cisco.



Cisco OfficeExtend TECHNOLOGY DESIGN GUIDE

August 2013



Table of Contents

Preface	1
CVD Navigator	2
Use Cases	2
Scope	2
Proficiency	2
Introduction	3
Technology Use Case	3
Use Case: Teleworker with Wireless Devices	
Design Overview	
Deployment Components	4
Design Models	5
Deployment Details	6
Deployment Details	6 6
Deployment Details Configuring Cisco Secure ACS Configuring Internet Edge	6
Deployment Details. Configuring Cisco Secure ACS Configuring Internet Edge Configuring LAN Distribution Switch.	
Deployment Details. Configuring Cisco Secure ACS Configuring Internet Edge Configuring LAN Distribution Switch Configuring WLC.	
Deployment Details. Configuring Cisco Secure ACS Configuring Internet Edge. Configuring LAN Distribution Switch Configuring WLC. Configuring Voice/Data Connectivity	6
Deployment Details. Configuring Cisco Secure ACS Configuring Internet Edge Configuring LAN Distribution Switch Configuring WLC Configuring Voice/Data Connectivity Configuring AP Authentication.	6
Deployment Details. Configuring Cisco Secure ACS Configuring Internet Edge. Configuring LAN Distribution Switch. Configuring WLC. Configuring Voice/Data Connectivity Configuring AP Authentication. Configuring Cisco OfficeExtend AP.	6
Deployment Details. Configuring Cisco Secure ACS Configuring Internet Edge Configuring LAN Distribution Switch Configuring WLC Configuring Voice/Data Connectivity Configuring AP Authentication Configuring Cisco OfficeExtend AP Enabling AP Radios	6
Deployment Details. Configuring Cisco Secure ACS . Configuring Internet Edge. Configuring LAN Distribution Switch. Configuring WLC . Configuring Voice/Data Connectivity . Configuring AP Authentication. Configuring Cisco OfficeExtend AP. Enabling AP Radios . Configuring WLC Resiliency .	6

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-classtransmit 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



To view the related CVD guides, click the titles or visit the following site: http://www.cisco.com/go/cvd

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.





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.

5

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	desian	parameters
rabic			Oniversar	acoign	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	



- 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 wireles

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)

PROCESS

6

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

Network Resources >	Network Device Groups > Devi	ice Type > Create		
Device Group Name: Description:	General WLC			
😛 Parent:	All Device Types		Select	
Required field	elds			
Submit Can	cel			

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.

	non Tasks Custom Attribute	s	
Common Tasks A	ttributes		
Attribute	Requirement	Value	
lanually Entered			_
Attribute	Requirement	Value	
role1	Mandatory	All	
Add A	Edit V Replace A Delet	e	
Attribute:			
Requirement: Ma	andatory 👻		
/alue: St	atic 👻		

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.

8

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

01				
General Name: Network Admin	Status: Ena	hled -	•	
Name. Network Admin	Status. Ena	bieu +		
The Custor policy conc	mize button in the low litions and results are	ver right ar e available	ea of the policy rules scree here for use in policy rules	n controls which
Conditions				
Identity Group:	in		oups:Network Admins	Select
NDG:Location:	-ANY-			
NDG:Device Type:	not in	✓ All De	vice Types:WLC	Select
Time And Date:	-ANY-			
Results				
Shell Profile: Level 15		Select		
K Cancel				Hel

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.

9

Step 9: Click Save Changes.

General				
Name: WLC Admin	Status: Ena	abled	▼ 😉	
The Custor policy cond	mize button in the lo litions and results ar	wer r e ava	ight area of the policy rules scree ailable here for use in policy rules	en controls which
Conditions				
Identity Group:	in	•	All Groups:Network Admins	Select
NDG:Location:	-ANY-			
NDG:Device Type:	in	•	All Device Types:WLC	Select
Time And Date:	-ANY-			
Results				
Shell Profile: WLC Shell			Select	

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.

Access Policies > Ac	cess Services > Cre	ate						
General A	Allowed Protocols							
Step 1 - Ge	eneral							
General								
Name:	Wireless LAN							
Description:								
Access Service	Policy Structure							
Based on s	ervice template	Network A	ccess - Simple	Select				
O Based on e	xisting service			Select				
O User Select	ed Service Type	Network A	CCESS -					
					Back	Next	Finish	Cancel

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.

 Image: Number of the second second

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 RADIO Status: Enabled V
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: Attribute:
RADIUS-IETF VAS-Port-Type Select
Operator: Value:
match - Static -
Current Condition Set:
Add V Edit A Replace V
And
RADIUS-IETF:Service-Type match Framed
And >RADIOS-IETP.NAS-Poil-Type match wheless - IEEE 802. 11
Or > -
Delete
Results
Service: Wireless LAN

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

Procedure 5 Modify the network access policy

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

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

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

Access Policies > Access Services > Default Network Acc	cess > Identity
Single result selection O Rule based result se	ection
Identity Source: AD then Local DB	Select
 Advanced Options 	
Save Changes Discard Changes	

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

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

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

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

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

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

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

The Custor policy cond	nize button in the lower right area of the policy rules screen controls which itions and results are available here for use in policy rules.	
onditions		
NDG:Location:	-ANY-	
Time And Date:	-ANY-	
NDG:Device Type:	in All Device Types:WLC Select	
Identity Group:	-ANY-	
ermit Access	You may select multiple authorization profiles. Attributes defined in multiple profiles will use the value from the first profile defined.	I

Step 10: Click Save Changes.



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 > Networ	k Devices and AAA Clients > (reate
Name: WLC-0 Description:	EAP-1	
Network Device Groups	3	
Location	All Locations	Select
Device Type	All Device Types:WLC	Select
IP Address ● Single IP Address G IP: 192.168.19.20 ■ IP: 192.168.19.20	○ IP Range(S) By Mask	Authentication Options P Range(s) • TACACS+ Shared Secret: SecretKey • Hide Single Connect Device • Legacy TACACS+ Single Connect Support • TACACS+ Draft Compliant Single Connect Support • RADIUS • RADIUS • Shared Secret: SecretKey • Hide CoA port: 1700 • Enable KeyWrap Key Encryption Key: Message Authenticator Code Key: Key Input Format • ASCII • HEXADECIMAL
Submit Cancel		

PROCESS

Configuring Internet Edge

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

Procedure 1 Configure the DMZ switch

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

vlan 1119 name WLAN Mgmt

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

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

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

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

Procedure 2 Configure the DMZ interface

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

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

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

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

eneral Advanced	IPv6		
Hardware Port: 0	igabitEthernet0/1	Configure Hardware Properties	
Interface Name:			
Security Level:			
Dedicate this in	terface to management only		
Channel Group:			
🔽 Enable Interfa	e		
P Address		000-5	
Use static If		SE FFFUE	_
IP Address:			
Subnet Mask:	255.0.0.0 🗸		
Description: dmz	runk to dmz-3750 stack port x/0/1		
Description: dmz	runk to dmz-3750 stack port x/0/1		

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)

Add Interface	×
General Advanced IPv6	
Hardware Port: GigabitEthernet0/1 -	
Subinterface ID: 1119	
Interface Name: dmz-wlc	
Security Level: 50	
Dedicate this interface to management only	
V Enable Interface	
IP Address	
IP Address: 192.168.19.1	
Subnet Mask: 255.255.255.0	
Description:	
OK Cancel Help	

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.

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		

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

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)

🔁 Add Netwo	rk Object 💌
Name:	outside-wlc-ISPa
Type:	Host
IP Version:	IPv4 O IPv6
IP Address:	172.16.130.20
Description:	WLC to support Office Extend APs on ISP A.
NAT	8
	OK Cancel Help

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.

Add Network	Object 💌				
Name:	dmz-wlc-1				
Type:	Host 🗸 🗸				
IP Version:					
IP Address:	192.168.19.20				
Description:	Primary WLC to support Office Extend APs				
NAT	۲				
Add Automa	atic Address Translation Rules				
Type:	Static 👻				
Translated A	ddr: outside-wlc-ISPa				
Use one-	to-one address translation				
PAT Pool	Translated Address:				
Round	Robin				
Extend	PAT uniqueness to per destination instead of per interface				
Transla	te TCP and UDP ports into flat range 1024-65535 🗌 Include range 1-1023				
Fall throu	gh to interface PAT(dest intf): IPS-mgmt 👻				
Use IPv6	for interface PAT				
	Advanced				
	OK Cancel Help				

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)

🔂 Advanced NAT Settings				
Translate DNS replies for rule				
Disable Proxy ARP on egress interface				
Lookup route table to locate egress interface				
Interface				
Source Interface: Any				
Destination Interface: outside-16				
Service				
Protocol: 📧 tcp 👻				
Real Port:				
Mapped Port:				
OK Cancel Help				

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)

August 2013

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.

24 🗹 🚅 dmz-networks 📀 any 📼 ip 🔇 Deny

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.

🔁 Add Access I	Rule			
Interface:	Any 🔻			
Action: Permit Deny				
Source Criteria				
Source:	dmz-wlc-group			
User:				
Security Group:				
Destination Crite	ria			
Destination:	internal-aaa			
Security Group:				
Service:	tcp/tacacs, udp/1812, udp/1813			
Description:	Allow WLCs to communicate to the AAA server.			
🔽 Enable Loggi	ing			
Logging Leve	el: Default 🗸			
More Option	s 🛞			
	OK Cancel Help			

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.

🔁 Add Access I	Rule
Interface:	Any 👻
Action: Perm 	nit 💿 Deny
Source Criteria	
Source:	dmz-wlc-group
User:	
Security Group:	
Destination Crite	ria
Destination:	internal-ntp
Security Group:	
Service:	udp/ntp
Description:	Allow WLCs to communicate to the NTP server.
🔽 Enable Loggi	ing
Logging Leve	al: Default 🗸
More Option	s 🛞
	OK Cancel Help

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.

🔁 Add Access I	Rule	-
Interface:	Any 👻	
Action: Perm 	nit 💿 Deny	
Source Criteria		_
Source:	dmz-wic-group	
User:		
Security Group:		
Destination Crite	ria	-
Destination:	any -	
Security Group:		
Service:	tcp/ftp, tcp/ftp-data	
Description:	Allow WLCs to transfer files using FTP.]
🔽 Enable Loggi	ing	
Logging Leve	el: Default 🔹	
More Option	s 🛞	
	OK Cancel Help	

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.

💁 Add Access F	tule 💌				
Interface:	Any 🔹				
Action: Perm 	Action: Permit Deny				
Source Criteria					
Source:	any "				
User:					
Security Group:					
Destination Crite Destination:	ria				
Security Group:					
Service:	udp/5246, udp/5247				
Description:	Allow Office Extend APs to communicate with the WLCs.				
✓ Enable Logging					
Logging Leve	d: Default 🗸				
More Option	5				
	OK Cancel Help				



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
```

Configuring WLC

- 1. Configure the WLC platform
- 2. Configure the WLC for NAT
- 3. Configure the time zone
- 4. Configure SNMP

PROCESS

- 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)

սիսիս								ogout <u>R</u> efresh
cisco	MONITOR WLANS C	ONTROLLER	WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP FEEDBACK	
Controller	Interfaces > Edit						< Back	Apply
General Inventory Interfaces Interface Groups Multicast Network Routes	General Information Interface Name MAC Address Configuration	manage d0:d0:f	ment d:1f:59:e0					
Internal DHCP Server	Quarantine							
Mobility Management	Quarantine Vlan Id	0						
Ports NTP	NAT Address							
► CDP	Enable NAT Address	\checkmark						
Advanced	NAT IP Address	172.16.130	0.20					
	Interface Address							
	VLAN Identifier	C	1					
	IP Address	1	92.168.19.20					
	Netmask	2	55.255.255.0					
	Gateway	1	92.168.19.1					
	Physical Information							
	Port Number	1						
	Backup Port	C						
	Active Port	1						
	Enable Dynamic AP Mana	agement 🛛	1					
	DHCP Information							
	Primary DHCP Server	1	0.4.48.10					
	Secondary DHCP Server	C	.0.0.0					
	Access Control List							
	ACL Name	r	ione 👻					
	Note: Changing the Interfac temporarily disabled and th clients.	ce parameters us may result	causes the WL in loss of conne	ANs to be ectivity for som	ne			

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.

ululu cisco	Saye Configuration Eng Logout Befresh MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP EEEDBACK
Commands	Set Time Set Timezone
Download File Upload File Reboot	Current Time Tue May 31 11:07:38 2011 Date
Config Boot Scheduled Reboot 	Month May -
Reset to Factory Default	Day 31 V Year 2011
Set Time	
Login Banner	Time
	Hour 11 👻
	Minutes 7
	Seconds 38
	Timezone
	Delta hours 0 mins 0
	Location ¹ (GMT -8:00) Pacific Time (US and Canada)
	Foot Notes
	1. Automatically sets daylight savings time where used.

Procedure 4 Con

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.

ahaha							Sa <u>v</u> e Co	nfiguration <u>P</u> ing	Logout <u>R</u> efresh
cisco	MONITOR	<u>W</u> LANs		WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP FEEDBA	аск
Management Summary SNNP General SNNP V3 Users Communities Trap Logs HTTP-HTTPS Telnet-SSH Serial Port Local Management Users	MONITOR SNMP v1 Communi IP Addres IP Mask Access M Status	WLANS / v2c Cc ty Name is	CONTROLLER mmunity > N cisco123 10.4.48.0 255.255.255.0 Read/Write • Enable •	WIRELESS ew	SECURITY	MANAGEMENT	Saye Co	nfiguration Eing HELP <u>F</u> EEDBJ < Back	Logout <u>R</u> efresh ICK Apply
 Logs Mgmt Via Wireless Software Activation Tech Support 									

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.

ululu cisco	MONITOR	WLANs	CONTROLLER	WIRELESS	SECURITY	MANAG	EMENT CO	Sa <u>v</u> e Con MMANDS	figuration HELP	FEEDBACH	Logout <u>R</u> efresh
Management	SNMP v1 /	v2c Co	mmunity	Manazado	geourin	- Iginito				Tecopila	New
Summary SNMP	Community	Name		IP Address	IP Mask	А	ccess Mode	Status			
General	cisco			10.4.48.0	255.255.25	55.0 R	Read-Only	Enable			
SNMP V3 Users Communities	cisco123			10.4.48.0	255.255.25	55.0 R	Read-Write	Enable			
Trap Receivers Trap Controls											
Trap Logs											
HTTP-HTTPS											
Telnet-SSH											
Serial Port											
Local Management Users											
User Sessions											
Logs											
Mgmt Via Wireless											
Software Activation											
Tech Support											

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

սիսիս							Sa <u>v</u> e Co	nfiguratio	n <u>P</u> ing Logout <u>R</u> efresh
cisco	MONITOR	<u>W</u> LANs		WIRELESS	SECURITY	MANAGEMEN	t c <u>o</u> mmands	HELP	<u>F</u> EEDBACK
Security	Access C	ontrol L	ists > Rules >	New					< Back Apply
 AAA Local EAP Priority Order 	Sequence Source		1 IP Address	•	IP Addr 10.4.4	ess 8.0	Netmask 255.255.255.0		
Certificate	Destination		Any	-					
 Access Control Lists Access Control Lists CPU Access Control Lists ElexConnect ACLs 	Protocol Source Port		TCP Any	- -					
Wireless Protection Policies	Destination P	ort	HTTPS	•					
Web Auth	DSCP		Any	•					
TrustSec SXP Advanced	Direction		Any	•					
	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	ТСР	Other/22	Permit
3	Any	Any	ТСР	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)

31

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

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

սիսիս										.ogout <u>R</u> efresh
cisco	MONITOR	<u>W</u> LANs		WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK	
Security	RADIUS	Authenti	cation Server	s > New					< Back	Apply
 AAA General RADIUS Authentication Accounting Fallback TACACS+ LOAP Local Net Users MAC Filtering Disabled Clients User Login Policies Periority Order Certificate Access Control Lists Wireless Protection Policies Wireless Stretection Policies Web Auth TrustSec SXP Advanced 	Server In Server IP Shared St Shared St Confirm 5 Key Wrap Port Num Server St Support fo Server Ti Network I Managem IPSec	dex (Priorit Address scret Forma scret ihared Secr ber atus or RFC 3570 meout Jser ent	v) it et	1 v 10.4.48.15 ASCII v (Designed fr 1812 Enabled v 2 secon Ø Enable Enable	or FIPS custom	ars and requires a l	xey wrap complia	nt RADIU	- Server)	

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)

սիսիս						Sa <u>v</u> e Co	nfiguration <u>P</u> ing	Logout <u>R</u> efresh
CISCO	MONITOR WLANS		WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP FEEDBAC	ж
CISCO Security AAA General RADIUS Authentication Accounting Fallback TACACS+ LDAP Local Net Users MAC Filtering Disabled Clients User Login Policies Password Policies Password Policies Password Policies Paschart Policies Paschart Policies Paschart Policies Paschart Policies Paschart Policies Paschart Policies Portificate ACCess Control Lists Wireless Protection Policies Web Auth TrustSec SXP Advanced	NONTOR WLANK RADIUS Account Server Index (Prio Server IP Address Shared Secret Fon Shared Secret Fort Number Server Status Server Status Server Timeout Network User JPSec	CONTROLLER nting Servers > nty) 1 10.4 10.4 cret	WJRELESS New 4.46.15 II • Hed • seconds nable Enable	SECURITY			HELP <u>FEEDBAC</u>	K Apply

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)

h. dha								Logout <u>R</u> efresh
CISCO	MONITOR WLANS		WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP FEEDE	BACK
AAA General AAA General AAAUUS TACACS+ Authentication Accounting Authentication Local Net Users MAC Filtering Disabled Clients User Login Policies	MONITOR WLANS TACACS+ Author Server Index (Prior Server IP Address Shared Secret Form Shared Secret Confirm Shared Se Port Number Server Status Server Timeout	CONTROLLER entication Serv ity) nat cret	WIRELESS ers > New 1 • 10.4.48.15 ASCII • ••••••••• 49 Enabled • 5 second	SECURITY	MANAGEMENT	Sa <u>ve</u> Cor C <u>Q</u> MMANDS	figuration £ing HEL₽ £EEOE < Back	Logout Befresh NACK Apply
Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies Password Policies I Local EAP Priority Order Access Control Lists Wireless Protection Policies	Port Number Server Status Server Timeout		Enabled • 5 second	łs				
Web Auth TrustSec SXP Advanced								

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)

սիսիս						Sa <u>v</u> e Co	nfiguration <u>P</u> ir	ng Lo <u>q</u> out <u>R</u> e	efresh
	TOR <u>W</u> LANS <u>C</u>	ONTROLLER \	WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP FEED	BACK	
Security TAC/	ACS+ Accountir	ng Servers >	New				< Back	App	y
 AAA General FADIUS FADIUS FACACS+ Accounting Sha Accounting Control Control Control Ret Users MAC Filtering Disabled Clients User Login Policies Password Policies Local EAP Priority Order Certificate Access Control Lists Wireless Protection Policies Wireless Protection Policies Web Auth TrustSec SXP Advanced 	ver Index (Priority) ver IP Address ared Secret Format ared Secret firm Shared Secret t Number ver Status ver Timeout	1 • 10.4.48 ASCII 49 Enabled 5 s	.15]				

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)

h. du								I <u>P</u> ing Logout <u>R</u> efresh
cisco	MONITOR WLANS		WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK
Security AAA General P RADIUS TACACS+	TACACS+ Author Server Index (Priorit Server IP Address	ization Serve y)	1 ▼ 10.4.48.15				4	: Back Apply
Authentication Accounting Authorization	Shared Secret Forma Shared Secret Confirm Shared Secr	et	ASCII +					
LDAP Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies Password Policies	Port Number Server Status Server Timeout		49 Enabled • 5 second	ls				
Local EAP								
Priority Order								
Certificate Access Control Lists Vireless Protection Policies Web Auth TrustSec SXP Advanced								

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 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)

iiliiilii cisco	MONITOR	<u>W</u> LANs	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	Sa <u>v</u> e Co C <u>O</u> MMANDS	nfiguration <u>P</u> ing HELP <u>F</u> EEDB4	Logout <u>R</u> efresh ACK
Controller	Interface	s > New	r					< Back	Apply
General Inventory Interfaces Interface Groups Multicast Network Routes Internal DHCP Server Mobility Management Ports NTP CDP Advanced	Interface VLAN Id	Name	Wireless-Data 244						0007

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)

արտիս							Sa <u>v</u> e Cor		.ogout <u>R</u> efresh
CISCO	MONITOR	<u>W</u> LANs		WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP FEEDBACK	
Controller	Interfaces	s > Edit						< Back	Apply
General									
Inventory	Conoral I								
Interfaces	General I	mormatic	м						
Interface Groups	Interface	Name	Wireles	s-Data					
Multicast	MAC Addr	ess	d0:d0:f	d:1f:59:e0					
Network Routes	Configura	tion							
Internal DHCP Server	Guest Lan								
Mobility Management	Quarantin	e							
Ports	Quarantin	e Vlan Id	0						
▶ NTP	Physical I	nformati	0.0						
▶ CDP	Filysicul	inormati	-						
Advanced	Port Numb	ber	2						
	Backup Po	ort •	0						
	Enable Dv	r namic AP							
	Managem	ent							
	Interface	Address							
	VLAN Ider	ntifier	244						
	IP Address	s	10.4.144.5	i					
	Netmask		255.255.25	52.0					
	Gateway		10.4.144.1						
	DHCP Info	ormation							
	Primary D	HCP Server	:	10.4.48.10					
	Secondary	/ DHCP Serv	er						
	Access Co	ntrol List							
	ACL Name			none 🔻					
	Note: Chang temporarily o some clients.	ing the Inter disabled and	face parameters thus may result	causes the WL in loss of conn	ANs to be ectivity for				

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)

սիսին										Logout <u>R</u> efresh
cisco	MONITOR	<u>W</u> LANs		WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	FEEDBACK	(
Controller	Interface	s > New						<	Back	Apply
General Inventory Interfaces Interface Groups Multicast Network Routes Internal DHCP Server Mobility Management Ports NTP CDP Advanced	Interface VLAN Id	Name [Wireless-Voice 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)

ahaha						Sa <u>v</u> e Co	nfiguration	<u>P</u> ing L	ogout <u>R</u> efresh
cisco	MONITOR WLA	ANS <u>C</u> ONTROLLER	WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP FE	EDBACK	
Controller	Interfaces > E	dit					< Ba	ick	Apply
General									
Inventory	General Infor	mation							
Interfaces	Interface Name	wireles	a voice						
Interface Groups	MAC Address	dordor	64-16-50-e0						
Multicast	MAC Address	00.00.	10.11.39.60						
Network Routes	Configuration								
Internal DHCP Server	Guest Lan								
Mobility Management	Quarantine								
Ports	Quarantine Vlar	n Id 0							
▶ NTP	Physical Infor	mation							
▶ CDP	Dest Number								
Advanced	Port Number	2							
	Active Port	0							
	Enable Dynamic Management	AP							
	Interface Add	ress							
	VLAN Identifier	248							
	IP Address	10.4.148.	5						
	Netmask	255.255.2	52.0						
	Gateway	10.4.148.	1						
	DHCP Informa	tion							
	Primary DHCP S	Gerver	10.4.48.10						
	Secondary DHC	P Server							
	Access Contro	l List							
	ACL Name		none 👻						
	Note: Changing th temporarily disable some clients.	e Interface parameters ed and thus may result	causes the WL in loss of conne	ANs to be ectivity for					

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)

	MONITOR	<u>W</u> LANs		WIRELESS	SECURITY	MANAGEMENT	Sa <u>v</u> e Co C <u>O</u> MMANDS	nfiguration <u>P</u> ing Lo HELP <u>F</u> EEDBACK	gout <u>R</u> efresh
Controller	Interfaces	s > New						< Back	Apply
General Inventory Interfaces Interface Groups Multicast Network Routes Internal DHCP Server Mobility Management Ports NTP CDP Advanced	Interface I	Name [Remote-LAN 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)

սիսիս					Sa <u>v</u> e Configuration <u>P</u> ing Logout <u>R</u> ef				
cisco	MONITOR WLANS		WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	FEEDBACK	
Controller	Interfaces > Edit	t						< Back	Apply
General									
Interfaces	General Informa	tion							
Interface Groups	Interface Name	Remote	-LAN						
Multicast	MAC Address	d0:d0:	d:1f:59:e0						
Network Routes	Configuration								
Internal DHCP Server	Guest Lan								
Mobility Management	Quarantine								
Ports	Quarantine Vlan Id	0							
▶ NTP	Physical Informa	tion							
Advanced	Port Number	2							
P Advanced	Backup Port	0							
	Active Port	0							
	Enable Dynamic AF Management								
	Interface Addres	s							
	VLAN Identifier	252							
	IP Address	10.4.152.5	5						
	Netmask	255.255.2	52.0						
	Gateway	10.4.152.3							
	DHCP Informatio	'n							
	Primary DHCP Serv	er	10.4.48.10						
	Secondary DHCP S	erver							
	Access Control L	ist							
	ACL Name		none 👻						
	Note: Changing the Ir temporarily disabled a some clients.	terface parameters and thus may result	causes the WL in loss of conn	ANs to be ectivity for					

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.

սիսիս		Sa <u>v</u> e Configuration <u>P</u> ing Logout <u>R</u> efresh
cisco	MONITOR WLANS CONTROLLER WIRELESS SEC	URITY MANAGEMENT COMMANDS HELP FEEDBACK
WLANs	WLANs	Entries 1 - 1 of 1
WLANS	Current Filter: None [Change Filter] [Clear Filter]	Create New - Go
Advanced	WLAN	Admin
	1 WLAN WLAN-Data	WLAN SSID Status Security Policies 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)



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

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

alialia –	Sa <u>v</u> e Configuration <u>P</u> ing Log	out <u>R</u> efres
CISCO	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK	
WLANs	WLANs > Edit 'WLAN-Data'	Apply
WLANS	General Security QoS Advanced	
Advanced	Allow AAA Override Enabled DHCP Coverage Hole Detection Enabled DHCP Server Override Enable Seaion Timeout 1800 DHCP Addr. Assignment Required Aironet IE Enabled Management Frame Protection (MPP) Diagnostic Channel Enabled Management Frame Protection (MPP) Diagnostic Channel Enabled MPP Client Protection 4 Optional PV6 Enable 2 Override Interface ACL None DTIH Period (in beacon intervals) P2P Blocking Action Disabled 802.11a/n (1 - 255) 1 Maximum Allowed Clients 0 802.11a/n (1 - 255) 1 Static IP Tunneling 2 Enabled NAC NAC State None Off Channel Scanning Defer Client Load Balancing and Band Select Client Load Balancing 0 0 Static IP Tunneling 1 2.3.4.5.6.7 Client Band Select 0 Static IP Tunneling be used in combination with IPsec 2.H-REAP Local Switching is not supported with IPsec, CRANITE authentication 3 3 Whon class Studie L P1 is configurable only when HR2P Local Switching is enabled Genet Baller Timocut Salleve Cover Times there the colusion is enabled,	clients)

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.

ahaha				<u>v</u> e Configuration <u>P</u> ing Lo <u>g</u> out <u>R</u> efresh
CISCO	MONITOR WLANS CO	ONTROLLER WIRELESS SECU	IRITY M <u>A</u> NAGEMENT C <u>O</u> MMA	NDS HELP FEEDBACK
WLANs	WLANs			Entries 1 - 1 of 1
WLANS	Current Filter: None	[Change Filter] [Clear Filter]	Create New	Go
Advanced	WLAN ID Type	Profile Name	WLAN SSID	Admin Status Security Policies
	1 WLAN	WLAN-Data	WLAN-Data	Enabled [WPA2][Auth(802.1X)]

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)

սիսիս						figuration <u>P</u> ing Lo <u>q</u> out <u>R</u> efresh
cisco	MONITOR WLANS	CONTROLLER WIRELESS	SECURITY I	MANAGEMENT	COMMANDS	HELP FEEDBACK
WLANs	WLANs > New					< Back Apply
WLANS WLANS Advanced	Type Profile Name SSID ID	Voice WLAN-Voice 2 •				

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.

ահահո	Sa <u>v</u> e Configuration <u>P</u> ing Logout <u>R</u> efresh
CISCO	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
WLANs	WLANS > Edit 'Voice' < Back Apply
WLANS WLANS	General Security QoS Advanced
Advanced	Quality of Service (QoS) Platinum (voice) WHM Platinum (voice) WMM Policy Allowed 7920 AP CAC Enabled 7920 Client CAC Enabled
	Foot Notes 1 Web Policy cannot be used in combination with IPsec. 2 H-R2AP 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 HR2P 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 IPr6. 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 should be enabled. 11 MAC Filtering should be enabled. 12 Guest tunneling, Local switching. hICP Required should be disabled. 13 Man-associate-Clients Fature is not supported with HREAP Local Authentication.

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

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

սիսիս	Sage Configuration Ping Log	lout <u>R</u> efresh
CISCO	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK	
WLANs	WLANs > Edit 'Voice'	Apply
WLANS	General Security QoS Advanced	
Advanced	Allow AAA Override Enabled DHCP Coverage Hole Detection Enabled DHCP Server Override Enable Session Timeout I 1800 Session Timeout (secs) DHCP Addr. Assignment Required Aironet IE Enabled Management Frame Protection (MFP) Diagnostic Channel Enabled MFP Client Protection 4 Optional • IPv6 Enable 7 Override Interface ACL None • DTIM Period (in beacon intervals) P2P Blocking Action Disabled • 802.11a/n (1 - 255) 1 802.11b/g/n (1 - 255) 1 Client Exclusion 3 ©Enabled 7 NAC NAC State None •	E
	Off Channel Scanning Defer Client Load Balancing Client Load Balancing	
	Scan Defer Priority 0 1 2 3 4 5 6 7 Client Band Select 2	-
	Foot Notes I Web Policy cannot be used in combination with IPsec ANTE authentication I Heb Policy cannot be used in combination with IPsec ANTE authentication I Heb Policy cannot be used in combination with IPsec CANTE authentication I Hes Policy cannot be used in combination with IPsec CANTE authentication I Hes Policy cannot be used in combination with IPsec CANTE authentication I Hes Policy cannot be used in combination with IPsec I HeBP I Foot active unless WPA2 is configured I cannot the IPs inot active unless WPA2 is configured I cannot the IPs inot active unless WPA2 is configured I cannot the IPs inot active unless WPA2 is configured I cannot the IPs inot active unless WPA2 is configured I cannot the IPs inot active unless WPA2 is configured I cannot the IPsec I with a down on the IPs	clients)

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.

uluilu cisco	MONITOR WLANS CONTROLLER WIRELESS S	Sa <u>v</u> e Configuration Ping Logout <u>R</u> efresh ECURITY MANAGEMENT COMMANDS HELP <u>F</u> EEDBACK
WLANs	WLANs	Entries 1 - 2 of 2
WLANS	Current Filter: None [Change Filter] [Clear Filter	Create New Go
▶ Advanced	WLAN ID Type Profile Name 1 WLAN WLAN-Data 2 WLAN Voice	Admin Admin WLAN SSID Status Security Policies WLAN-Data Enabled [WPA2][Auth(602.1X)] WLAN-Voice Enabled [WPA2][Auth(602.1X)]

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)

cisco	MONITOR WLANS CON	TROLLER WIRELESS	SECURITY MANA	– GEMENT C <u>O</u> MMANDS	HELP FEEDBACK
WLANs	WLANs > Edit 'LAN'				< Back Apply
WLANS	General Security	Advanced			
Advanced	Profile Name	LAN			
	Туре	Remote LAN			
	SSID	LAN			
	Status	Enabled			
	Egress Interface	remote-lan •			
	Foot Notes 3 When client exclusion is e 9 Value zero implies there i	nabled, a Timeout Value o s no restriction on maximu	f zero means infinity (w m clients allowed.	vill require administrative ov	erride to reset excluded clients)

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.

PROCESS

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	Default Network Device Status: Enabled 🗸 \Theta						
Network Device Group	S						
Location	All Locations	Select					
Device Type	All Device Types	Select					
Authentication Options							
Shared Secret. S	ecretkey						
Single Connec	ct Device						
Legacy TACAC	CS+ Single Connect Support						
TACACS+ Dra	Ift Compliant Single Connect Support						
▼ RADIUS							
Shared Secret: S	3ecretKey						
CoA port: 1700							
Enable KeyW	/rap						
Key Encryption Ke	ey:						
Message Authent	ticator Code Key:						
Key Input Format	O ASCII HEXADECIMAL						
Required fields							
Submit Cancel							

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.

neral						
Name:	XX-XX	-XX-XX-XX-XX	Status:	Enabled •	• •	
Description:						
Identity Group:	All Gro	oups		S	elect	
assword Inform	nation			Enat	le Password Info	ormation
assword must:				Pas	word must:	
Contain 4	- 32 ch	aracters			Contain 4 - 32	characters
Decouverd Two		Internal Users		Er	able Password:	
rassword typ	e.	Select		_ C	onfirm	
Password:		•••••	••	Pas	sword:	
Confirm Pass	word:	•••••	••			
🔲 Change pa	asswor	d on next login				
er Information						
There are no ac	ditiona	al identity attributes de	efined for u	ser records		

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.

ahaha										: <u>R</u> efresh
cisco	MONITOR	<u>W</u> LANs		WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK	
Security	AP Policie	s							Apply	Add
▼ AAA General ▼ RADIUS	Policy Conf	figuratio	n							
Authentication Accounting	Accept Sel	f Signed C	Certificate (SSC)							
Fallback TACACS+	Accept Mar	nufactured	Installed Certific	ate (MIC)		\checkmark				
LDAP	Accept Loc	al Significa	ant Certificate (LS	(C)						
Local Net Users	Authorize I	MIC APs a	gainst auth-list or	AAA						
Disabled Clients	Authorize I	LSC APs a	gainst auth-list							
User Login Policies AP Policies Password Policies	AP Authoriz	zation Lis	st			Enti	ries 1 - 1 of 1			
Local EAP	Search by M	1AC		Search	h					
Priority Order	MAC Addres			Contificato	Tuna EN	At Key Hack				
Certificate	00:50:56:a2	54.96		sec	type SH	7711ab605f6af05al	a3fc7b84496ee9	972cd8f		_
Access Control Lists	00.00:00:02			330	00	2/41000001001930	0010/004490660	5720001		



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.



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.

abab						Refresh Close Window		
CISCO Office Extend Access Point	<u>H</u> OME	CONFIGURATION	EVENT_LOG	HELP				
Home: Summary								
General Information								
Ap Name		APE05F.B9DC.FC30						
AP IP Address		192.168.1.100						
AP Mode		Local						
AP MAC Address		E0:5F:B9:DC:FC:30						
AP Uptime		1 minutes, 28 second	is					
AP Software Version		7.0.112.53						
AP Statistics								
Radio	Admin Status	1	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	Associa	ation Time	Bytes In/Out	Duplicate/Retries		Decrypt Failed		
Client MAC Association Time Bytes In/Out Duplicate/Retries Decrypt Failed Image: The dit 'Personal SSID' association and settings, click on Configuration To edit 'Personal SSID' association and settings, click on Configuration Image: Click on Systems Inc. All rights reserved. Click on 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)

CISCO Office Extend Access Point	<u>H</u> OME	<u>CONFIGURATION</u>	EVENT_LOG	HELP	
Configuration					Apply
System	SSID	DHCP	WAN		
Primary Contro	ller				
IP Address		172.16.130.20			
Uplink IP Config	guration				
Uplink IP Config Static IP	guration				
Uplink IP Config Static IP Domain Name	guration	cisco.com			
Uplink IP Config Static IP Domain Name IP Address	guration	cisco.com 192.168.1.100			
Uplink IP Config Static IP Domain Name IP Address Subnet Mask:	guration	cisco.com 192.168.1.100 255.255.255.0			
Uplink IP Config Static IP Domain Name IP Address Subnet Mask: Default Gateway	guration	cisco.com 192.168.1.100 255.255.255.0 192.168.1.1			

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.

i	Tech Tip
After the of the a is com access or purp	he access point makes a connection to the WLC, the Status LED on the top access point flashes. The Status LED continues flashing until the download aplete. When the download is complete, your access point restarts. After the s point connects to the controller again, the Status LED is displayed as solid blue ple.



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.

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**.

ululu cisco	MONITOR WLANS CONTROLLER	WIRELESS	SECURITY MA	NAGEMENT (COMMANDS	HELP FEEDB						g Logout j	Befresh
Wireless	802.11a/n Radios				_							Entries 1 - 4	l of 4
Access Points All APs	Current Filter: None							[Change	Filter] [Cle	ar Filter]			
 Radios 802.11a/n 802.11b/g/n Dual-Band Radios 	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	
Global Configuration	APd0d0.fd45.4ae1	1	d0:57:4c:09:c0:80		Enable	UP	157 *	NA	NA	N/A	1 *	External	
Advanced	APd0d0.fdcb.b85c	1	58:bc:27:0e:1c:60	1.1	Enable	UP	64 *	NA	NA	N/A	6 *	Internal	
Mesh	AP442b.039a.9c3a	1	3c:ce:73:1b:43:50	1.1	Enable	UP	161 *	Enable	DOWN	N/A	1 *	Internal	
RF Profiles	APECC8.82B8.2B58	1	ec:c8:82:c0:ad:30		Disable	DOWN	36 *	NA	NA	N/A	1 *	Internal	. 🖸
FlexConnect Groups FlexConnect ACLs													
▶ 802.11a/n													
▶ 802.11b/g/n	* giobai assignment												
Media Stream													
Application Visibility And Control													
Country													
Timers													
▶ Netflow													
▶ QoS													

սիսիս				Saye Configuration Ping Logout <u>R</u> efresh
CISCO	MONITOR WLANS CONTROLLE	ER WIRELESS SECURITY MANAGEMEN	F COMMANDS HELP FEEDBAC	к
Wireless	802.11a/n Cisco APs > Confi	gure		< Back Apply
Access Points All APs Radios Roo 110(a	General		RF Channel Assignment	
802.11b/g/n	AP Name	APECC8.82B8.2B58	Current Channel	36
Dual-Band Radios	Admin Status	Enable 👻	Channel Width *	20 MHz 👻
Advanced	Operational Status	DOWN	* Channel width can be configured mode	l only when channel configuration is in custom
Mesh	Slot #	1	Assignment Method	AP Controlled
RF Profiles	11n Parameters			Custom
FlexConnect Groups FlexConnect ACLs	11n Supported	Yes	Tx Power Level Assignmen	t
▶ 802.11a/n			Current Tx Power Level	1
▶ 802.11b/g/n			Assignment Method	AP Controlled
Media Stream				Custom
Application Visibility And Control				
Country			Note: Changing any of the param and thus may result in loss of con	ters causes the Radio to be temporarily disabled nectivity for some clients.
Timers				
Netflow				
▶ QoS				

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.



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.

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)

August 2013

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)

Wireless All APs > Details for APE05F.B9DC.FC30 < Back	uluilu cisco	Saye Configuration <u>Ping</u> Logout <u>R</u> efre MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK	esh
Access Points General Interfaces High Availability Inventory Advanced All APs Radios 802.11a/n Name Management IP Address 802.11a/n Primary Controller WLC-0EAP-1 172.16.130.20 Global Configuration Secondary Controller WLC-0EAP-2 172.17.130.20 Mesh Tertiary Controller Interfaces Interfaces	Wireless	All APs > Details for APE05F.B9DC.FC30 < Back Apply	
HREAP Groups 902.11a/n AP Failover Priority Wedia Stream Country Timers QoS	 Access Points All APs Radios 802.11a/n 802.11b/g/n Global Configuration Advanced Mesh HREAP Groups 802.11a/n 802.11b/g/n Media Stream Country Timers QoS 	Ceneral Interfaces High Availability Inventory Advanced Name Management IP Address 172.16.130.20 172.17.130.20 Secondary Controller 172.17.130.20 172.17.130.20 Tertiary Controller 172.17.130.20 172.17.130.20 AP Failover Priority Low Image: Controller Image: Controller AP Failover Priority Low Image: Controller Image: Controller Fort Notes 1 DNS server IP Address and the Domain name can be set only after a valid static IP is pushed to the AP.	

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.

•1|1•1|1• CISCO

Americas Headquarters Cisco Systems, Inc. San Jose, CA Asia Pacific Headquarters Cisco Systems (USA) Pte. Ltd. Singapore Europe Headquarters Cisco Systems International BV Amsterdam, The Netherlands

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

ALL DESIGNS, SPECIFICATIONS, STATEMENTS, INFORMATION, AND RECOMMENDATIONS (COLLECTIVELY, "DESIGNS") IN THIS MANUAL ARE PRESENTED "AS IS," WITH ALL FAULTS. CISCO AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE. IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THE DESIGNS, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE DESIGNS ARE SUBJECT TO CHANGE WITHOUT NOTICE. USERS ARE SOLELY RESPONSIBLE FOR THEIR APPLICATION OF THE DESIGNS. THE DESIGNS DO NOT CONSTITUTE THE TECHNICAL OR OTHER PROFESSIONAL ADVICE OF CISCO, ITS SUPPLIERS OR PARTNERS. SHOULD CONSULT THEIR OWN TECHNICAL ADVISORS BEFORE IMPLEMENTING THE DESIGNS. RESULTS MAY VARY DEPENDING ON FACTORS NOT TESTED BY CISCO.

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2013 Cisco Systems, Inc. All rights reserved.

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

B-0000315-1 08/13