Cisco OfficeExtend

TECHNOLOGY DESIGN GUIDE

August 2013

VALIDATED DESIGN

Table of Contents

Preface

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

CVDs include two guide types that provide tested and validated design and deployment 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 or reference existing CVDs, but also include product features and functionality across Cisco products and may 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 using their own setup and configuration.

How to Read Commands

Many CVD guides tell you how to use a command-line interface (CLI) to configure network devices. This section describes the conventions used to specify commands that you must enter.

Commands to enter at a CLI appear as follows:

```
configure terminal
```

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

```
ntp server 10.10.48.17
```

Commands with variables that you must define appear as follows:

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

Commands at a CLI or script prompt appear as follows:

```
Router# enable
```

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

```
police rate 10000 pps burst 10000 packets conform-action set-discard-class-
transmit 48 exceed-action transmit
```

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

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

Comments and Questions

If you would like to comment on a guide or ask questions, please use the feedback form.

For the most recent CVD guides, see the following site:

http://www.cisco.com/go/cvd

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 following site: http://www.cisco.com/go/cvd

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 and zero-touch deployment at 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

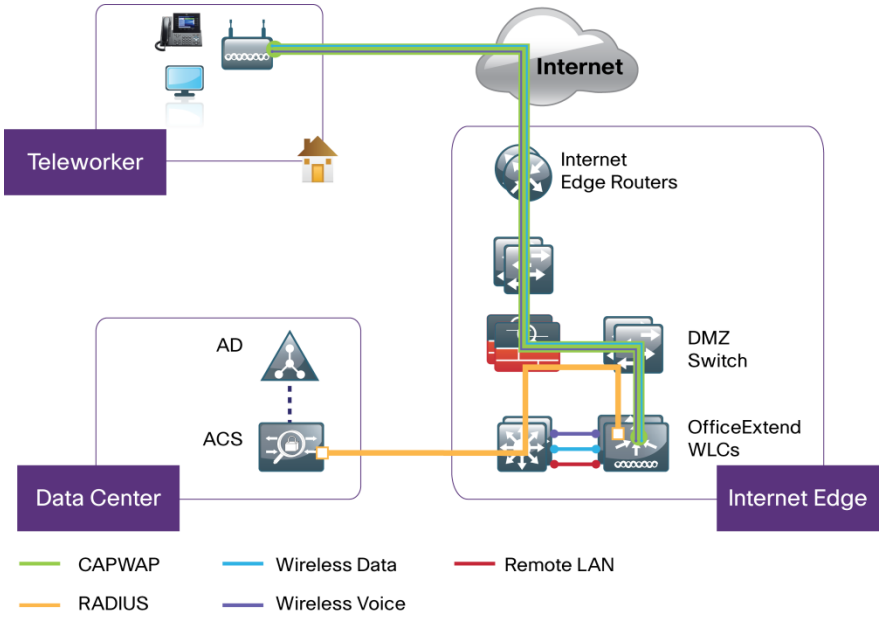
Cisco Aironet 600 Series OfficeExtend Access Points are lightweight. This means they cannot act independently of a wireless LAN controller (WLC). As the access point communicates with the WLC resources, it will download its configuration and synchronize its software/firmware image, if required. Cisco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

Deployment Details

This 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	

PROCESS

Configuring Cisco Secure ACS

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

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

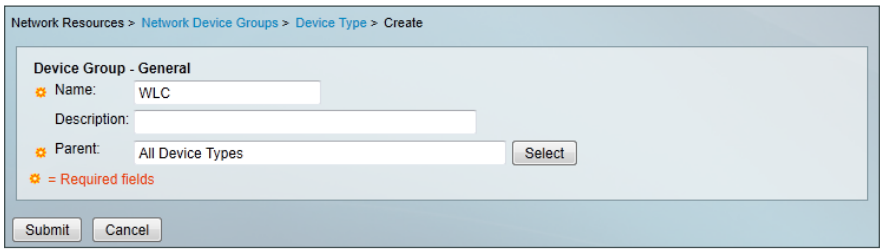
Procedure 1 Create the wireless device group

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**.



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**.

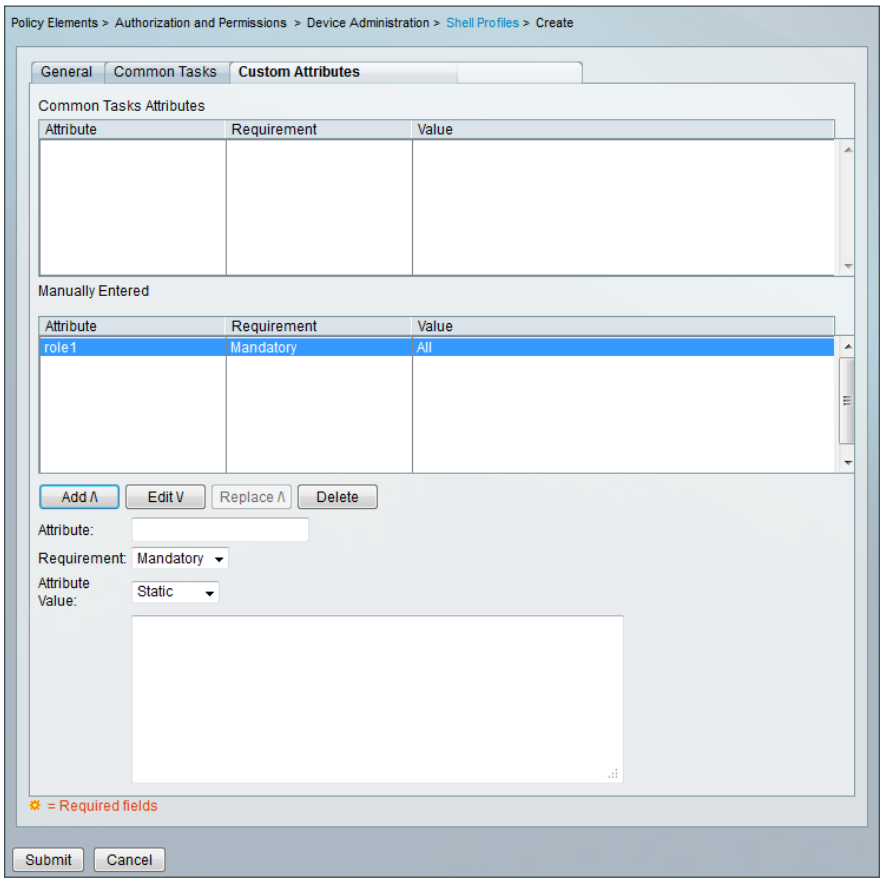
Step 2: Under the General tab, in the **Name** box, enter a name for the wireless shell profile. (Example: WLC Shell)

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**.



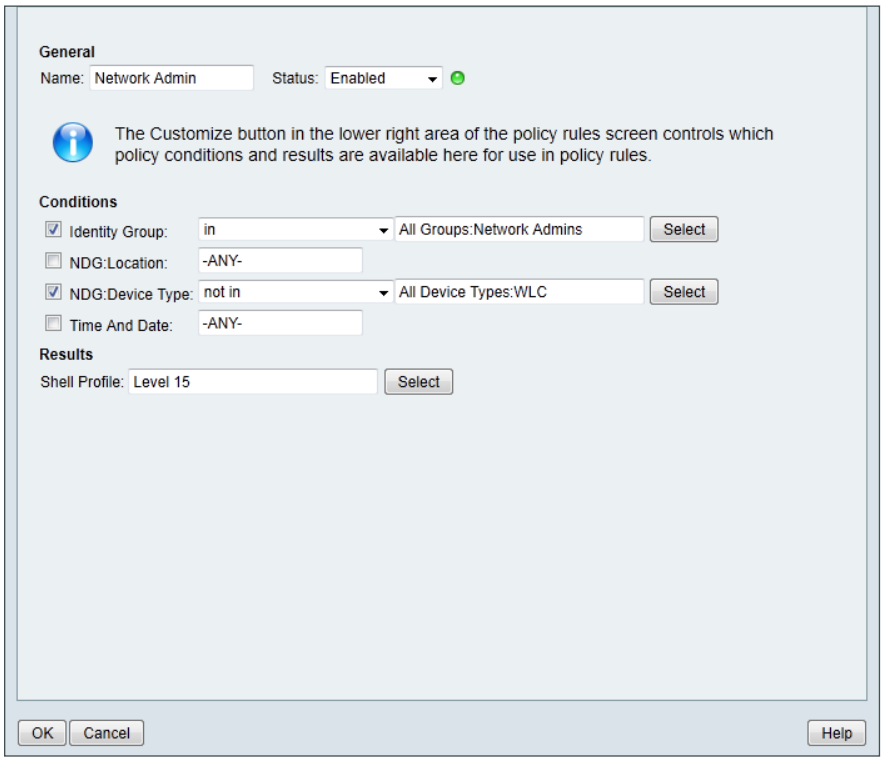
Procedure 3 Modify the device admin policy

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**.



Next, create a WLC authorization rule.

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

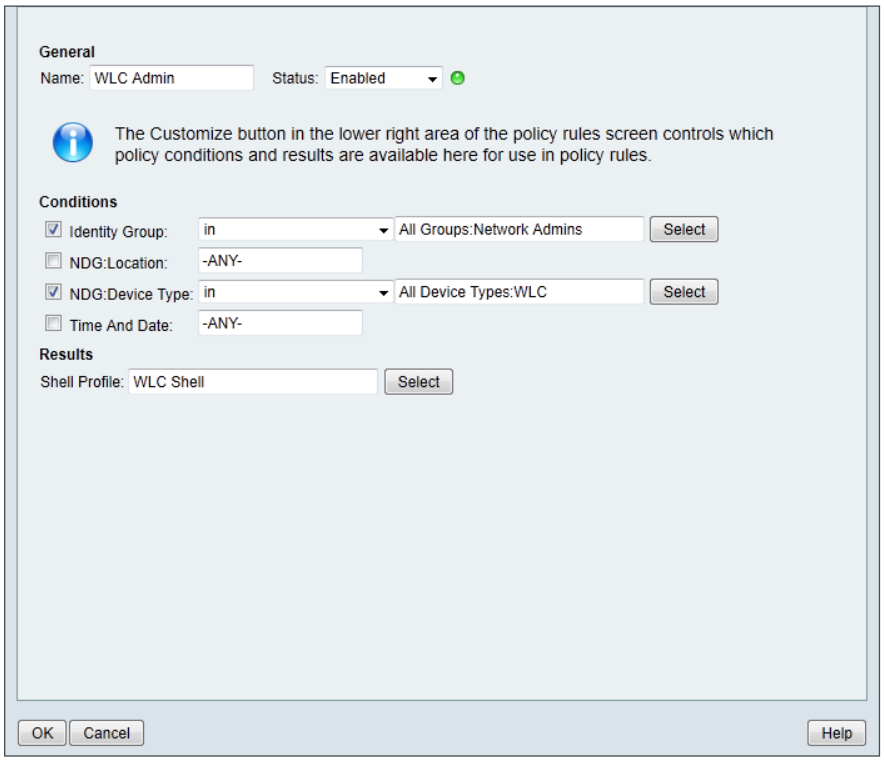
Step 5: In the **Name** box, enter a name for the WLC authorization rule. (Example: WLC Admin)

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**.

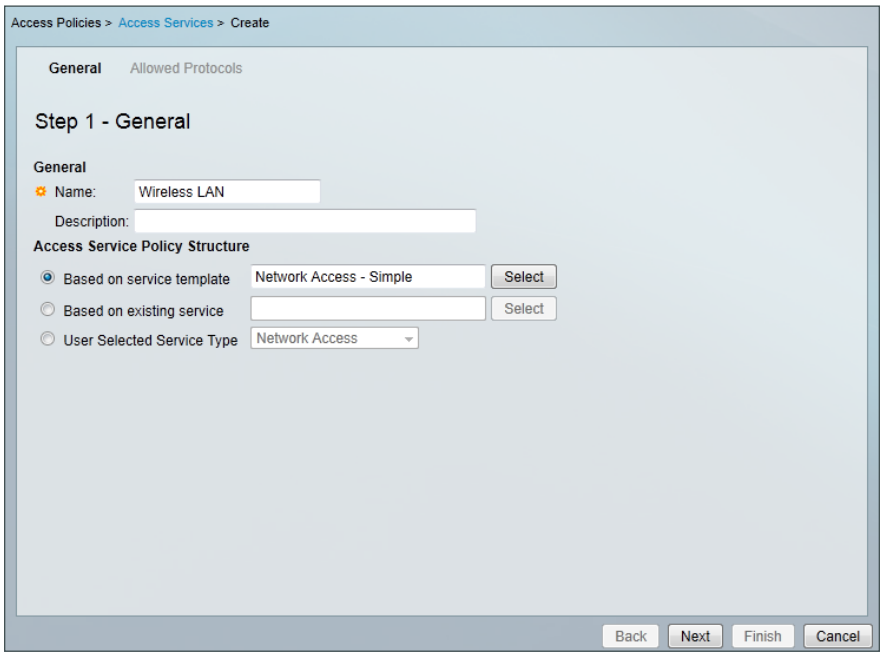


Procedure 4 Create the network access policy

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

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

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



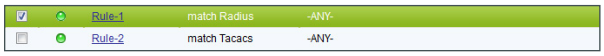
Step 4: On the Allowed Protocols pane, ensure **Allow PEAP** and **Allow EAP-Fast** are selected, and then click **Finish**.

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

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

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

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



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**.

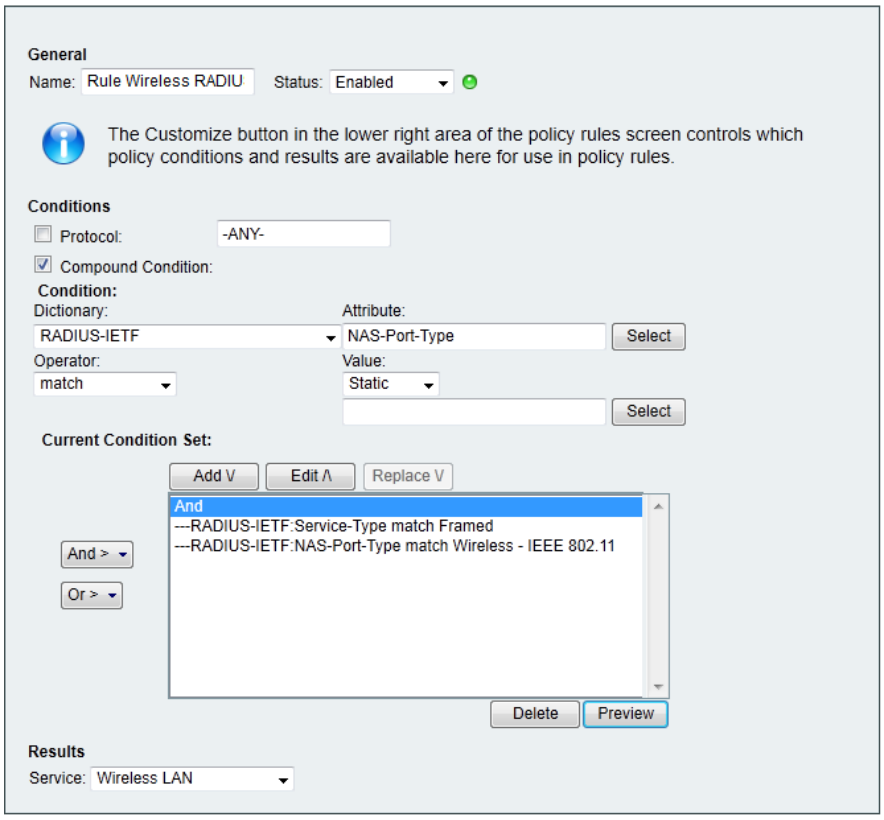
Step 14: In the **Value** box, select **Framed**, and then click **Add V**.

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**.



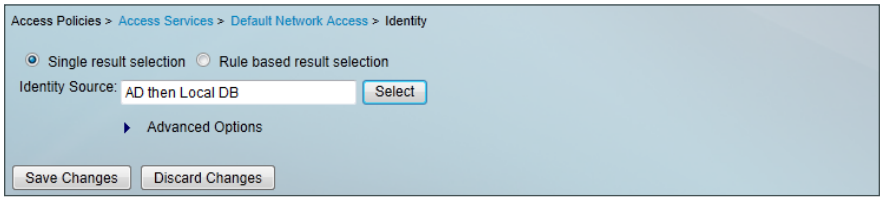
Step 19: On the Service Selection Rules pane, click **Save Changes**.

Procedure 5 Modify the network access policy

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

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

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



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

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

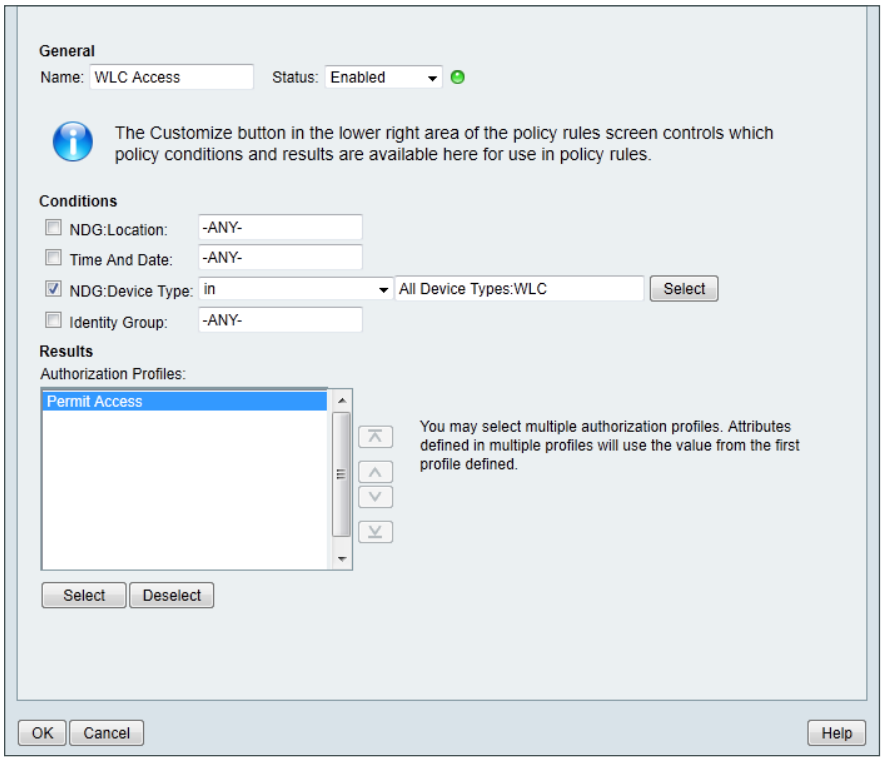
Step 5: Using the arrow buttons, move **NDG:Device Type** from the **Available** list to the **Selected** list, and then click **OK**.

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**.



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**.

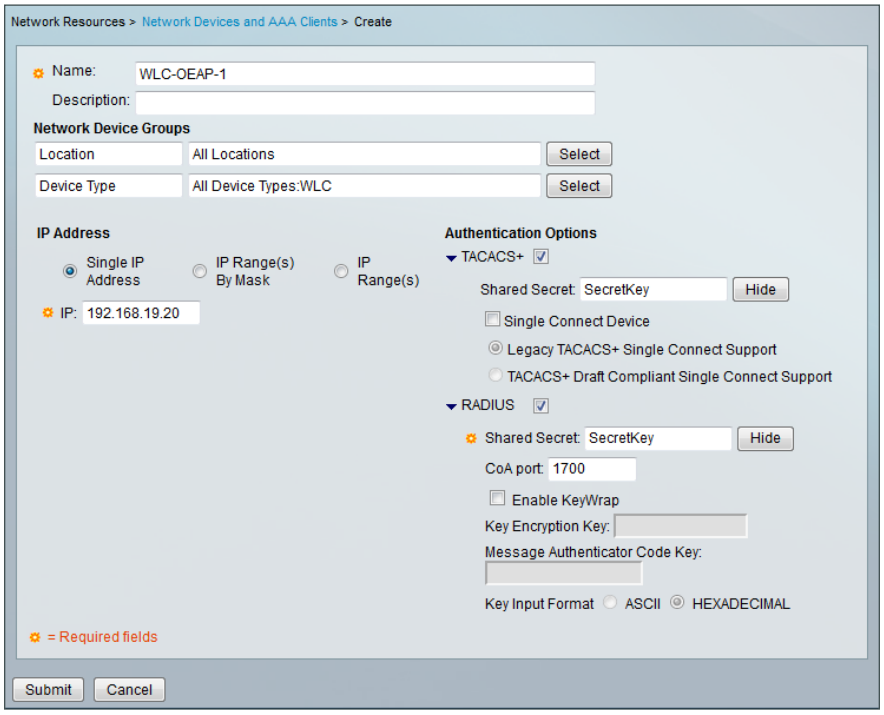
Step 4: In the **IP** box, enter the WLC's management interface IP address. (Example: 192.168.19.20)

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)



PROCESS

Configuring Internet Edge

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

Procedure 1 Configure the DMZ switch

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

```
vlan 1119
 name WLAN_Mgmt
```

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

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

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

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

Procedure 2 Configure the DMZ interface

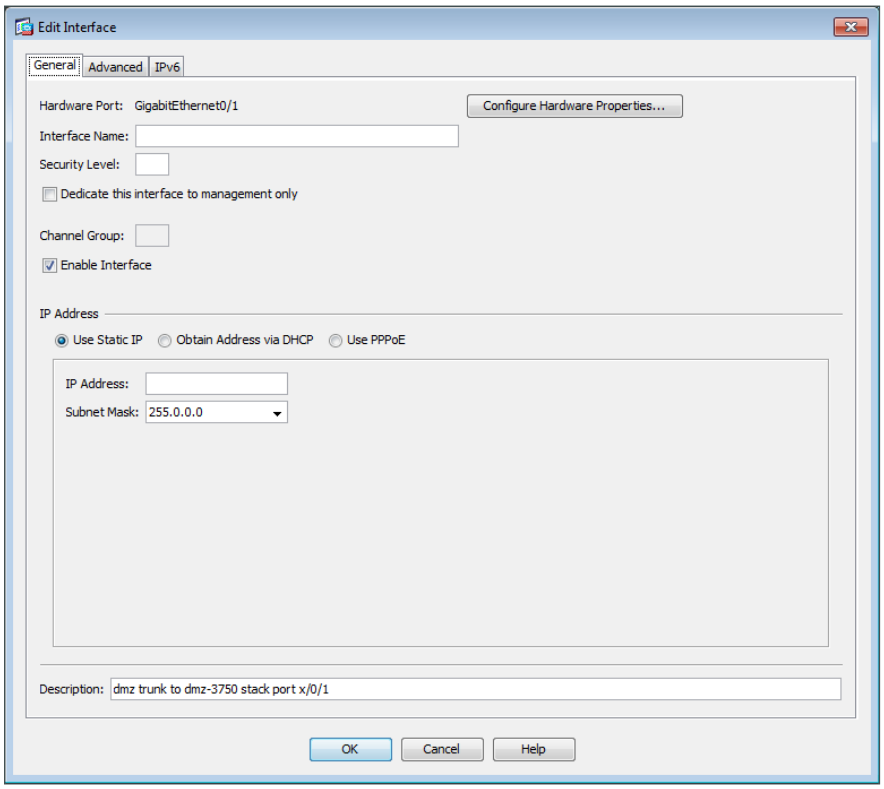
Typically, the firewall DMZ is a portion of the network where traffic to and from other parts of the network is tightly restricted. Organizations place network services in a DMZ for exposure to the Internet; these services are typically not allowed to initiate connections to the inside network, except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

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

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

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

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



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

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

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

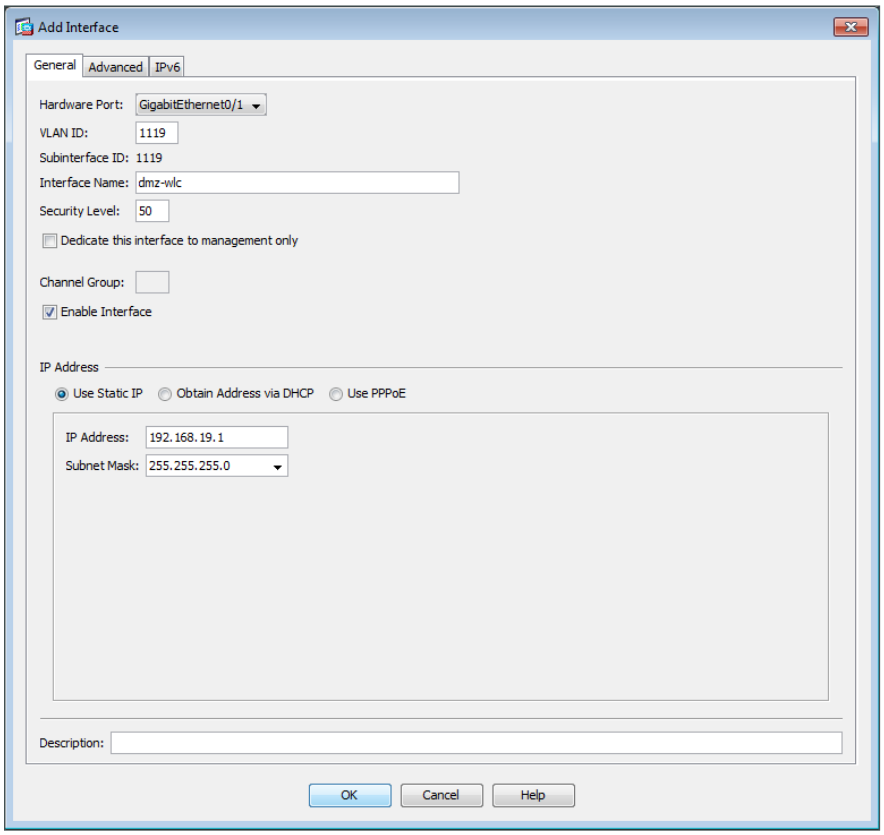
Step 7: In the **Subinterface ID** box, enter the VLAN number for the DMZ VLAN. (Example: 1119)

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

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

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

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



Procedure 3 Configure address translation

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

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

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

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

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

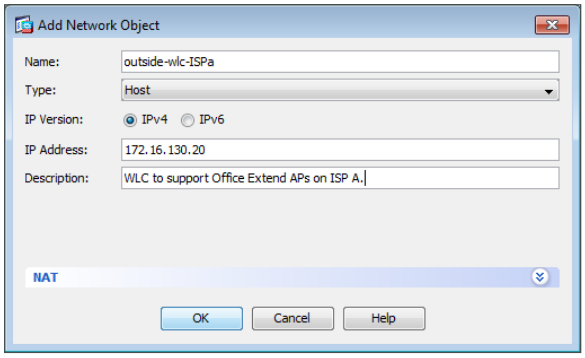
Step 1: Navigate to **Configuration > Firewall > Objects > Network Objects/Groups**.

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

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

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

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



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

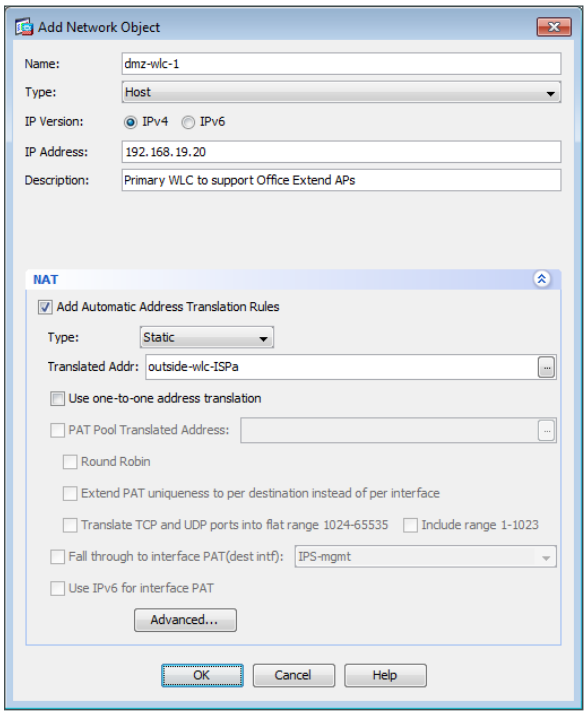
Step 5: In the Add Network Object dialog box, in the **Name box**, enter a description for the primary WLC's private DMZ IP address. (Example: dmz-wlc-1)

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

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

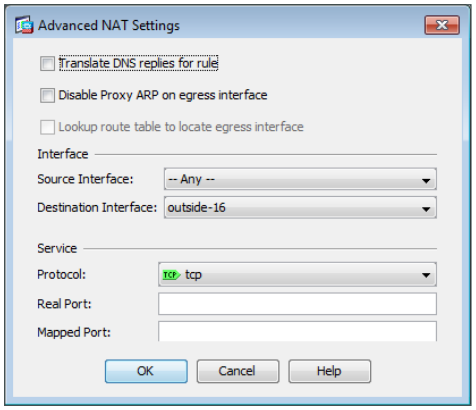
Step 8: Select **Add Automatic Address Translation Rules**.

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



Step 10: Click **Advanced**.

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



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

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

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

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

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

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

Procedure 4 Configure security policy

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

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

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

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

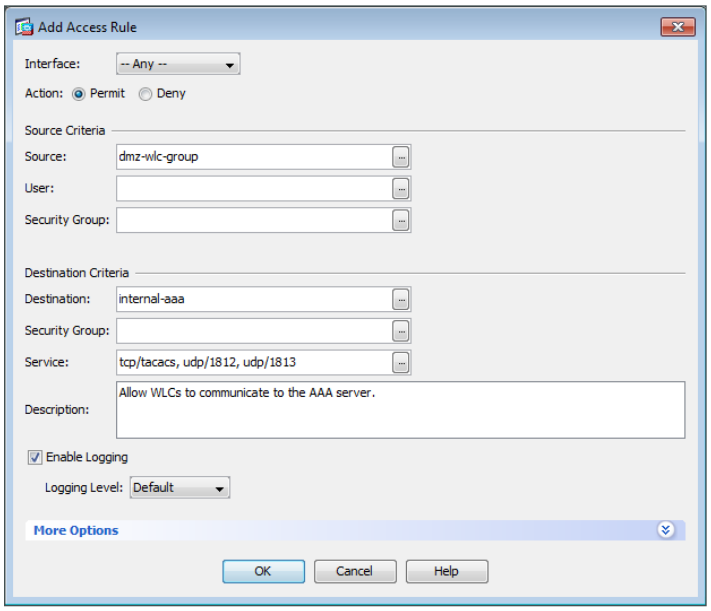
Step 4: In the Internet Access Rule dialog box, in the **Interface** list, select **–Any–**.

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

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

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

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



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

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

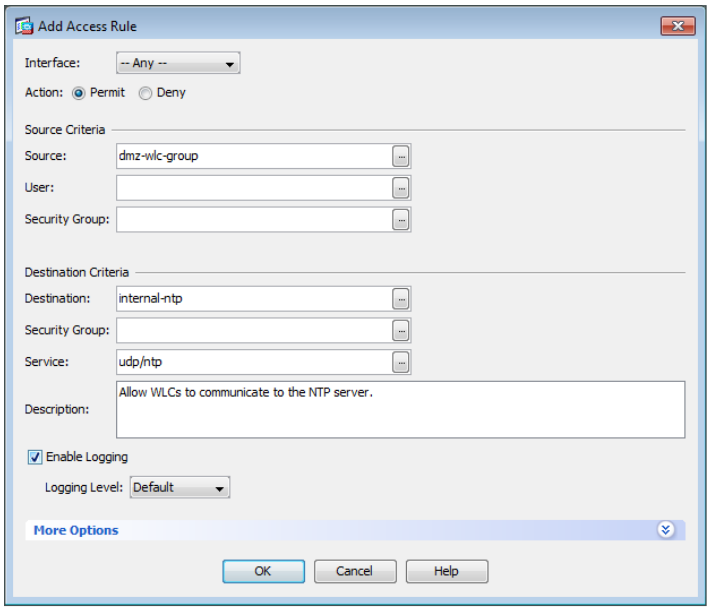
Step 10: In the Internet Access Rule dialog box, in the **Interface** list, select **–Any–**.

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

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

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

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



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

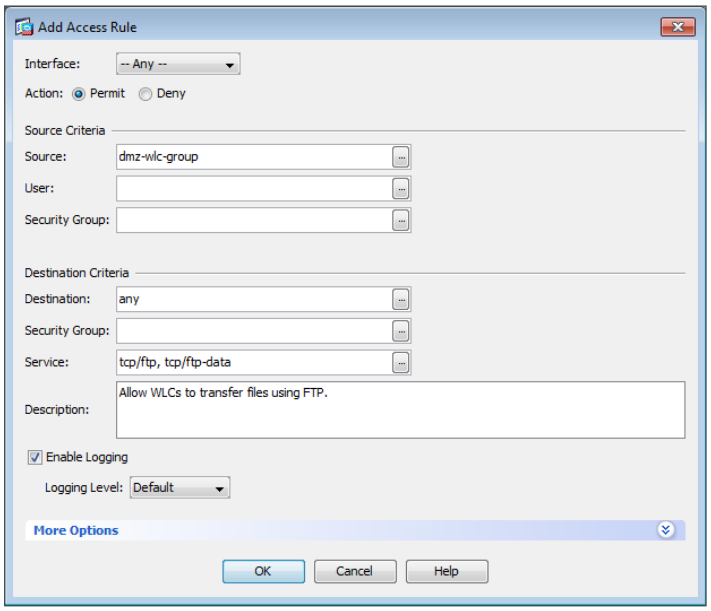
Step 15: Click **Add > Insert**.

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

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

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

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



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

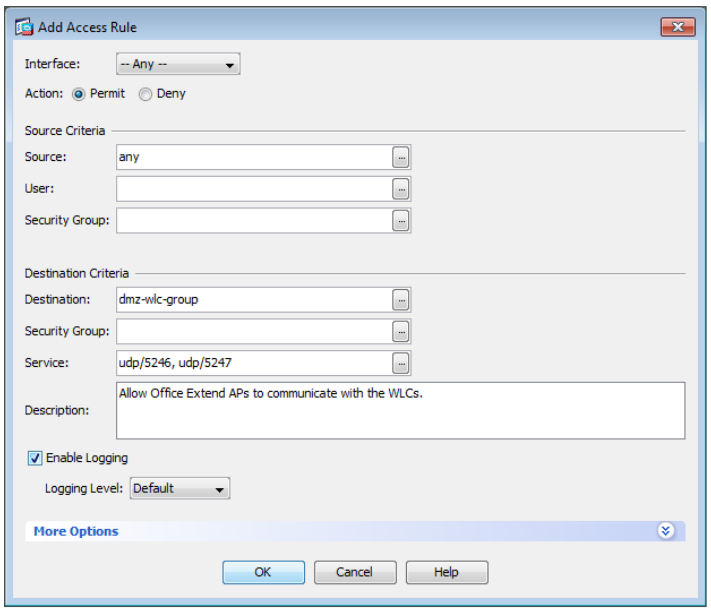
Step 20: Click **Add > Insert**.

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

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

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

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



Step 25: Click **Apply**.

PROCESS

Configuring LAN Distribution Switch

1. Configure the distribution switch

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
 macro apply EgressQoS
 logging event link-status
 logging event trunk-status
 no shutdown
```

PROCESS

Configuring WLC

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

Procedure 1 Configure the WLC platform

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

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

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

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

Step 2: Enter an administrator username and password.

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

```
Enter Administrative User Name (24 characters max): admin
Enter Administrative Password (24 characters max): *****
Re-enter Administrative Password : *****
```

Step 3: Use DHCP for the service port interface address.

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

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

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

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

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

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

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

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

```
Enable HA [yes][NO]: NO
```

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

```
Virtual Gateway IP Address: 192.0.2.1
```

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

```
Multicast IP Address: 239.40.40.40
```

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

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

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

```
Network Name (SSID): WLAN-Data
Configure DHCP Bridging Mode [yes][NO]: NO
```

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

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

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

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

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

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

Step 15: Enable all wireless networks.

```
Enable 802.11b network [YES][no]: YES
Enable 802.11a network [YES][no]: YES
Enable 802.11g network [YES][no]: YES
```

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

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

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

```
Configure a NTP server now? [YES][no]:YES
Enter the NTP server's IP address: 10.4.48.17
Enter a polling interval between 3600 and 604800 secs: 86400
```

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

```
Configuration correct? If yes, system will save it and reset. [yes][NO]: YES
Configuration saved!
Resetting system with new configuration
```

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

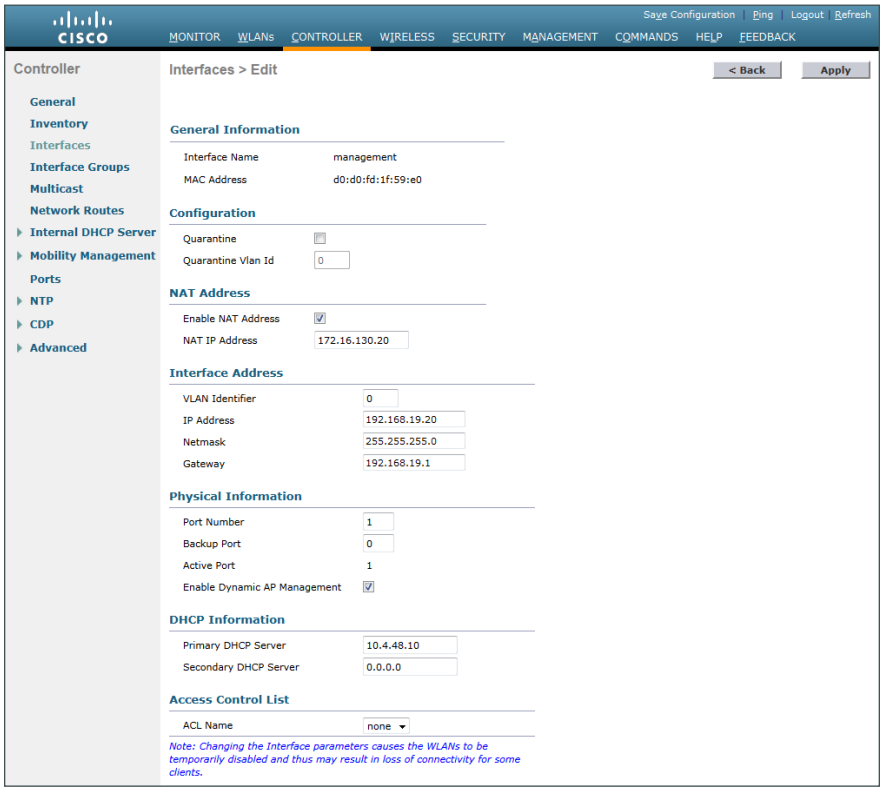
Procedure 2 Configure the WLC for NAT

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

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

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

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

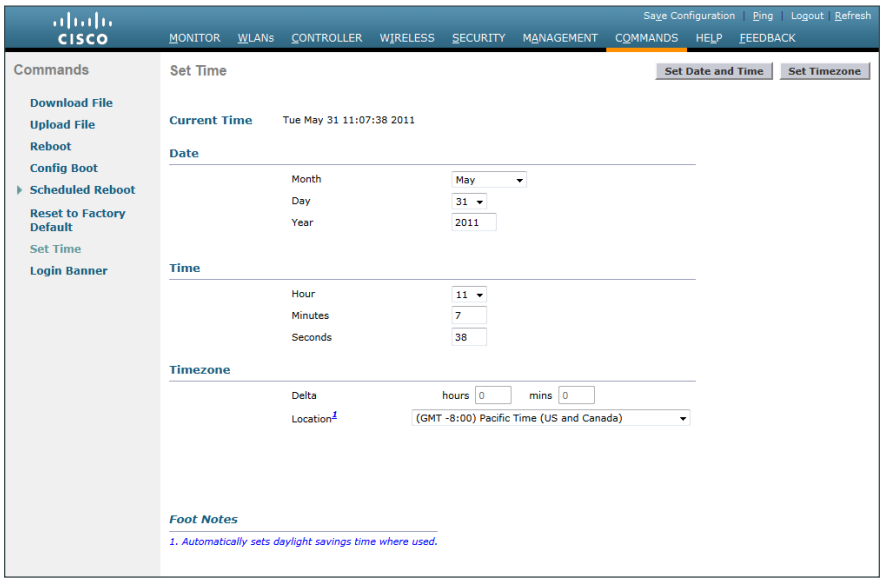


Procedure 3 Configure the time zone

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**.



Procedure 4 Configure SNMP

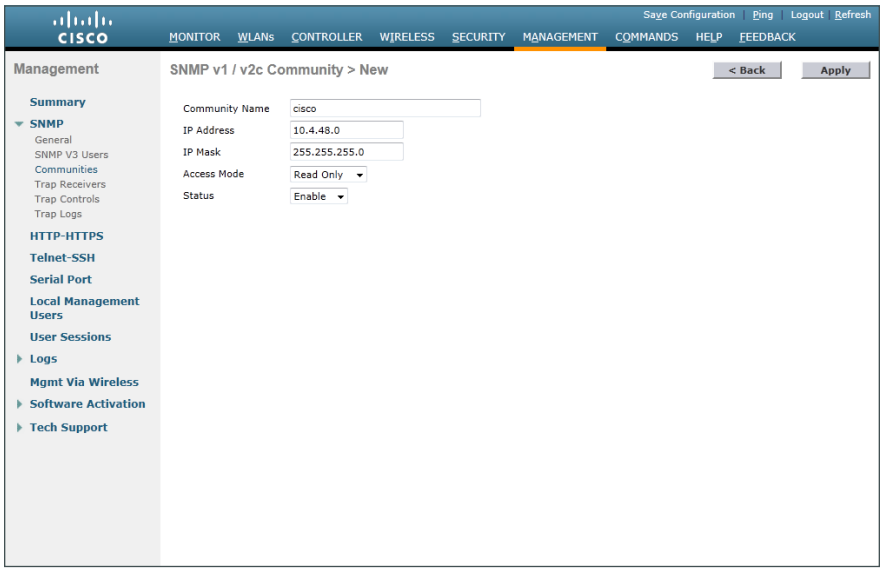
Step 1: In **Management > SNMP > Communities**, click **New**.

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**.



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

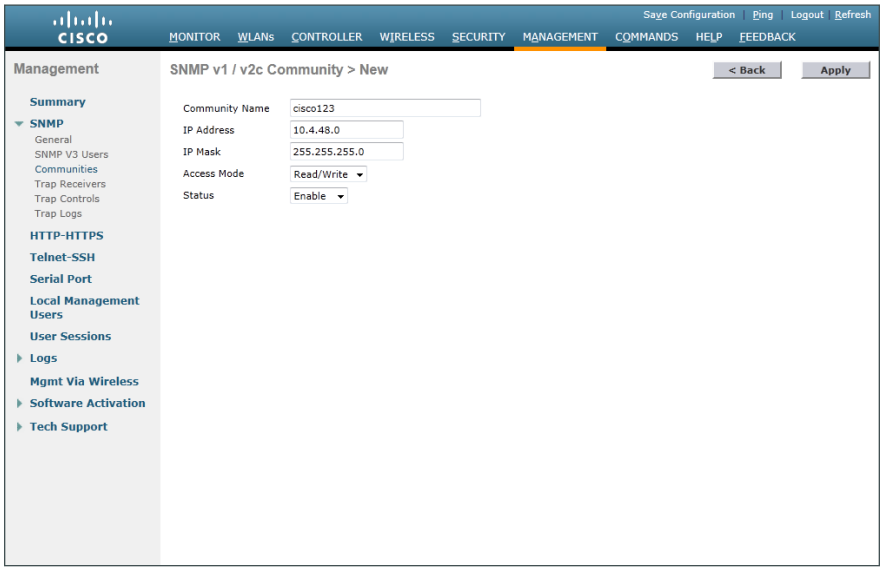
Step 7: Enter the **Community Name**. (Example: cisco123)

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**.

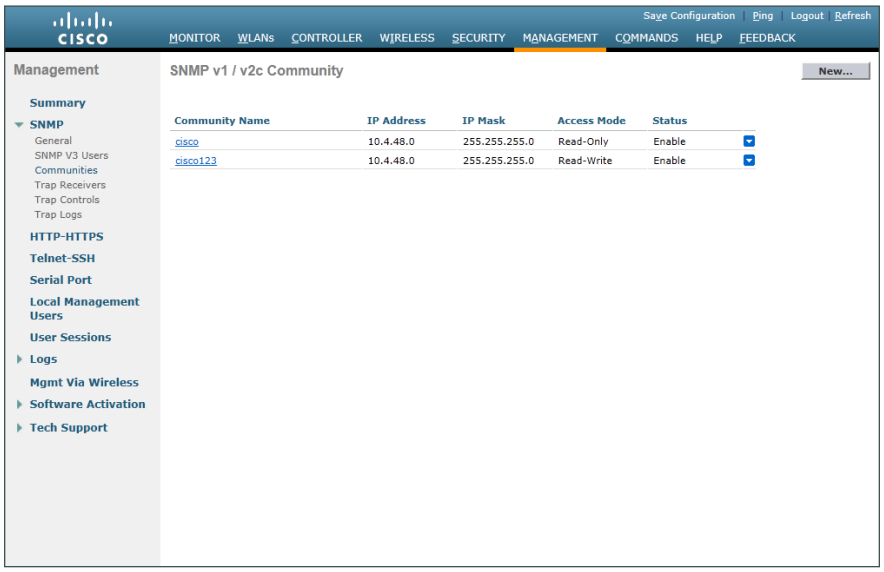


Step 12: Navigate to **Management > SNMP > Communities**.

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

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

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



Procedure 5 Limit what networks can manage the WLC

(Optional)

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

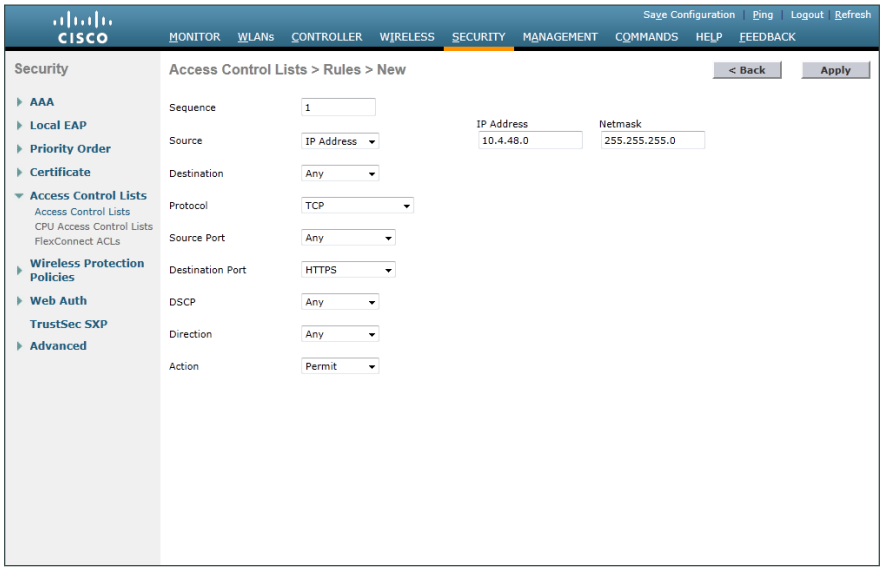
Step 1: In **Security > Access Control Lists > Access Control Lists**, click **New**.

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

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

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

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



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

Table 3 - Rule configuration values

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

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

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

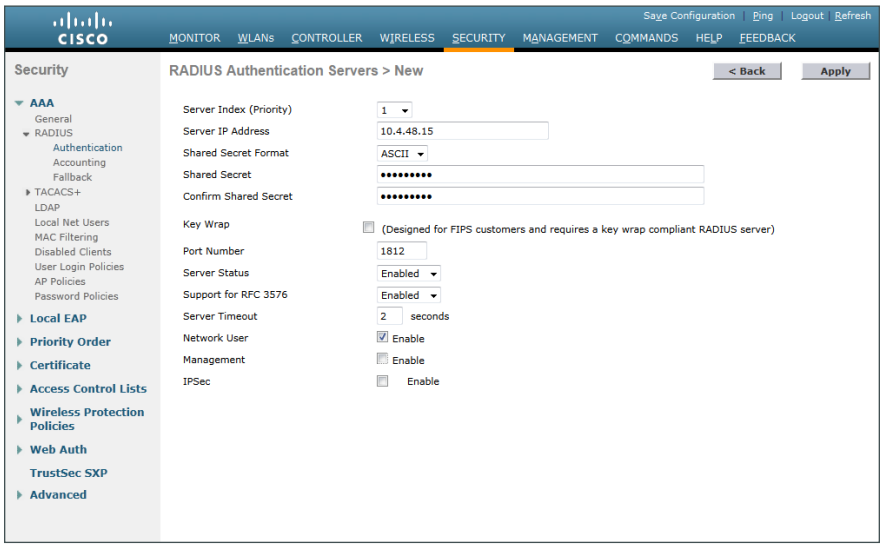
Procedure 6 Configure wireless user authentication

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

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

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

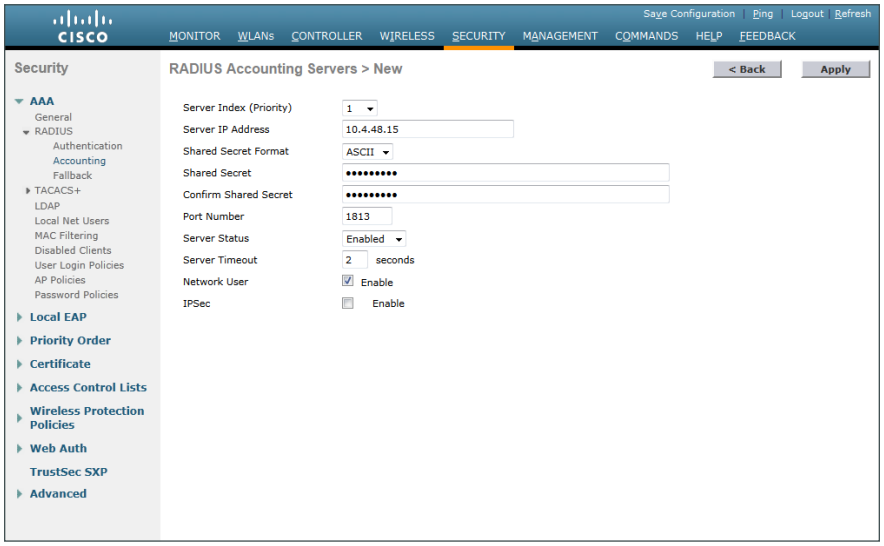
Step 4: To the right of Management, clear **Enable**, and then click **Apply**.



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)



Procedure 7 Centralize management authentication

(Optional)

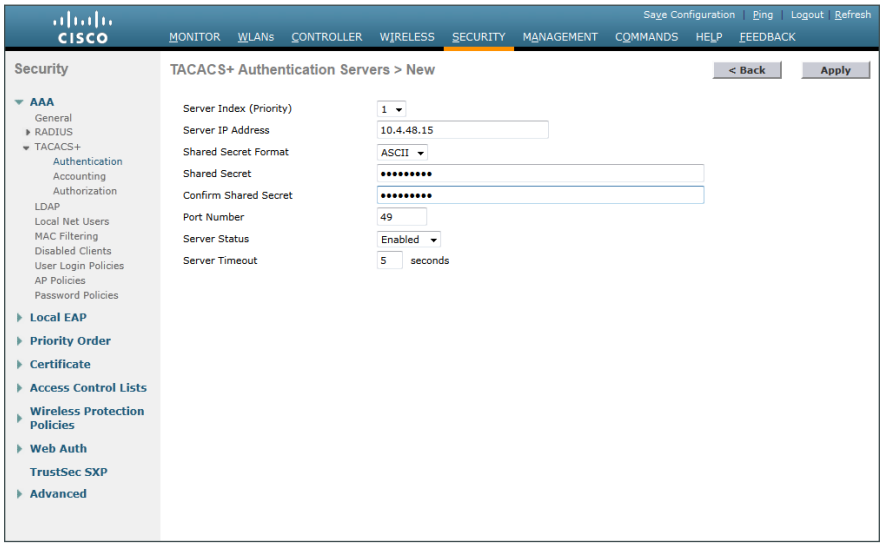
You can use this procedure to deploy centralized management authentication by configuring the authentication, authorization, and accounting (AAA) service. If you prefer to use local management authentication, skip this procedure.

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)

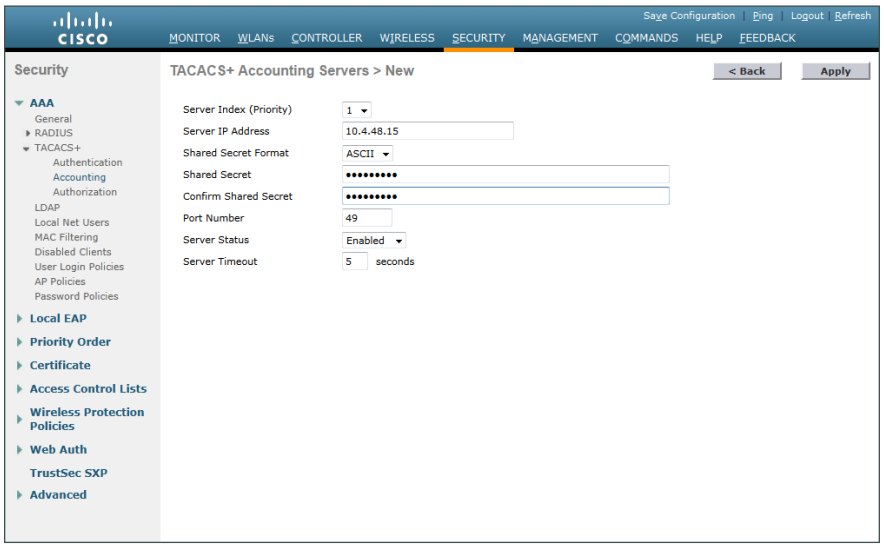
Step 3: Enter and confirm the **Shared Secret**, and then click **Apply**. (Example: SecretKey)



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

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

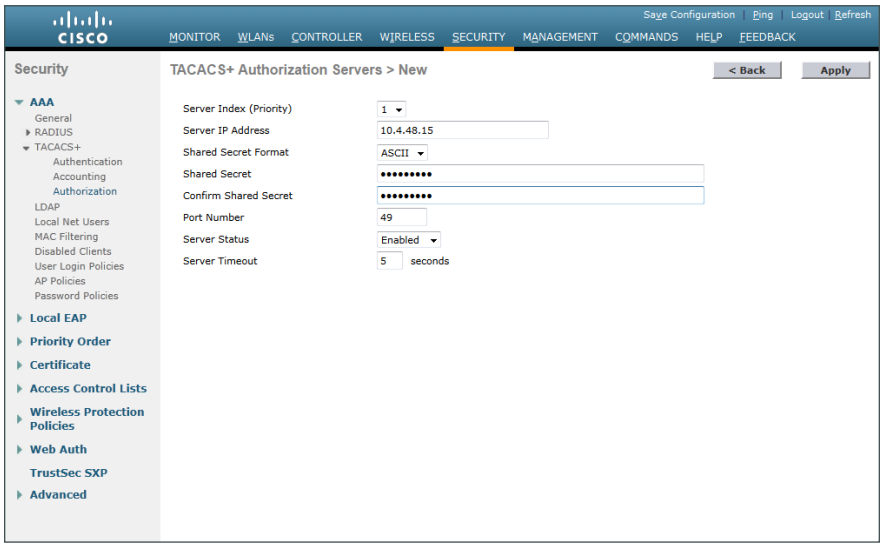
Step 6: Enter and confirm the **Shared Secret**, and then click **Apply**. (Example: SecretKey)



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)

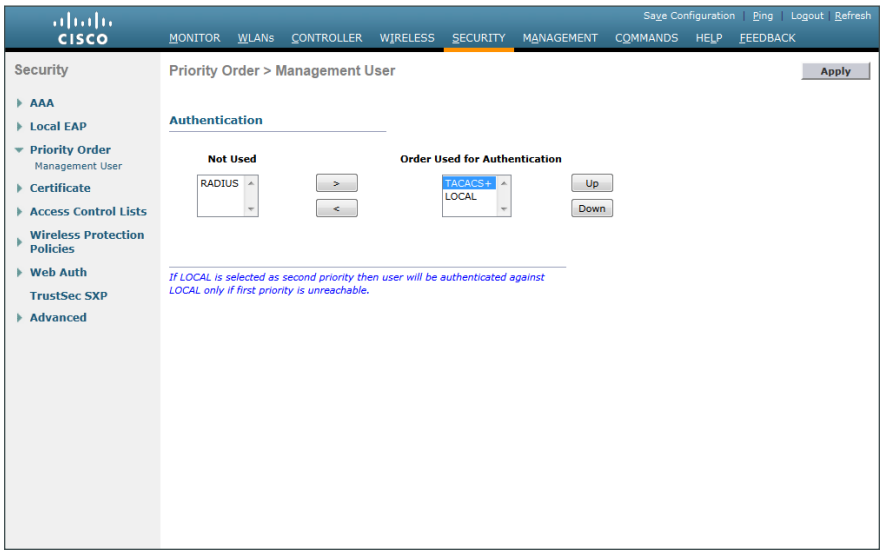


Step 10: Navigate to **Security > Priority Order > Management User.**

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**.



PROCESS

Configuring Voice/Data Connectivity

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

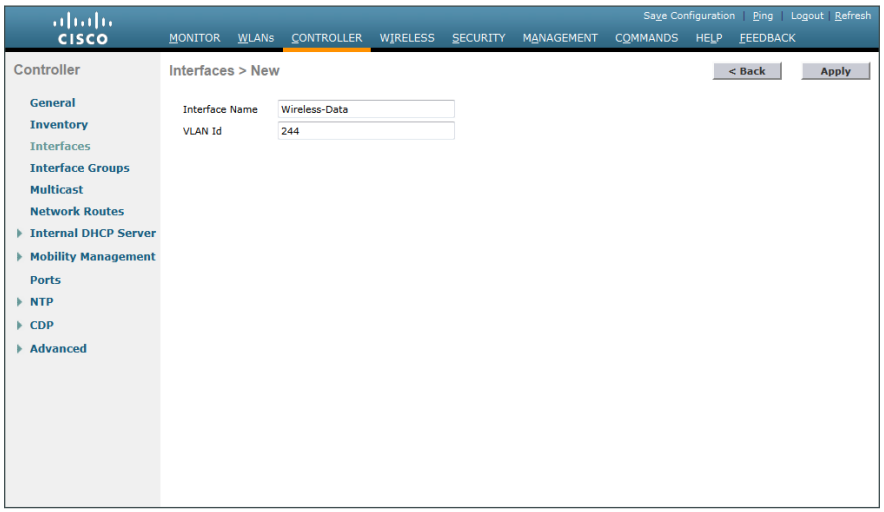
The Cisco OfficeExtend Access Point supports a maximum of two wireless LANs and one remote LAN. Configure the SSIDs to separate voice and data traffic, which is essential in any good network design in order to ensure proper treatment of the respective IP traffic, regardless of the medium it is traversing.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

Procedure 1 Create the wireless LAN data interface

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

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

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



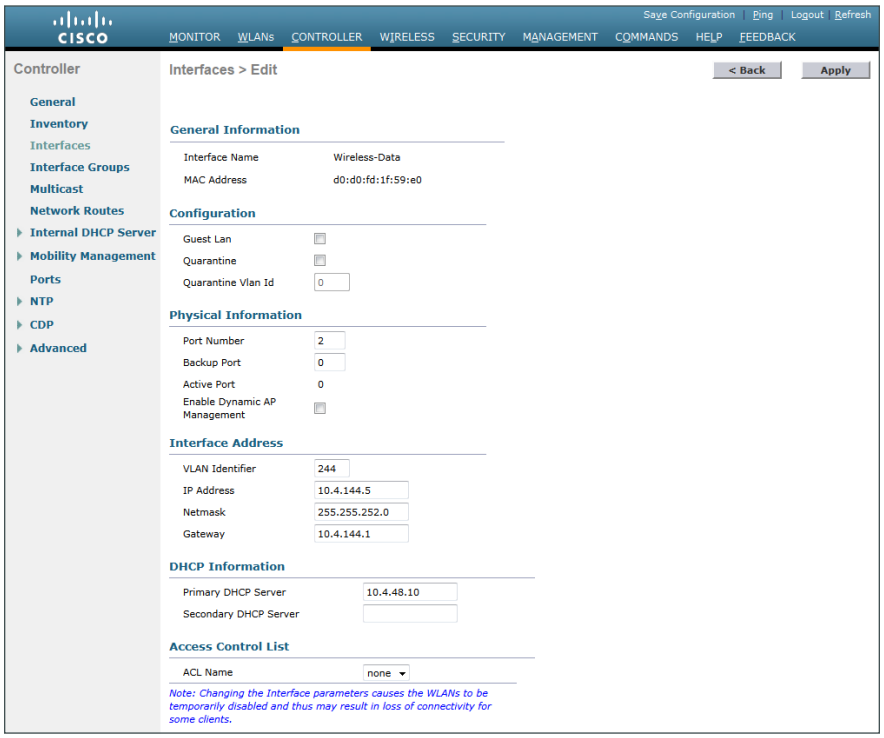
Step 4: In the **Port Number** box, enter the WLC interface that connects to the LAN distribution switch. (Example: 2)

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)



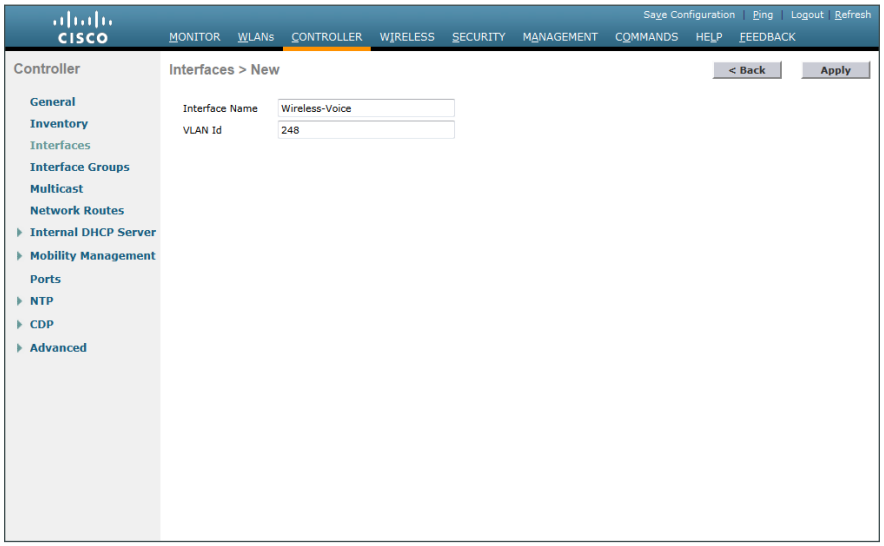
Procedure 2 Create the wireless LAN voice interface

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)



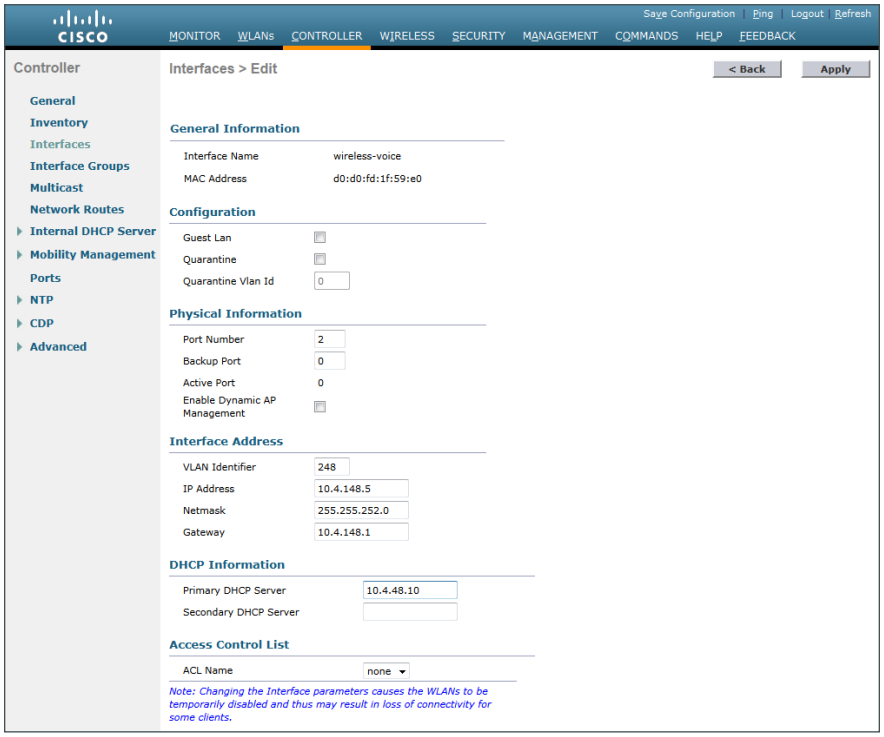
Step 4: In the **Port Number** box, enter the WLC interface that connects to the LAN distribution switch. (Example: 2)

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)



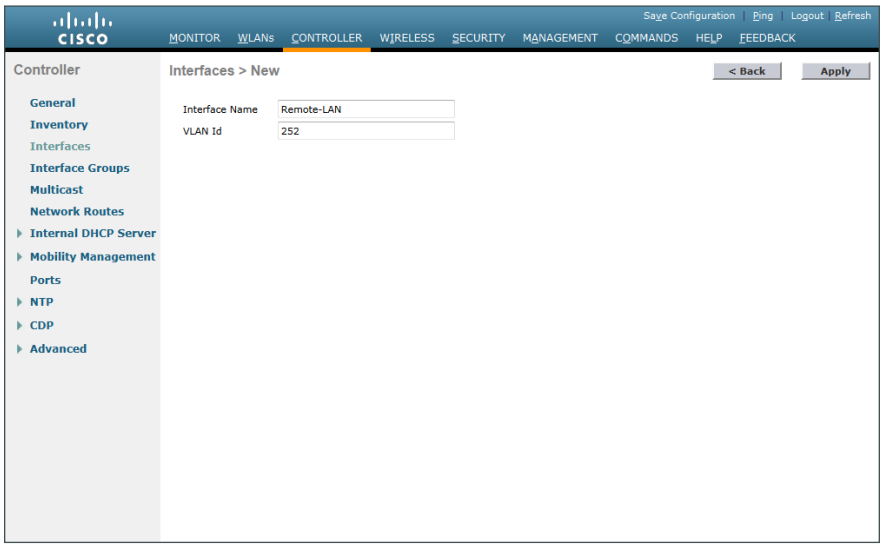
Procedure 3 Create the remote LAN interface

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)



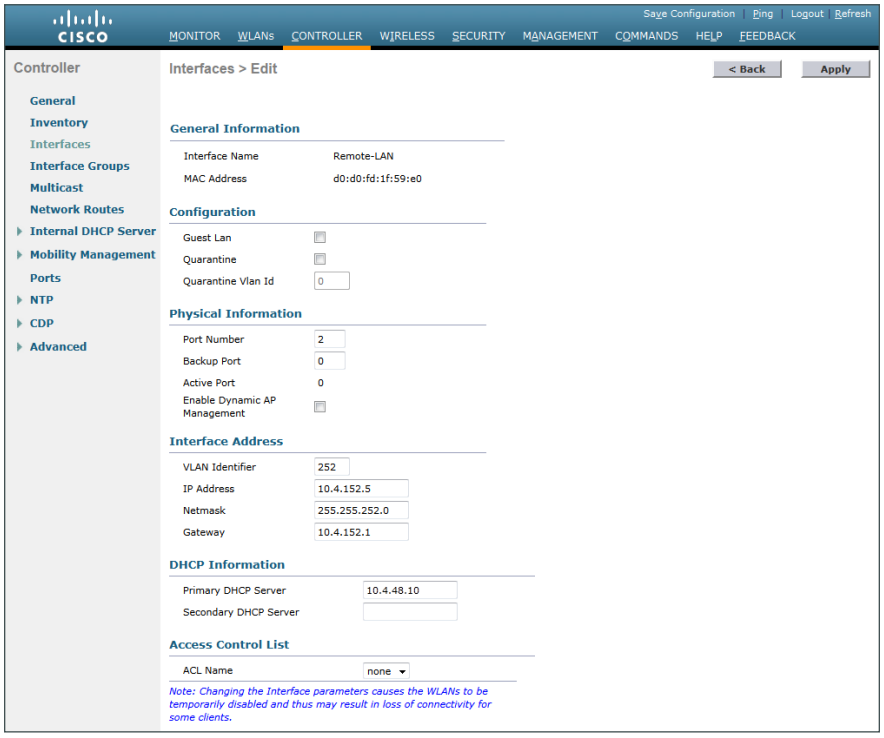
Step 4: In the **Port Number** box, enter the WLC interface that connects to the LAN distribution switch. (Example: 2)

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)

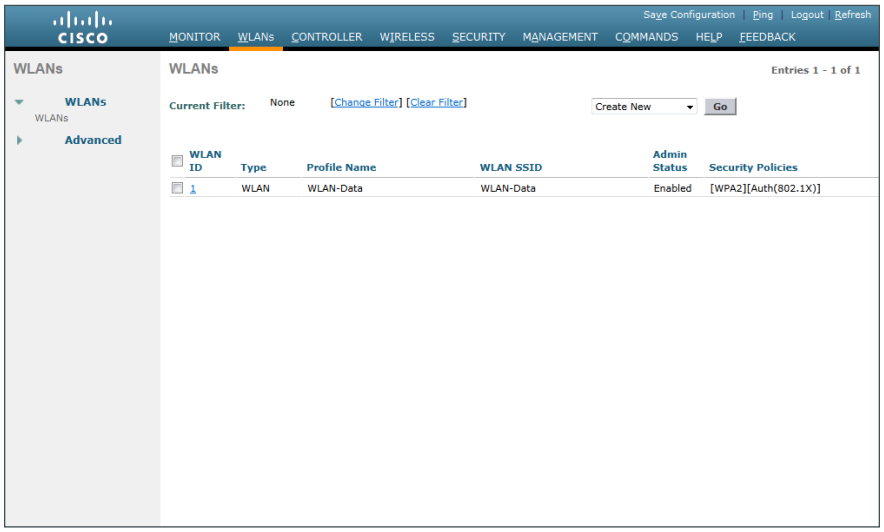


Procedure 4 Configure the data wireless LAN

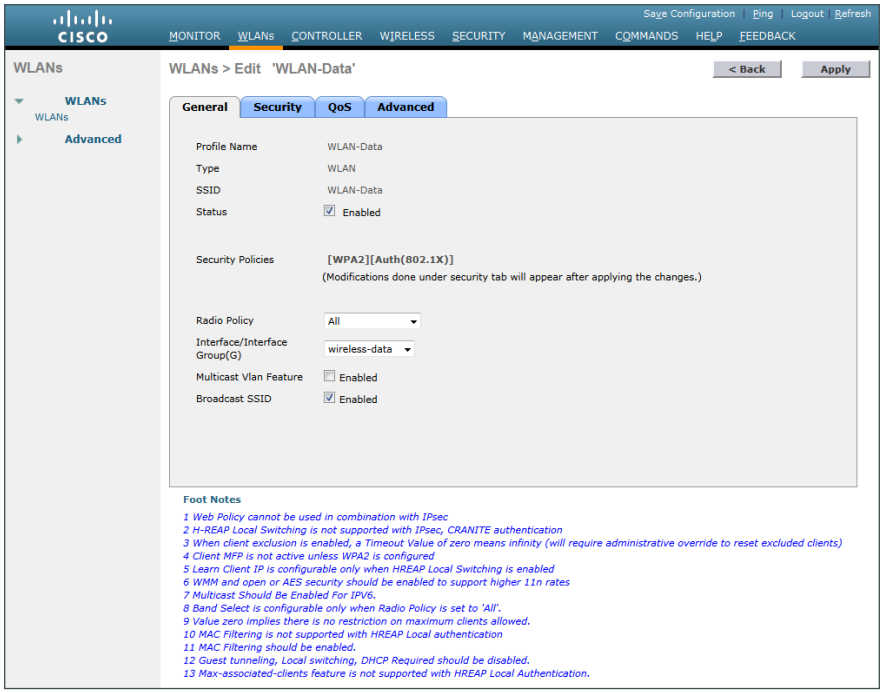
Wireless data traffic is different from voice traffic in that it can more efficiently handle delay and jitter as well as greater packet loss. For the data wireless LAN, keep the default QoS settings and segment the data traffic onto the data wired VLAN.

Step 1: Navigate to **WLANs**.

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

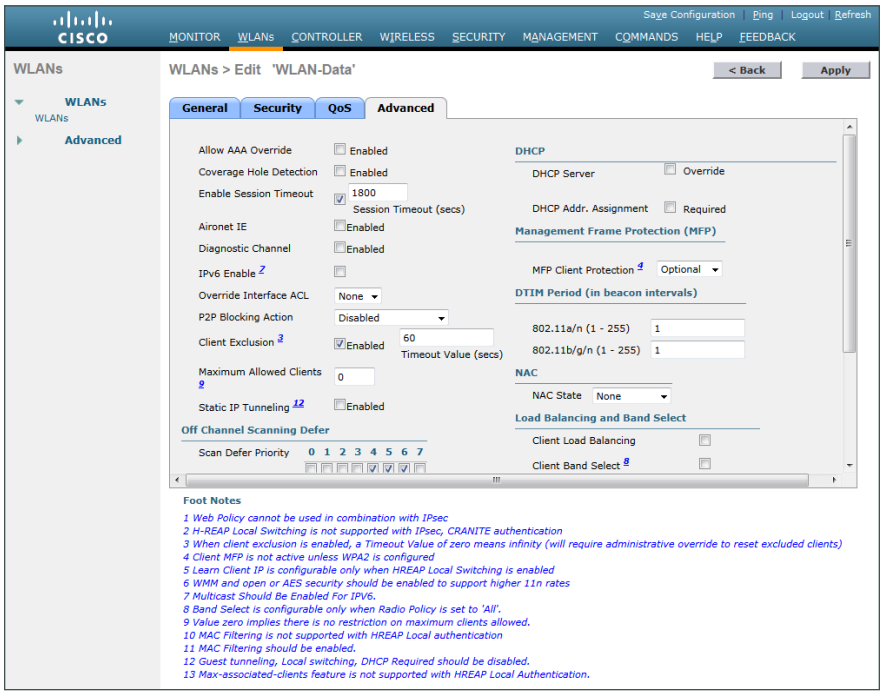


Step 3: On the General tab, in the **Interface** list, choose the interface created in Procedure 1. (Example: Wireless-Data)



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

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

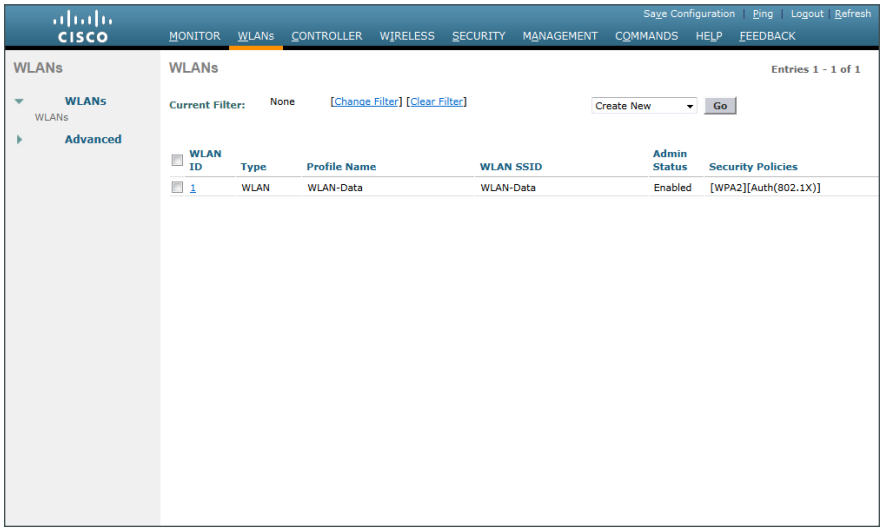


Procedure 5 Configure voice wireless LAN

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.

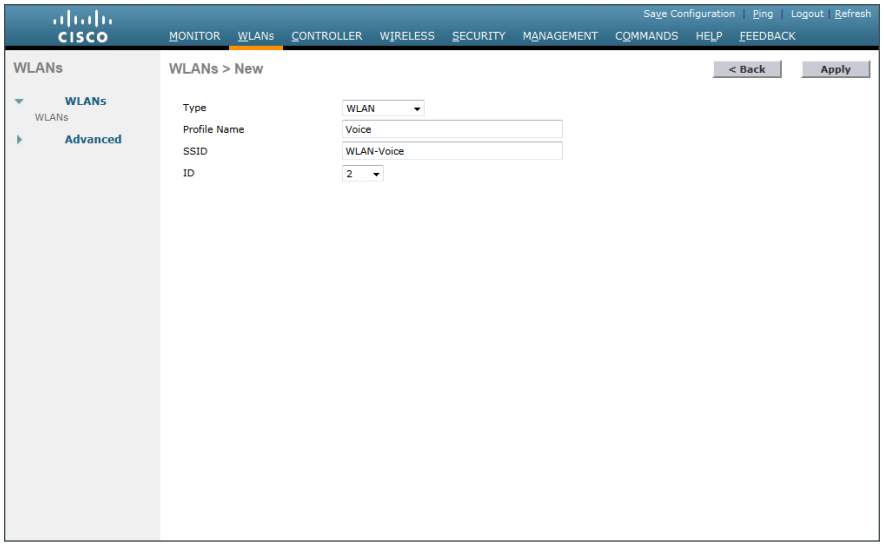
Step 1: Navigate to **WLANs**.

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



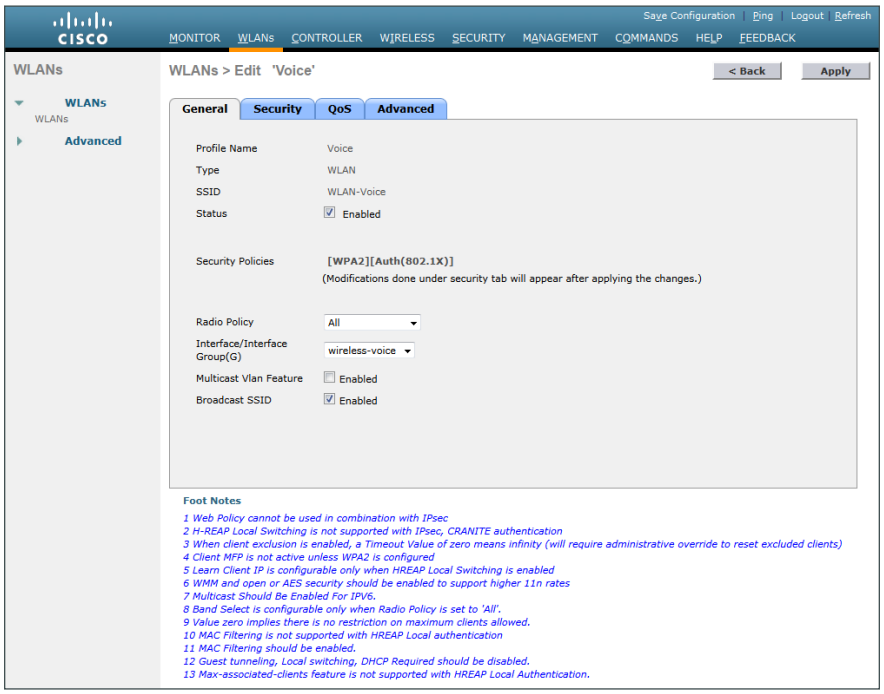
Step 3: Enter the **Profile Name**. (Example: Voice)

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

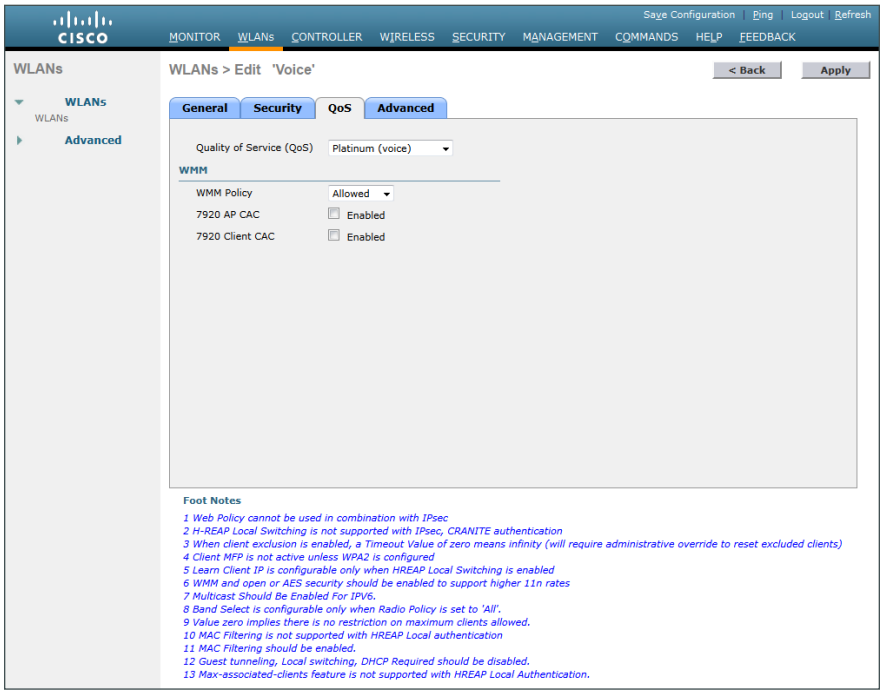


Step 5: On the General tab, to the right of **Status**, select **Enabled**.

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

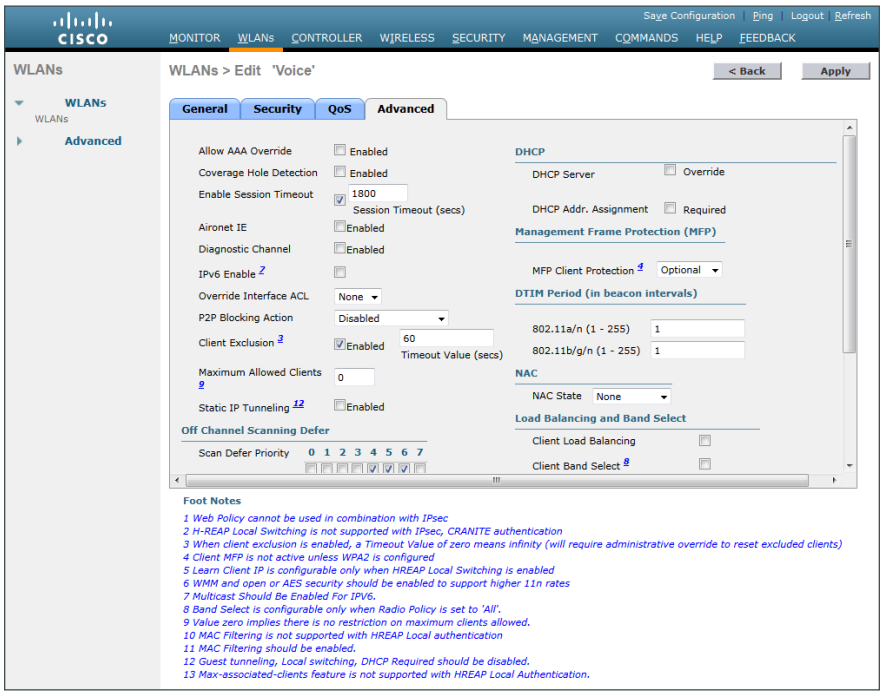


Step 7: Click the **QoS** tab, and in the **Quality of Service (QoS)** list, choose **Platinum**.



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

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

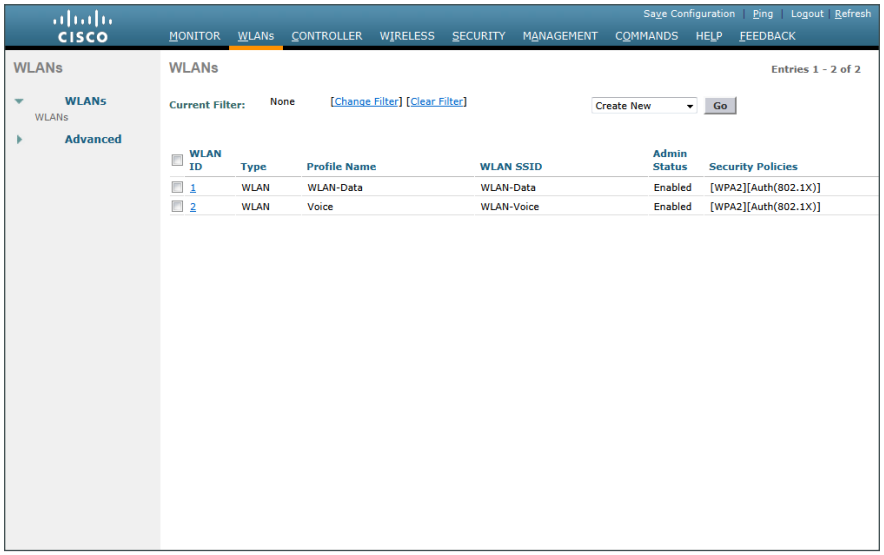


Procedure 6 Configure the remote LAN

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.

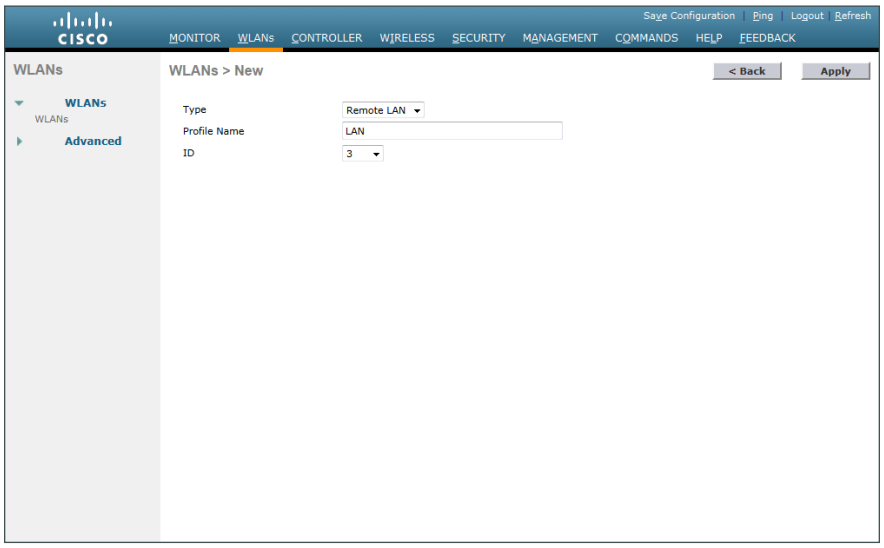
Step 1: Navigate to **WLANs**.

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



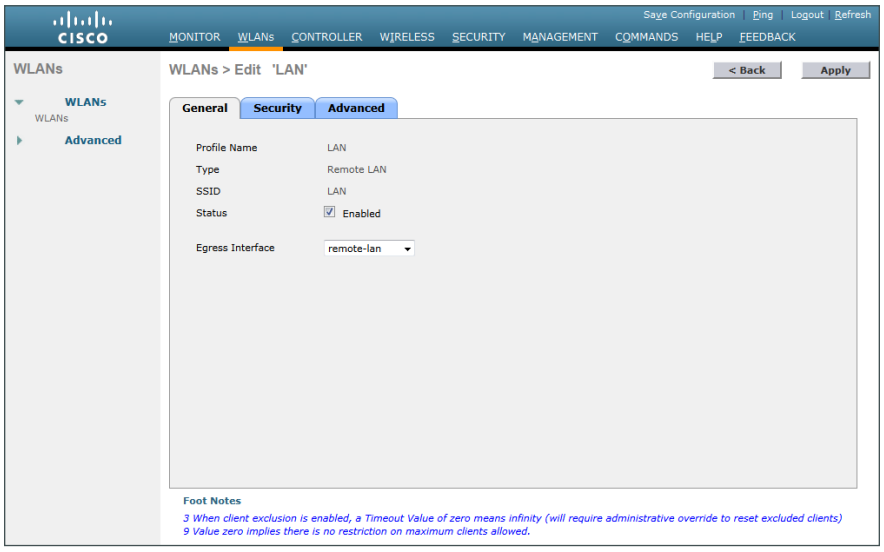
Step 3: In the **Type** list, choose **Remote LAN**.

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



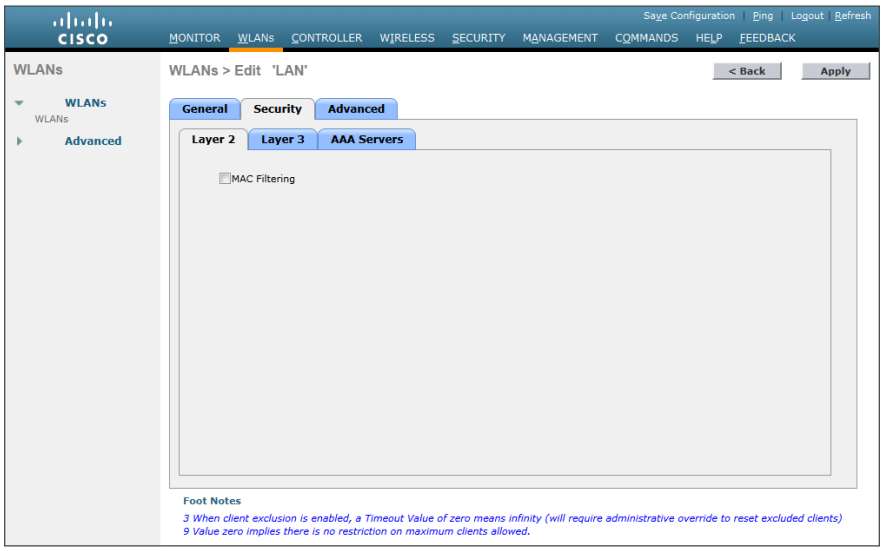
Step 5: On the General tab, to the right of **Status**, select **Enabled**.

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**.



PROCESS

Configuring AP Authentication

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

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

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

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

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

Procedure 1 Enable the default network device

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

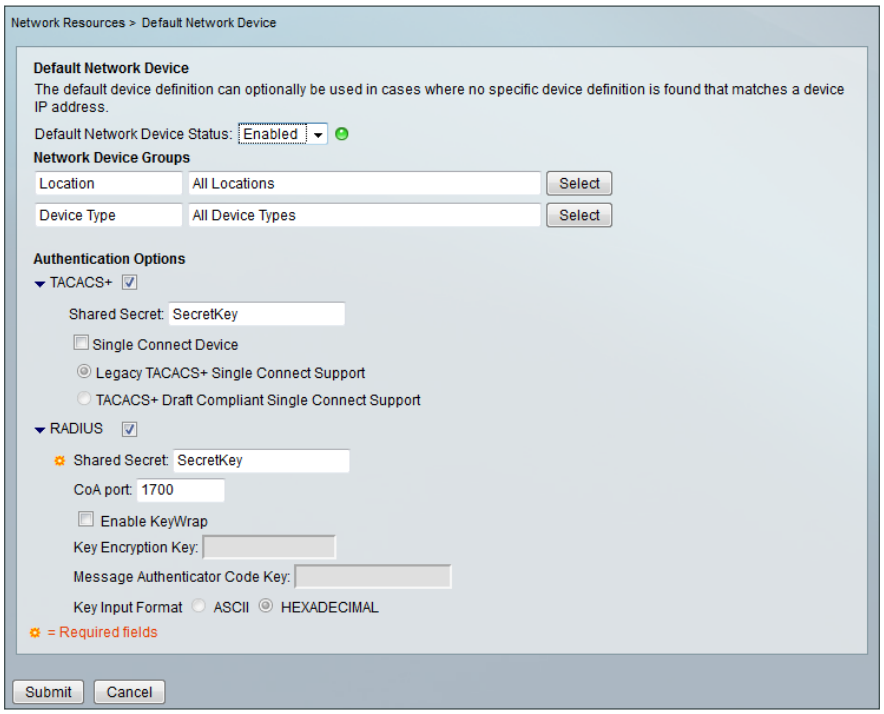
Step 1: Navigate to the Cisco Secure ACS Administration page. (Example: https://acs.cisco.local)

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

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

Step 4: Select **RADIUS**.

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



Procedure 2 Configure the access point account

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

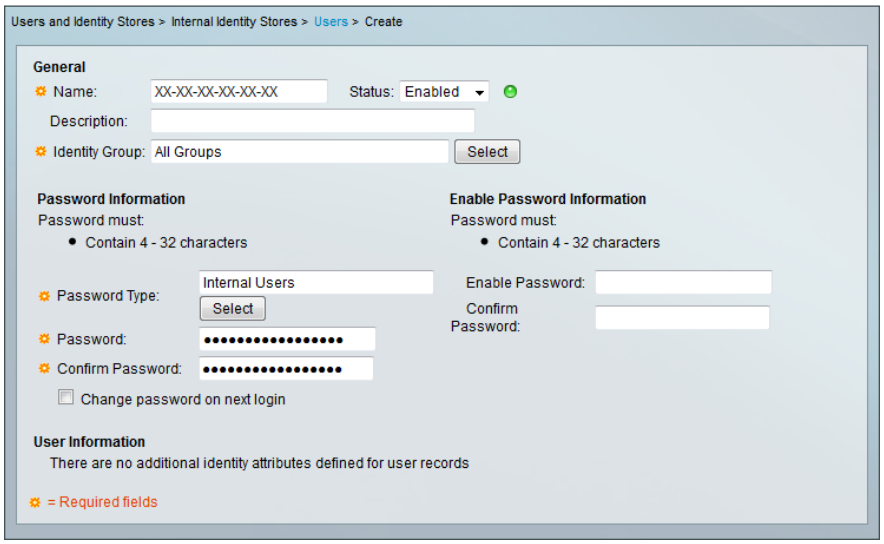
Step 1: In Cisco Secure ACS, navigate to **Users and Identity Stores > Internal Identity Stores > Users**.

Step 2: Click **Create**.

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

Step 4: Enter and confirm a password.

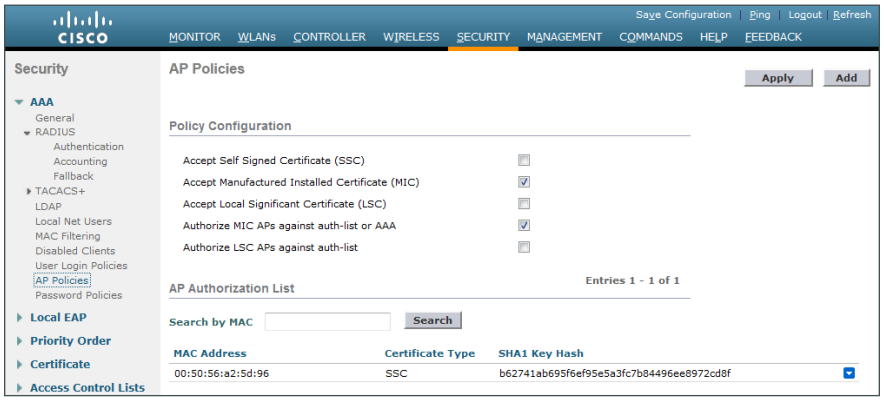
Step 5: Click **Submit**. This applies the changes.



Procedure 3 Configure AP authentication in the WLC

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

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

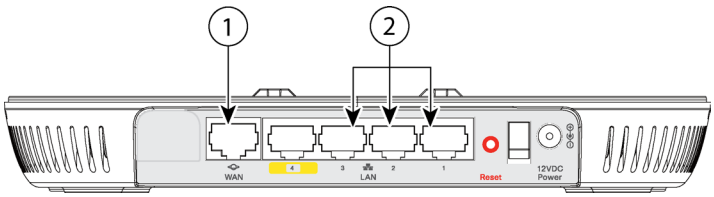


PROCESS

Configuring Cisco OfficeExtend AP

1. Configure the Cisco OfficeExtend AP

Procedure 1 Configure the Cisco OfficeExtend AP



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

Tech Tip

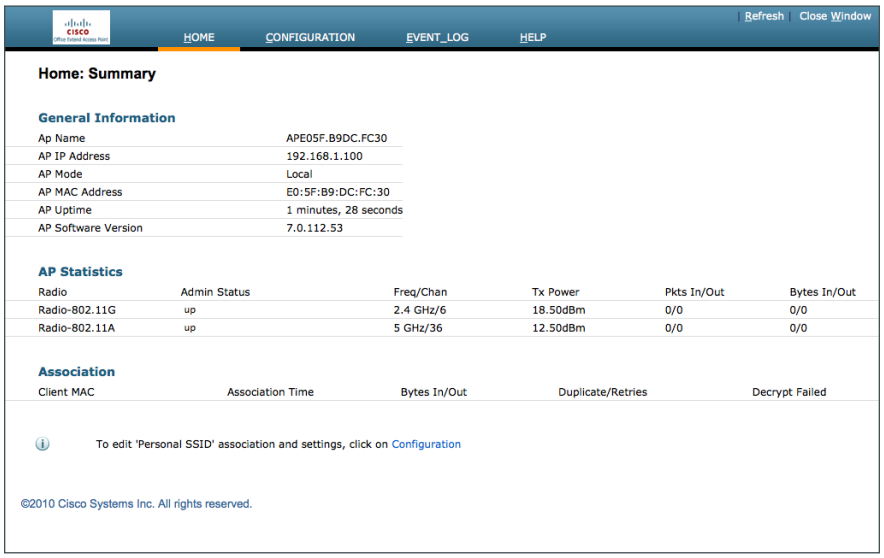
The Cisco OfficeExtend Access Point is not designed to replace the functionality of a home router, and it should not be connected directly to the service provider gateway.

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

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

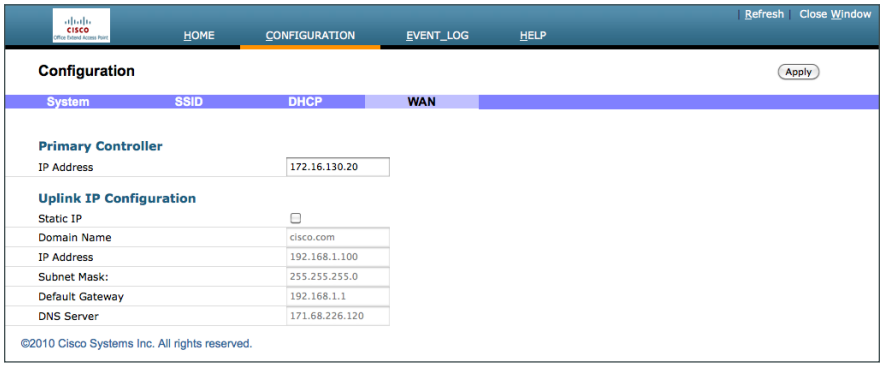
Step 4: Log in to the Administration page by using the default credentials **admin/admin**.

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



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)



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

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

Tech Tip

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

PROCESS

Enabling AP Radios

1. Configure the WLC

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

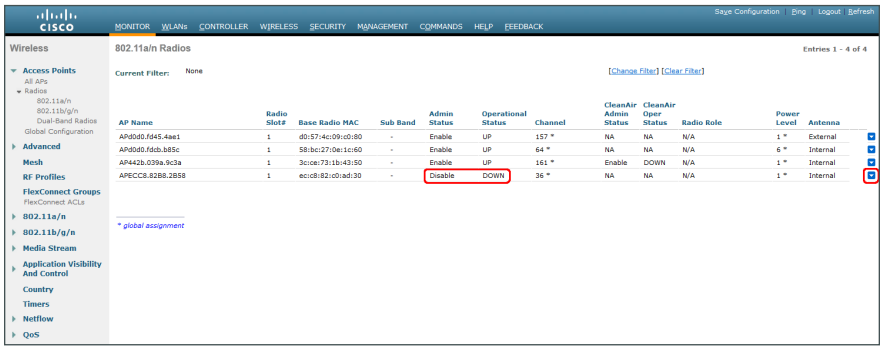
Procedure 1 Configure the WLC

First, enable the 5-GHz radio.

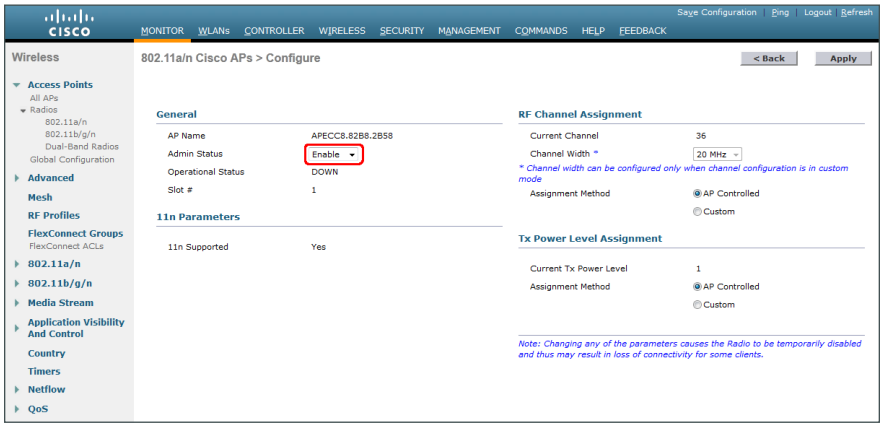
Step 1: On the primary WLC, navigate to **Wireless > Access Points > Radios > 802.11a/n**.

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

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



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



Next, enable the 2.4-GHz radio.

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

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

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

PROCESS

Configuring WLC Resiliency

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

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

The secondary controller, also called the *resilient controller*, provides resiliency in case the primary controller or Internet connection fails. Under normal operation, there will not be any Cisco OfficeExtend Access Points registered to the resilient controller.

Procedure 1 Configure the resilient WLC

On the resilient WLC, repeat the procedures in the "Configuring WLC" process.

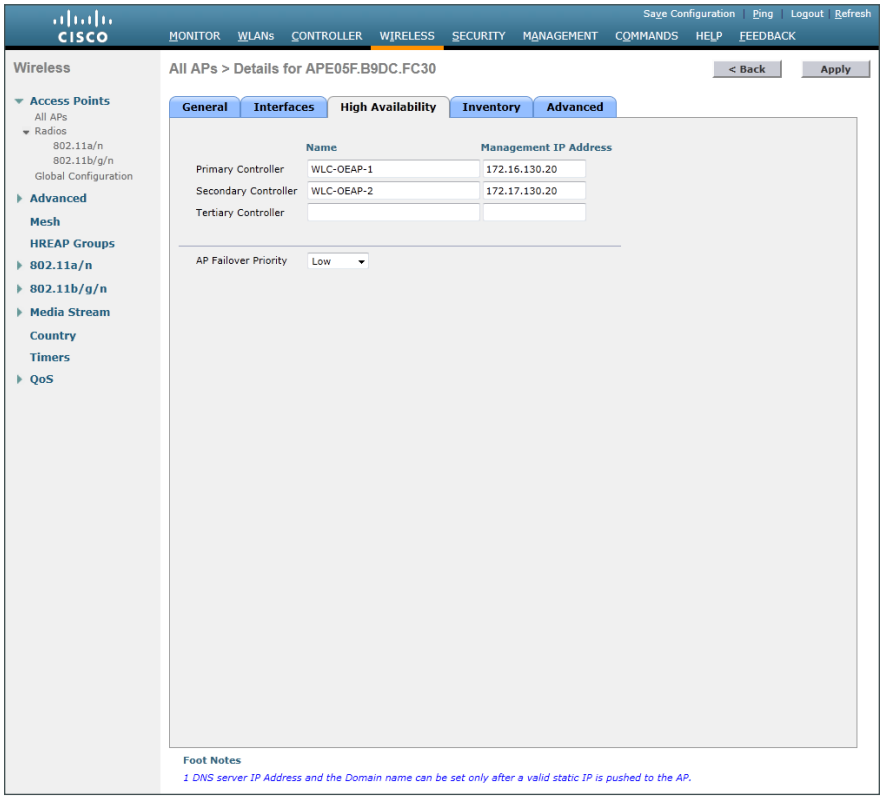
Procedure 2 Configure APs for resiliency

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

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

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

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



Appendix A: Product List

Wireless LAN OfficeExtend Access Points

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

Wireless LAN Controllers

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

Access Control

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

Internet Edge

Functional Area	Product Description	Part Numbers	Software
Firewall	Cisco ASA 5545-X IPS Edition - security appliance	ASA5545-IPS-K9	ASA 9.0(1) IPS 7.1(7) E4
	Cisco ASA 5525-X IPS Edition - security appliance	ASA5525-IPS-K9	
	Cisco ASA 5515-X IPS Edition - security appliance	ASA5515-IPS-K9	
	Cisco ASA 5512-X IPS Edition - security appliance	ASA5512-IPS-K9	
	Cisco ASA5512-X Security Plus license	ASA5512-SEC-PL	
	Firewall Management	ASDM	7.0(2)

Internet Edge LAN

Functional Area	Product Description	Part Numbers	Software
DMZ Switch	Cisco Catalyst 3750-X Series Stackable 24 Ethernet 10/100/1000 ports	WS-C3750X-24T-S	15.0(2)SE2 IP Base license

LAN Distribution Layer

Functional Area	Product Description	Part Numbers	Software
Modular Distribution Layer Virtual Switch Pair	Cisco Catalyst 6500 E-Series 6-Slot Chassis	WS-C6506-E	15.1(1)SY 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 24-port GbE SFP Fiber Module w/DFC4	WS-X6824-SFP-2T	
Modular Distribution Layer Switch	Cisco Catalyst 4507R+E 7-slot Chassis with 48Gbps per slot	WS-C4507R+E	3.4.0.SG(15.1-2SG) Enterprise Services license
	Cisco Catalyst 4500 E-Series Supervisor Engine 7-E, 848Gbps	WS-X45-SUP7-E	
	Cisco Catalyst 4500 E-Series 24-port GbE SFP Fiber Module	WS-X4624-SFP-E	
	Cisco Catalyst 4500 E-Series 12-port 10GbE SFP+ Fiber Module	WS-X4712-SFP+E	
Stackable Distribution Layer Switch	Cisco Catalyst 3750-X Series Stackable 12 GbE SFP ports	WS-C3750X-12S-E	15.0(2)SE2 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	

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.

B-0000315-1 08/13