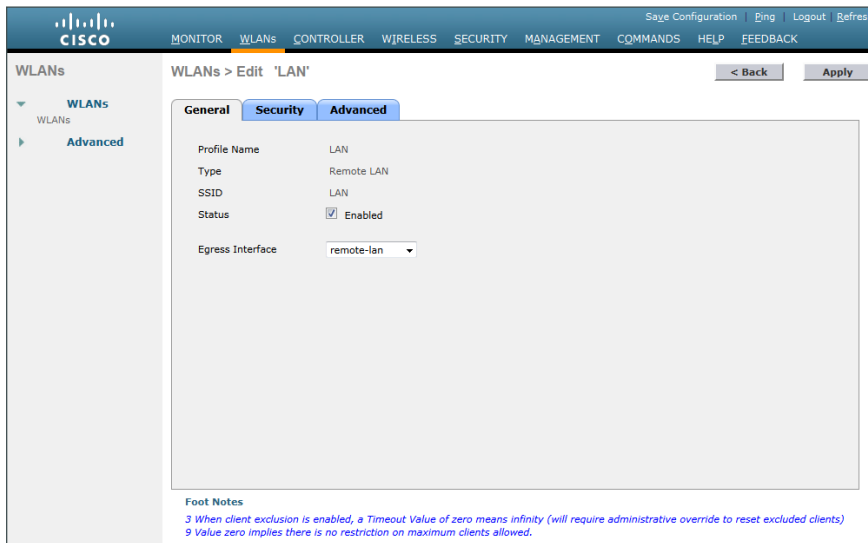
**Step 4:** Enter the **Profile Name**, and then click **Apply**. (Example: LAN)

The screenshot shows the 'WLANs > New' configuration page. The 'Type' dropdown is set to 'Remote LAN'. The 'Profile Name' text box contains 'LAN'. The 'ID' dropdown is set to '3'. There are '< Back' and 'Apply' buttons at the top right of the form area.

Type: Remote LAN  
Profile Name: LAN  
ID: 3

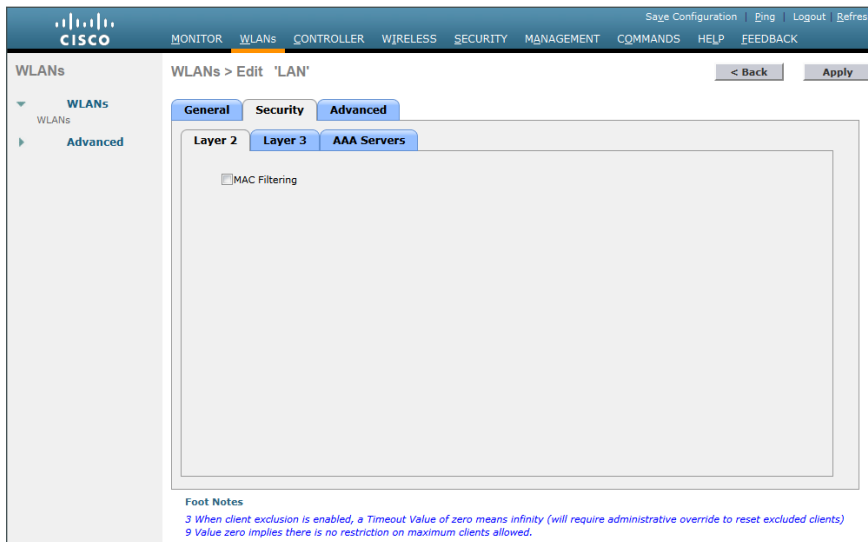
**Step 5:** On the General tab, to the right of **Status**, select **Enabled**.

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



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

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



## 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)

Network Resources > Default Network Device

**Default Network Device**  
The default device definition can optionally be used in cases where no specific device definition is found that matches a device IP address.

Default Network Device Status:

**Network Device Groups**

Location

Device Type

**Authentication Options**

▼ TACACS+

Shared Secret:

Single Connect Device

Legacy TACACS+ Single Connect Support

TACACS+ Draft Compliant Single Connect Support

▼ RADIUS

Shared Secret:

CoA port:

Enable KeyWrap

Key Encryption Key:

Message Authenticator Code Key:

Key Input Format  ASCII  HEXADECIMAL

= Required fields

### Tech Tip

If management authentication to the WLC does not work, ensure that the Internet edge OEAP WLCs have been added to the ACS server as AireOS devices which require the use of the AireOS TACACS+ shell template.

## **Procedure 2** Configure the access point account

**Step 1:** 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 MAC address for the access point is found on a label outside of the product packaging and on a label on the bottom of the access point. In Cisco Secure ACS, navigate to **Users and Identity Stores > Internal Identity Stores > Users**.

**Step 2:** Click **Create**.

**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.

Users and Identity Stores > Internal Identity Stores > Users > Create

**General**

Name:  Status: Enabled

Description:

Identity Group: All Groups

**Password Information**

Password must:

- Contain 4 - 32 characters

Enable Password Information

Password must:

- Contain 4 - 32 characters

Password Type:

Enable Password:

Password:

Confirm Password:

Change password on next login

**User Information**

There are no additional identity attributes defined for user records

= Required fields

### 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**.

CISCO MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

Security

AAA

- General
- 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

AP Policies

Policy Configuration

Accept Self Signed Certificate (SSC)

Accept Manufactured Installed Certificate (MIC)

Accept Local Significant Certificate (LSC)

Authorize MIC APs against auth-list or AAA

Authorize LSC APs against auth-list

AP Authorization List Entries 1 - 1 of 1

Search by MAC

MAC Address	Certificate Type	SHA1 Key Hash
00:50:56:a2:5d:96	SSC	b62741ab695f6ef95e5a3fc7b84496ee8972cd8f



## Configuring Cisco OfficeExtend AP

1. Configure the Cisco OfficeExtend AP

The OfficeExtend 600 AP requires minimal configuration by the end user. For environments where zero-touch end user deployments are required, the corporate IT department or network-integration partner should pre-configure the OEAP-600 with the address of the head-end OfficeExtend-based Wireless LAN controller, as described in this procedure.

### Procedure 1 Configure the Cisco OfficeExtend AP

Figure 2 - Cisco Aironet 600 Series OfficeExtend Access Point Ports

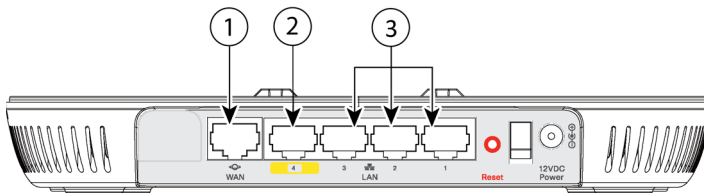


Table 8 - Cisco Aironet 600 Series OfficeExtend Access Point Ports

Port on OEAP 600	Port as Noted in Figure 2	Port Number as shown on OEAP 600
WAN	1	WAN
Remote LAN Port (Corporate)	2	4
Local Ethernet Ports (Pass through)	3	1, 2, 3

**Step 1:** Connect the WAN port (noted as 1 in Figure 2) 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.

#### **i** 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 to ports 1, 2 or 3, noted as 3 in Figure 2. 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.

The screenshot shows the Cisco OfficeExtend Access Point Welcome page. The navigation bar includes HOME, CONFIGURATION, EVENT\_LOG, and HELP. The main content area is titled "Home: Summary" and contains the following sections:

**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
No associations listed.				

A note indicates: "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 Cisco OfficeExtend Access Point Configuration page. The navigation bar includes HOME, CONFIGURATION, EVENT\_LOG, and HELP. The main content area is titled "Configuration" and contains the following sections:

**Primary Controller**

IP Address:

**Uplink IP Configuration**

Static IP	<input type="checkbox"/>
Domain Name	cisco.com
IP Address	192.168.1.100
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.1
DNS Server	171.68.226.120

©2010 Cisco Systems Inc. All rights reserved.

**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

While the access point attempts to make a connection to the WLC, the Cisco logo status LED on the top of the access point flashes blue and amber. Once connected, the status LED flashes blue until the AireOS download is complete. When the download is complete, the access point restarts. After the access point connects to the controller again, the status LED is displayed as solid blue or purple.

Status LED	Meaning
Purple	Association status, when CAPWAP is connected: Normal operating condition, but no wireless client associated.
Blue	Association status, when CAPWAP is connected: Normal operating condition, at least one wireless client association.
Flashing Blue	Operating Status: Software upgrade in progress.
Flashing Orange	Operating Status: No IP address, waiting for DHCP IP.
Cycling through purple, orange and blue	Operating Status: Discovery/join process in progress, no client associated.
Cycling through purple, orange	Operating Status: Discovery/join process in progress, with client associated.
Orange	Cisco IOS errors: Software failure; try disconnecting and reconnecting unit power.

## PROCESS

### Enabling AP Radios

1. Configure the WLC

After a new Cisco OfficeExtend Access Point joins the controller, the radios may be 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**.

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
AP008.845.4441	1	40:37:ac:09:0d:80	-	Enable	UP	157 *	NA	NA	N/A	1 *	External
AP000.f0c0.b85c	1	58:bc:27:0e:1c:60	-	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
APECC8.8288.2858	1	ecc8:82: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**.

**General**

AP Name: APECC8.8288.2858

Admin Status: **Enable**

Operational Status: DOWN

Slot #: 1

**11n Parameters**

11n Supported: Yes

**RF Channel Assignment**

Current Channel: 36

Channel Width: 20 MHz

Assignment Method:  AP Controlled

**Tx Power Level Assignment**

Current Tx Power Level: 1

Assignment Method:  AP Controlled

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**.

## 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)

The screenshot displays the Cisco WLC configuration interface for AP APE05F.B9DC.FC30. The 'High Availability' tab is active, showing a table with the following data:

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

Below the table, the 'AP Failover Priority' is set to '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.

## Enable Fast SSID Change

1. Globally enable Fast SSID change

By enabling fast SSID change, the wireless client can rapidly switch between wireless LAN SSIDs.

### Procedure 1 Globally enable Fast SSID change

#### (Optional)

**Step 1:** Navigate to **Controller > General** and, in the **Fast SSID change** list, choose **Enabled**.

**Step 2:** Press **Apply** and **Save Configuration**.

The screenshot shows the Cisco Controller configuration interface. The top navigation bar includes: MONITOR, WLANs, CONTROLLER (selected), WIRELESS, SECURITY, MANAGEMENT, COMMANDS, HELP, and FEEDBACK. The left sidebar lists various configuration categories: Controller, General, Inventory, Interfaces, Interface Groups, Multicast, Network Routes, Mobility Management, Ports, and NTP. The main content area is titled 'General' and contains the following configuration items:

Name	vWLC-RemoteSites-1
802.3x Flow Control Mode	Disabled
Broadcast Forwarding	Disabled
AP Multicast Mode	Unicast
AP Fallback	Enabled
Fast SSID change	Enabled
Default Mobility Domain Name	REMOTES
RF Group Name	REMOTES

# 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	7.6.120.0

## 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	7.6.120.0
	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 5.5 VMware Software And Base License	CSACS-5.5-VM-K9	5.5.0.46.2 Cumulative Patch



## Internet Edge

Functional Area	Product Description	Part Numbers	Software
Firewall	Cisco ASA 5545-X IPS Edition - security appliance	ASA5545-IPS-K9	ASA 9.1(5) IPS 7.1(8p2)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 ASA 5512-X Security Plus license	ASA5512-SEC-PL	
	Firewall Management	ASDM	7.1(6)

## Internet Edge LAN

Functional Area	Product Description	Part Numbers	Software
DMZ Switch	Cisco Catalyst 2960-X Series 24 10/100/1000 PoE and 2 SFP+ Uplink	WS-C2960X-24PS	15.0(2)EX5 LAN Base license
	Cisco Catalyst 2960-X FlexStack-Plus Hot-Swappable Stacking Module	C2960X-STACK	

## LAN Distribution Layer

Functional Area	Product Description	Part Numbers	Software
Modular Distribution Layer Virtual Switch Pair	Cisco Catalyst 6800 Series 6807-XL 7-Slot Modular Chassis	C6807-XL	15.1(2)SY3 IP Services license
	Cisco Catalyst 6500 VSS Supervisor 2T with 2 ports 10GbE and PFC4	VS-S2T-10G	
	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	
	Cisco Catalyst 6500 CEF720 48 port 10/100/1000mb Ethernet	WS-X6748-GE-TX	
	Cisco Catalyst 6500 Distributed Forwarding Card 4	WS-F6K-DFC4-A	
	Cisco Catalyst 6500 Series 6506-E 6-Slot Chassis	WS-C6506-E	
	Cisco Catalyst 6500 VSS Supervisor 2T with 2 ports 10GbE and PFC4	VS-S2T-10G	
	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	
	Cisco Catalyst 6500 48-port GigE Mod (SFP)	WS-X6748-SFP	
	Cisco Catalyst 6500 Distributed Forwarding Card 4	WS-F6K-DFC4-A	
	Cisco Catalyst 6500 24-port GigE Mod (SFP)	WS-X6724-SFP	
	Cisco Catalyst 6500 Distributed Forwarding Card 4	WS-F6K-DFC4-A	

Functional Area	Product Description	Part Numbers	Software
Extensible Fixed Distribution Layer Virtual Switch Pair	Cisco Catalyst 6800 Series 6880-X Extensible Fixed Aggregation Switch (Standard Tables)	C6880-X-LE	15.1(2)SY3 IP Services license
	Cisco Catalyst 6800 Series 6880-X Multi Rate Port Card (Standard Tables)	C6880-X-LE-16P10G	
Modular Distribution Layer Virtual Switch Pair	Cisco Catalyst 4500E Series 4507R+E 7-slot Chassis with 48Gbps per slot	WS-C4507R+E	3.5.3E(15.2.1E3) Enterprise Services license
	Cisco Catalyst 4500E Supervisor Engine 7-E, 848Gbps	WS-X45-SUP7-E	
	Cisco Catalyst 4500E 12-port 10GbE SFP+ Fiber Module	WS-X4712-SFP+E	
	Cisco Catalyst 4500E 48-Port 802.3at PoE+ 10/100/1000 (RJ-45)	WS-X4748-RJ45V+E	
Fixed Distribution Layer Virtual Switch Pair	Cisco Catalyst 4500-X Series 32 Port 10GbE IP Base Front-to-Back Cooling	WS-C4500X-32SFP+	3.5.3E(15.2.1E3) Enterprise Services license
Stackable Distribution Layer Switch	Cisco Catalyst 3850 Series Stackable Switch with 12 SFP Ethernet	WS-C3850-12S	3.3.3SE(15.0.1EZ3) IP Services license
	Cisco Catalyst 3850 Series 4 x 1GE Network Module	C3850-NM-4-1G	
	Cisco Catalyst 3850 Series 2 x 10GE Network Module	C3850-NM-2-10G	
	Cisco Catalyst 3750-X Series Stackable 12 GbE SFP ports	WS-C3750X-12S-E	15.2(1)E3 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 Cisco made to this guide since its previous edition.

- We upgraded the Cisco Wireless LAN Controllers to release 7.6.120.0.
- We incorporated and validated numerous wireless best practices, including:
  - Implemented the **switchport nonegotiate** command, which eliminates Dynamic Trunking Protocol (DTP) overhead for OEAP WLCs that use trunk ports
  - Disabled SNMP v3
  - Enabled Fast SSID change support
  - Required DHCP address assignment for added security to Data WLAN
  - Enabled Allow AAA Override to allow ISE/RADIUS to override local WLC policy if necessary (QoS, VLAN, etc.)
- We improved overall readability of the Cisco ASA Firewall configuration sections throughout the guide.

## Feedback

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



**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](http://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.

© 2014 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](http://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)