

Newer Cisco Validated Design Guides Available

This guide is part of an older series of Cisco Validated Designs.

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





cisco.



Campus Wireless LAN TECHNOLOGY DESIGN GUIDE

August 2013



Table of Contents

Preface	1
CVD Navigator	2
Use Cases	2
Scope	2
Proficiency	2
Introduction	3
Technology Use Cases	3
Use Case: Network Access for Mobile Devices	3
Use Case: Guest Wireless Access	3
Design Overview	4
Deployment Components	5
Design Models	7
High Availability	9
Multicast Support	10
Guest Wireless	10
Deployment Details	12
Configuring the RADIUS Server: Cisco Secure ACS	13
Configuring the RADIUS Server: Windows Server 2008	22
Configuring On-Site Wireless Controllers	39
Configuring Remote-Site Wireless with Cisco FlexConnect	71
Configuring Guest Wireless: Shared Guest Controller	112
Configuring Guest Wireless: Dedicated Guest Controller	128
Appendix A: Product List	. 176

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:

- Network Access for Mobile Devices—At the headquarters and remote sites, mobile users require the same accessibility, security, quality of service (QoS), and high availability currently enjoyed by wired users.
- Guest Wireless Access—Most organizations host guest useraccess services for customers, partners, contractors, and vendors. Often these services give guest users the ability to check their email and other services over the Internet.

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

Scope

This guide covers the following areas of technology and products:

- · Onsite, remote-site, and guest wireless LAN controllers
- · Internet edge firewalls and demilitarized zone (DMZ) switching
- · Campus routing, switching, and multicast
- High availability wireless using access point stateful switchover (AP SSO)
- · Management of user authentication and policy
- Integration of the above with the LAN and data center switching infrastructure

Proficiency

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

- CCNP Wireless—3 to 5 years designing, installing, and troubleshooting wireless LANs
- CCNP Security—3 to 5 years testing, deploying, configuring, maintaining security appliances and other devices that establish the security posture of the network
- VCP VMware–At least 6 months installing, deploying, scaling, and managing VMware vSphere environments

Related CVD Guides Campus CleanAir Technology cisco. VALIDATED DESIGN **Design Guide** Campus Wired LAN cisco. ALIDATED **Technology Design Guide Device Management Using** cisco. VALIDATED ACS 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 Cases

With the adoption of smartphones and tablets, the need to stay connected while mobile has evolved from a niceto-have to a must-have. The use of wireless technologies improves our effectiveness and efficiency by allowing us to stay connected, regardless of the location or platform being used. As an integrated part of the conventional wired network design, wireless technology allows connectivity while we move about throughout the day.

Wireless technologies have the capabilities to turn cafeterias, home offices, classrooms, and our vehicles into meeting places with the same effectiveness as being connected to the wired network. In fact, the wireless network has in many cases become more strategic in our lives than wired networks have been. Given our reliance on mobility, network access for mobile devices, including guest wireless access, is essential.

Use Case: Network Access for Mobile Devices

At the headquarters and remote sites, the mobile user requires the same accessibility, security, quality of service (QoS), and high availability currently enjoyed by wired users.

This design guide enables the following network capabilities:

- Mobility within buildings or campus—Facilitates implementation of applications that require an always-on network and that involve movement within a campus environment.
- Secure network connectivity—Enables employees to be authenticated through IEEE 802.1x and Extensible Authentication Protocol (EAP), and encrypts all information sent and received on the WLAN.
- Simple device access—Allows employees to attach any of their devices to the WLAN using only their Microsoft Active Directory credentials.
- Voice services—Enables the mobility and flexibility of wireless networking to Cisco Compatible Extensions voice-enabled client devices.
- Consistent capabilities—Enables users to experience the same network services at main sites and remote offices.

Use Case: Guest Wireless Access

Most organizations host guest user-access services for customers, partners, contractors, and vendors. Often these services give guest users the ability to check their email and other services over the Internet.

This design guide enables the following network capabilities:

- Allows Internet access for guest users and denies them access to corporate resources
- · Allows groups of users called sponsors to create and manage guest user accounts
- Enables the use of shared and dedicated guest controller architectures

3

Design Overview

This deployment uses a wireless network in order to provide ubiquitous data and voice connectivity for employees and to provide wireless guest access for visitors to connect to the Internet.

Regardless of their location within the organization, on large campuses, or at remote sites, wireless users can have a similar experience when connecting to voice, video, and data services.

Benefits:

- Productivity gains through secure, location-independent network access—Measurable productivity improvements and communication.
- · Additional network flexibility-Hard-to-wire locations can be reached without costly construction.
- Cost effective deployment Adoption of virtualized technologies within the overall wireless architecture.
- Easy to manage and operate—From a single pane of glass, an organization has centralized control of a distributed wireless environment.
- **Plug-and-play deployment**—Automatic provisioning when an access point is connected to the supporting wired network.
- Resilient, fault-tolerant design-Reliable wireless connectivity in mission-critical environments, including complete RF-spectrum management.
- · Support for wireless users-Bring your Own Device (BYOD) design models.
- Efficient transmission of multicast traffic Support for many group communication applications, such as video and push-to-talk.

This Cisco Validated Design (CVD) deployment uses a controller-based wireless design. Centralizing configuration and control on the Cisco wireless LAN controller (WLC) allows the wireless LAN (WLAN) to operate as an intelligent information network and support advanced services. This centralized deployment simplifies operational management by collapsing large numbers of managed endpoints.

The following are some of the benefits of a centralized wireless deployment:

- Lower operational expenses—A controller-based, centralized architecture enables zero-touch configurations for lightweight access points. Similarly, it enables easy design of channel and power settings and real-time management, including identifying any RF holes in order to optimize the RF environment. The architecture offers seamless mobility across the various access points within the mobility group. A controller-based architecture gives the network administrator a holistic view of the network and the ability to make decisions about scale, security, and overall operations.
- **Improved Return on Investment**—With the adoption of virtualization, wireless deployments can now utilize a virtualized instance of the wireless LAN controller, reducing the total cost of ownership by leveraging their investment in virtualization.
- Easier way to scale with optimal design—As the wireless deployment scales for pervasive coverage and to address the ever-increasing density of clients, operational complexity starts growing exponentially. In such a scenario, having the right architecture enables the network to scale well. Cisco wireless networks support two design models, local mode for campus environments and Cisco FlexConnect for lean remote sites.

Figure 1 - Wireless overview



Deployment Components

The CVD WLAN deployment is built around two main components: Cisco wireless LAN controllers and Cisco lightweight 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 lightweight access points to support business-critical wireless applications. From voice and data services to location tracking, Cisco wireless LAN controllers provide the control, scalability, security, and reliability that network managers need to build secure, scalable wireless networks—from large campus environments to remote sites.

Although a standalone controller can support lightweight access points across multiple floors and buildings simultaneously, you should deploy 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.

5

The following controllers are included in this release of CVD:

- Cisco 2500 Series Wireless LAN Controller
 —This controller supports up to 75 lightweight access points and 1000 clients. Cisco 2500 Series Wireless LAN Controllers are ideal for small, single-site WLAN deployments.
- Cisco 5500 Series Wireless LAN Controller—This controller supports up to 500 lightweight access points and 7000 clients, making it ideal for large-site and multi-site WLAN deployments.
- Cisco Virtual Wireless LAN Controller-vWLCs are compatible with ESXi 4.x and 5.x and support up to 200 lightweight access points across two or more Cisco FlexConnect groups and 3000 clients total. Each vWLC has a maximum aggregate throughput of 500 Mbps when centrally switched with additional capacity achieved horizontally through the use of mobility groups. The virtualized appliance is well suited for small and medium-sized deployments utilizing a FlexConnect architecture.
- Cisco Flex 7500 Series Cloud Controller–Cisco Flex 7500 Series Cloud Controller for up to 6000
 Cisco access points supports up to 64,000 clients. This controller is designed to meet the scaling
 requirements to deploy the Cisco FlexConnect solution in remote-site networks.

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 you purchase incremental access-point licenses only when you need them.

Cisco Lightweight Access Points

In the Cisco Unified Wireless Network architecture, access points are *lightweight*. This means they cannot act independently of a wireless LAN controller (WLC). The lightweight access points (LAPs) have to first discover the WLCs and register with them before the LAPs service wireless clients. There are two primary ways that the access point can discover a WLC:

- Domain Name System (DNS)—When a single WLC pair is deployed in an organization, the simplest way
 to enable APs to discover a WLC is by creating a DNS entry for cisco-capwap-controller that resolves to
 the management IP addresses of WLCs.
- Dynamic Host Configuration Protocol (DHCP)—Traditionally, when multiple WLC pairs are deployed in an organization, DHCP Option 43 was used to map access points to their WLCs. Using Option 43 allows remote sites and each campus to define a unique mapping.

As the access point communicates with the WLC resources, it will download its configuration and synchronize its software or firmware image, if required.

Cisco lightweight access points work in conjunction with a Cisco wireless LAN controller to connect wireless devices to the LAN while supporting simultaneous data-forwarding and air-monitoring functions. The CVD wireless design is based on Cisco 802.11n wireless access points, which offer robust wireless coverage with up to nine times the throughput of 802.11a/b/g networks. The following access points are included in this release of the CVD:

 Cisco Aironet 1600 Series Access Points are targeted for small and medium enterprises seeking to deploy or migrate to 802.11n technology at a low price point. The access point features a 3x3 MIMO radio with support for two spatial-streams.

Wireless networks are more than just a convenience; they are mission-critical to the business. However, wireless operates in a shared spectrum with a variety of applications and devices competing for bandwidth in enterprise environments. More than ever, IT managers need to have visibility into their wireless spectrum to manage RF interference and prevent unexpected downtime. Cisco CleanAir provides performance protection for 802.11n networks. This silicon-level intelligence creates a self-healing, self-optimizing wireless network that mitigates the impact of wireless interference.

6

This release of the CVD includes two Cisco CleanAir access points:

- Cisco Aironet 2600 Series Access Points with Cisco CleanAir technology create a self-healing, selfoptimizing wireless network. By intelligently avoiding interference, they provide the high-performance 802.11n connectivity for mission-critical mobility and performance protection for reliable application delivery.
- Cisco Aironet 3600 Series Access Points with Cisco CleanAir technology deliver more coverage for tablets, smart phones, and high-performance laptops. This next-generation access point is a 4x4 MIMO, three-spatial-stream access point, resulting in up to three times more availability of 450 Mbps rates and performance optimization for more mobile devices.

For more information on Cisco CleanAir, see the Campus CleanAir Design Guide.

Design Models

Cisco Unified Wireless networks support two major design models: local-mode and Cisco FlexConnect.

Local-Mode Design Model

In a local-mode design model, the wireless LAN controller and access points are co-located. The wireless LAN controller is connected to a LAN distribution layer at the site, and traffic between wireless LAN clients and the LAN is tunneled in Control and Provisioning of Wireless Access Points (CAPWAP) protocol between the controller and the access point.

Figure 2 - Local-mode design model



A local-mode architecture uses the controller as a single point for managing Layer 2 security and wireless network policies. It also enables services to be applied to wired and wireless traffic in a consistent and coordinated fashion.

In addition to providing the traditional benefits of a Cisco Unified Wireless Network approach, the local-mode design model meets the following customer demands:

- Seamless mobility—In a campus environment, it is crucial that users remain connected to their session even while walking between various floors or adjacent buildings with changing subnets. The local controller-based Cisco Unified Wireless network enables fast roaming across the campus.
- Ability to support rich media—As wireless has become the primary mode of network access in many campus environments, voice and video applications have grown in significance. The local-mode design model enhances robustness of voice with Call Admission Control (CAC) and multicast with Cisco VideoStream technology.
- Centralized policy—The consolidation of data at a single place in the network enables intelligent inspection through the use of firewalls, as well as application inspection, network access control, and policy enforcement. In addition, network policy servers enable correct classification of traffic from various device types and from different users and applications.

If any of the following are true at a site, you should deploy a controller locally at the site:

- The site has a LAN distribution layer.
- The site has more than 50 access points.
- The site has a WAN latency greater than 100 ms round-trip to a proposed shared controller.

In a deployment with these characteristics, use either a Cisco 2500 or 5500 Series Wireless LAN Controller. For resiliency, the design uses two wireless LAN controllers for the campus, although you can add more wireless LAN controllers in order to provide additional capacity and resiliency to this design.

Cisco FlexConnect Design Model

Cisco FlexConnect is a wireless solution for remote-site deployments. It enables organizations to configure and control remote-site access points from the headquarters through the WAN, without deploying a controller in each remote site.

If all of the following are true at a site, deploy Cisco FlexConnect at the site:

- The site LAN is a single access-layer switch or switch stack.
- The site has fewer than 50 access points.
- The site has a WAN latency less than 100 ms round-trip to the shared controller.

The Cisco FlexConnect access point can switch client data traffic out its local wired interface and can use 802.1Q trunking in order to segment multiple WLANs. The trunk native VLAN is used for all CAPWAP communication between the access point and the controller.

8

Figure 3 - Cisco FlexConnect design model



Cisco FlexConnect can also tunnel traffic back to the controller, which is specifically used for wireless guest access.

You can use a shared controller pair or a dedicated controller pair in order to deploy Cisco FlexConnect.

If you have an existing local-mode controller pair at the same site as your WAN aggregation, and if the controller pair has enough additional capacity to support the Cisco FlexConnect access points, you can use a shared deployment. In a shared deployment, the controller pair supports both local-mode and Cisco FlexConnect access points concurrently.

If you don't meet the requirements for a shared controller, you can deploy a dedicated controller pair by using Cisco 5500 Series Wireless LAN Controller, virtual wireless LAN controller, or Cisco Flex 7500 Series Cloud Controller. The controller should reside in and be connected to the server room or data center switches. For resiliency, the design uses two controllers for the remote sites, although you can add more controllers in order to provide additional capacity and resiliency to this design.

High Availability

As mobility continues to increase its influence in all aspects of our personal and professional lives, availability continues to be a top concern. The Cisco Validated Design models continue to support high availability through the use of resilient controllers within a common mobility group.

With the advent of access point stateful switchover (AP SSO), the resiliency of the wireless network continues to improve. By adopting the cost effective AP SSO licensing model, Cisco wireless deployments can improve the availability of the wireless network with recovery times in the sub-second range during a WLC disruption. In addition, AP SSO allows the resilient WLC to be cost-effectively licensed as a standby controller with its access point (AP) license count being automatically inherited from its paired primary WLC.

9

Operational and policy benefits also improve as the configuration and software upgrades of the primary WLC are automatically synchronized to the resilient standby WLC. Support for AP SSO is available on Cisco 5500 Series Wireless LAN Controllers and on Cisco Flex 7500 Series Cloud Controllers.

Multicast Support

Video and voice applications are growing exponentially as smartphones, tablets, and PCs continue to be added to wireless networks in all aspects of our daily life. Multicast is required in order to enable the efficient delivery of certain one-to-many applications, such as video and push-to-talk group communications. By extending the support of multicast beyond that of the campus and data center, mobile users can now use multicast-based applications.

This design guide now fully supports multicast transmission for the onsite controller through the use of Multicast-Multicast mode. *Multicast-Multicast mode* uses a multicast IP address in order to communicate multicast streams to access points that have wireless users subscribing to a particular multicast group. Multicast-Multicast mode is supported on both the Cisco 2500 and 5500 Series Wireless LAN Controllers.

Remote sites that utilized the Cisco Flex 7500 Series Cloud Controller or vWLC using Cisco FlexConnect in local switching mode can also benefit from the use of multicast-based applications. Multicast in remote sites leverage the underlying WAN and LAN support of multicast traffic. When combined with access points in FlexConnect mode using local switching, subscribers to multicast streams are serviced directly over the WAN or LAN network with no additional overhead being placed on the Wireless LAN Controller.

In each of the wireless design models in this CVD, the multicast support that users are accustomed to on a wired network is available wirelessly for those applications and user groups that require it.

Guest Wireless

Using the organization's existing WLAN for guest access provides a convenient, cost-effective way to offer Internet access for visitors and contractors. The wireless guest network provides the following functionality:

- Provides Internet access to guests through an open wireless Secure Set Identifier (SSID), with web access control.
- Supports the creation of temporary authentication credentials for each guest by an authorized internal user.
- Keeps traffic on the guest network separate from the internal network in order to prevent a guest from accessing internal network resources.
- Supports both local-mode and Cisco FlexConnect design models.

Figure 4 - Wireless architecture overview



You can use a shared controller pair or a dedicated controller in the Internet demilitarized zone (DMZ) in order to deploy a wireless guest network.

If you have one controller pair for the entire organization and that controller pair is connected to the same distribution switch as the Internet edge firewall, you can use a shared deployment. In a shared deployment, a VLAN is created on the distribution switch in order to logically connect guest traffic from the WLCs to the DMZ. The VLAN will not have an associated Layer 3 interface or switch virtual interface (SVI), and the wireless clients on the guest network will point to the Internet edge firewall as their default gateway.

If you don't meet the requirements for a shared deployment, you can use Cisco 5500 or 2500 Series Wireless LAN Controllers in order to deploy a dedicated guest controller. The controller is directly connected the Internet edge DMZ, and guest traffic from every other controller in the organization is tunneled to this controller.

In both the shared and dedicated guest wireless design models, the Internet edge firewall restricts access from the guest network. The guest network is only able to reach the Internet and the internal DHCP and DNS servers.

Deployment Details

This design guide uses certain standard design parameters and references various network infrastructure services that are not located within the wireless LAN (WLAN). These parameters are listed in the following table. In the "Site-specific values" column, enter the values that are specific to your organization.

Network	service	CVD values	Site-spe
Table 1 -	Universal design parame	eters	

Network service	CVD values	Site-specific values
Domain name	cisco.local	
Active Directory, DNS server, DHCP server	10.4.48.10	
Network Time Protocol (NTP) server	10.4.48.17	
SNMP read-only community	cisco	
SNMP read-write community	cisco123	

Many organizations use the RADIUS protocol to authenticate users to both their wired and wireless networks. These access control systems (ACS) often integrate to a common local directory that contains specific information regarding the user. Common examples include an LDAP-based user directory as well as Microsoft Active Directory.

In addition to providing user authentication services, network components such as switches, wireless LAN controllers, routers, firewalls, and so forth require administrative authentication and authorization when used by the network administrator to perform maintenance and configuration support.

In order to provide a customizable granular authorization list for network administrators as to the level of commands that they are permitted to execute, the TACACS+ (Terminal Access Control Access Control System) protocol is commonly used. Both TACACS+ and RADIUS protocols are available when deploying the Cisco Secure ACS solution.

If your organization has an existing Microsoft RADIUS server that is used to authenticate end user access for remote VPN, dial-up modem, and so forth, it may be a good choice to deploy the wireless user authentication using the existing Microsoft RADIUS server. If however, your organization requires both TACACS+ for administrative access and RADIUS for wireless user authentication, the Cisco Secure ACS solution is the recommend choice. Cisco Secure ACS interfaces directly to an existing Microsoft Active Directory, eliminating the need to define users in two separate authentication repositories.

If you don't require a comprehensive ACS system that spans the entire organization's management and user access, a simple RADIUS server can be used as an alternative to Cisco Secure ACS.



For information about configuring the RADIUS server on Windows Server 2008, skip to the next process.

Cisco Secure Access Control System (ACS) is the centralized identity and access policy solution that ties together an organization's network access policy and identity strategy. Cisco Secure ACS operates as a centralized authentication, authorization, and accounting (AAA) server that combines user authentication, user and administrator access control, and policy control in a single solution.

Cisco Secure ACS 5.3 uses a rule-based policy model, which allows for security policies that grant access privileges based on many different attributes and conditions in addition to a user's identity.

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

Tech Tip

ĺ

It has been found that certain browsers may render Cisco Secure ACS differently. In some cases, a browser may omit fields that are required for proper configuration. It is recommended that you refer to the following Secure ACS 5.3 release notes in order to obtain a list of supported browsers:

http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.3/ release/notes/acs_53_rn.html#wp222016

Procedure 1 Create the wireless device type group

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

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

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

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

Network Resources >	Network Device Groups > Devi	ice Type > Create		
Device Group -	General			
😛 Name:	WLC			
Description:				
😛 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: On 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: In the Attribute Value list, choose Static, and then click Submit.

cisco Cisco Secure AC	S		a	csadmin acs (Primary)	
🕨 😚 My Workspace	Policy Elements > Authorization and	Permissions > Device Administ	ration > Shell Profiles > Edit: "WLC S	hel"	
Network Resources	Country Country Trate				
🕨 🎒 Users and Identity Stores	General Common Lasks	Custom Attributes			
🔹 🛞 Policy Elements	Common Tasks Attributes				
 Session Conditions 	Aunoute	Requirement	value		<u>^</u>
Date and Time					
 Network Conditions 					=
 Authorization and Permissions 					-
 Network Access Device Administration 					
Shell Profiles	Manually Entand				-
Command Sets	manually Entered				
Named Permission Objects	Attribute	Requirement	Value		
Access Policies	10181	wandatory	ALL		
Monitoring and Reports					_
System Administration					-
					-
	Add A Edit V	Replace A Delete			
	Attribute:				
	Requirement Mandatory	•			
	Attribute Static -	1			
	Value:				
			^		
			Ŧ		
	e Required fields				1.1
	Submit Cancel				

Procedure 3 Modify the device admin access 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 in 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.

The Custo policy cone	mize button in the low	wer ri e ava	ight area of the policy rules scree allable here for use in policy rules	en controls whic	h
onditions					
Identity Group:	in	•	All Groups:Network Admins	Select	
NDG:Location:	-ANY-				
NDG:Device Type:	not in	•	All Device Types:WLC	Select	
Time And Date:	-ANY-				
ihell Profile: Level 15			Select		

Next, you 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, and in the box, select All Groups:Network Admins.
- Step 7: Select NDG:Device Type, and 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.

Caparal		
Name: WLC Admin	Status: Enab	ablad –
WEC Admin	Status. Ellab	weu 🗸
The Custo	mize button in the low	wer right area of the policy rules screen controls which
policy cond	ditions and results are	e available here for use in policy rules.
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 She		Select
KCancel		Не

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: In the Based on Service Template box, select Network Access - Simple, and then click Next.

Access Policies > A	ccess Services > Cr	eate			
General	Allowed Protocols				
Step 1 - G	eneral				
General					
Name:	Wireless LAN				
Description	:				
Access Servic	e Policy Structure	9			
Based on	service template	Network Access - Simple	Select		
Based on	existing service		Select		
O User Sele	cted Service Type	Network Access 👻			
				Back Next	Einish 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 Rules pane, click Customize.

cisco Cisco Secure A	cs					acsadmin acs (Prim	aryy) Log-Out About Help	
► S ¹ My Workspace	Acces	ccess Policies > Access Services > Service Selection Rules						
In the second	0	Single (result sel	ection 💿 Rule based res	ult selection			
B Users and Identity Stores	Ser	vice Se	election F	olicy				
Policy Elements	Fit	er: Sta	atus	 Match if: Eq 	juals 👻	▼ ClearFilter 00 ▼		
Access Policies						Conditions	Results	
 Access Services 		13	Status	Name	Protocol	Compound Condition	Service	
 O Default Device Admin 	1		Θ	Remote Access VPN	match Radius	NDG:Device Type in All Device Types:ASA	Remote Access VPN	
 O Default Network Access 	2		Θ	Rule Wireless RADIUS	-ANY-	(RADIUS-IETF:Service-Type match Framed And RADIUS-IETF:NAS-Port-Type match Wireless - IEEE 802.11)	Wireless LAN	
 Remote Access VPN Wireless LAN 	3			Rule-1	match Radius	-ANY-	Default Network Access	
Identity	4	5		Rule-2	match Tacacs	-ANY-	Default Device Admin	
Authorization								
 Max User Session Policy Max Session User Settings 								
Max Session Group Settings	1							
Monitoring and Reports	Default If no rules defined or no enabled rule matches. DemyAccess							
🕨 💐 System Administration	Create. • Duplicate. • Edit Delete A Move to.							
	S	ave Ch	anges	Discard Changes				

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

Customize Conditions		
Available:	Selected:	
ACS Host Name Device Filter Device IP Address Device Port Filter End Station Filter	Protocol Compound Condition	
NDG:Device Type NDG:Location Time And Date UseCase	» «	
OK Cancel		

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

cisco Cisco Secure A	CS						acsadi	min acs (Primary)	Log Out About Help
My Workspace Morkspace Morkspace Output Detwork Resources Sources Sources	Access Stand Netv	s Policies lard Pol work Ac	: > Acces licy <u>Exce</u> :cess Au	s Services > Wire aption Policy (thorization Polic	less LAN > Authori:	zation			
Solution Policy Elements Solution Access Policies	Filte	er: Stat	lus	▼ Ma	tch if: Equals	•	Clear Filter Go] 💌	
Access Services Service Selection Rules			Status	Name	NDG:Location	Condition Time And Date	NDG:Device Type	Results Authorization Profiles	Hit Count
O Default Device Admin O Default Network Access O Remote Access VPN O Wireless LAN Identify	1		۲	WLC Access	-ANY-	-ANY-	in All Device Types:WLC	Permit Access	0
Authorization Max User Session Policy Max Session User Settings Max Monitoring and Reports	++ Cr	eate	Default Default	uplicate 💌 🛛	If no rules defin dit Delete	ed or no enabled r	ule matches.	Permit Access	0 hize Hit Count
🕨 🧐 System Administration	88	ave Cha	inges	Discard C	hanges				

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: Under Current Condition Set, click And > Insert.
- Step 16: In the Attribute box, select NAS-Port-Type.

Step 17: In the Value box, select Wireless - IEEE 802.11, and then click Add V.

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

General
Jame: Rule Wireless RADIUS Status: Enabled 🚽 🤒
The Customize button in the lower right area of the policy rules screen controls which policy conditions and results are available here for use in policy rules.
Conditions
Protocol: -ANY-
Compound Condition:
Condition:
RADIUS-IETF VAS-Port-Type Select
Operator: Value:
match 👻 Static 👻
Select
Current Condition Set:
Add V Edit A Replace V
And
RADIUS-IETF:Service-Type match Framed
And >RADIUS-IETF:NAS-Port-Type match wireless - 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 that allows the WLCs to use RADIUS in order to authenticate clients.

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 Acce	ss > Identity
Single resul	t selection \odot Rule based result sele	ction
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 then in the box, select All DeviceTypes:WLC.

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

General Name: WLC Access	Status: Enabled • •	
Conditions	-ANY-	
Ime And Date:	in Vite All Device Types WI C Select	
Identity Group:	-ANY-	
Authorization Profiles: Permit Access	You may select multiple authorization profiles. Attributes defined in multiple profiles will use the value from the first profile defined.	
Select Deselec		Help



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. For each controller and/or AP-SSO controller pair in the organization, you must create a network device entry in Cisco Secure ACS.

If you are configuring a 2500 series WLC which does not support AP-SSO, you will need to include both of their IP addresses in this step to authorize them to use the ACS authentication services.

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-1)

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

Step 4: In the IP box, enter the WLCs management interface IP address. (Example: 10.4.46.64)

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)

🔉 Name:	WLC-1		
Description:			
Network Device	Groups		
Location		All Locations	Select
Device Type		All Device Types:WLC	Select
IP Address			Authentication Options
Single II	P Address	s 💿 IP Range(s)	▼ TACACS+ 🔽
🔅 IP: 10.4.46	.64		Shared Secret: SecretKey
			Single Connect Device
			Legacy TACACS+ Single Connect Support
			TACACS+ Draft Compliant Single Connect Support
			→ RADIUS
			Shared Secret: SecretKey
			CoA port: 1700
			Enable KeyWrap
			Key Encryption Key:
			Message Authenticator Code Key:
			Key Input Format 💿 ASCII 🔘 HEXADECIMAL
Required fie	lds		

Procedure 7 Enable the default network device

Access points, when they are configured for Cisco FlexConnect operation and when the controller is unavailable, can authenticate wireless clients directly to Cisco Secure ACS. Enable the default network device for RADIUS in order to allow the access points to communicate with Secure ACS without having a network device entry.

Step 1: Navigate to Network Resources > Default Network Device.

Step 2: In the Default Network Device Status list, choose Enabled.

Next, you must show the RADIUS configuration.

Step 3: Under Authentication Options, click the arrow next to RADIUS.

Step 4: In the **Shared Secret** box, enter the secret key that is configured on the organization's access points, and then click **Submit**. (Example: SecretKey)

Network Resources > Default N	letwork Device				
The default device definiti IP address.	ion can optionally be used in cases where no specific d	evice definition is found that matches a device	•		
Default Network Device S	Status: Enabled 👻 \Theta				
Network Device Groups					
Location	All Locations	Select			
Device Type	All Device Types	Select			
Authentication Options					
▼ TACACS+					
Shared Secret: Sec	cretKey				
Single Connect Device					
Legacy TACACS+ Single Connect Support					
TACACS+ Draft Compliant Single Connect Support					
🕶 RADIUS 🛛 📝					
Shared Secret: Se	cretKey				
CoA port: 1700					
Enable KeyWra	ар				
Key Encryption Key	<i>r</i> .				
Message Authentic	ator Code Key:				
Key Input Format	🔿 ASCII 🔍 HEXADECIMAL				
Required fields					
Submit Cancel			•		



If you want to configure the RADIUS server on Cisco Secure ACS, use the previous process instead of this one.

The following procedures describe the steps required in order to enable RADIUS authentication for the WLC deployment. In this guide, the Windows Server 2008 Enterprise Edition has already been installed.

Tech Tip

ĺ

This procedure assumes that this is the first certificate authority (CA) in your environment. If it's not, you either don't need to install this role or you can configure this server as a subordinate CA instead.

Procedure 1 Install services

- Step 1: Join the server to your existing domain (Example: cisco.local), and then restart the server.
- Step 2: After the server restarts, open Server Manager.
- Step 3: Navigate to Roles >Add Roles. The Add Roles Wizard opens.

- Step 4: Follow the instructions in the wizard. Note the following:
 - On the Server Roles page, select Active Directory Certificate Services and Network Policy and Access Services.

Add Roles Wizard	uni	×
Select Server Rol	es	
Before You Begin Server Roles AD CS Role Services Setup Type CA Type Private Key Cryptography CA Name Validity Period Certificate Database Confirmation Progress Results	Select one or more roles to install on this server. Roles: Active Directory Certificate Services Active Directory Domain Services (Installed) Active Directory Federation Services Active Directory Fights Management Services Application Server DHCP Server (Installed) Fax Server Hyper-V Network Policy and Access Services (Installed) Price Services Remote Desktop Services Web Server (IDS) Windows Deployment Services Windows Server Update Services More about server roles	Description: <u>Active Directory Certificate Services</u> (AD CS) is used to create certification authorities and related roles services that allow you to issue and manage certificates used in a variety of applications.

- On the Role Services page, select Network Policy Server and Access Services, and then for Active Directory Certificate Services (AD CS), leave the default Certification Authority role service selected. You may not be able to select the Network Policy and Access Services option if it has been installed previously.
- On the Setup Type page, for Active Directory Certificate Services, choose Enterprise.
- On the CA Type page, choose Root CA.

Follow the rest of the instructions in the wizard, making any changes you want or just leaving the default values as appropriate. Note that there is a warning at the end of the wizard, stating that the name of this server cannot be changed after installing the AD CS role.

Now that you have a root CA and an NPS server on your domain, you can configure the domain.

Step 1: Open an MMC console, and then click File > Add/Remove Snap-in.

Step 2: Choose Certificates from the available snap-ins.

ilable snap-ins:			Selected snap-ins:	
ap-in	Vendor	^	Console Root	Edit Extensions.
ActiveX Control	Microsoft Cor			Remove
Authorization Manager	Microsoft Cor			Kelliove
Certificates	Microsoft Cor	Ξ		
Component Services	Microsoft Cor			Move Up
Computer Managem	Microsoft Cor			Maus Dawa
Device Manager	Microsoft Cor		Add	Move Down
Disk Management	Microsoft and			
Event Viewer	Microsoft Cor			
Folder	Microsoft Cor			
Group Policy Object	Microsoft Cor			
IP Security Monitor	Microsoft Cor			
IP Security Policy M	Microsoft Cor			
Link to Web Address	Microsoft Cor	-		Advanced
cription: e Certificates snap-in allo	ows you to browse	the	contents of the certificate stores for yourself, a serv	rice, or a computer.

Step 3: On the Certificates snap-in page, select Computer account, and then click Next.

Certificates snap-in		×
This snap-in will always manage certificates for:		
O My user account		
C Service account		
Computer account		
	< Back Next >	Cancel

Step 4: On the Select Computer page, select Local computer, and then click Finish.

Select Computer	x
Select the computer you want this snap-in to manage. This snap-in will always manage: C Local computer: (the computer this console is running on)	
C Another computer: Browse	
Allow the selected computer to be changed when launching from the command line. This only applies if you save the console.	
< Back Finish Cancel	

Next, add the Certification Authority snap-in.

Step 5: On the Add or Remove Snap-ins dialog box, in the Available snap-ins list, choose Certification Authority, click Add >, choose Local computer, and then click Finish.

ailable snap-ins:				Selected snap-ins:	
nap-in	Vendor	-		Console Root	Edit Extensions
Active Directory Do	Microsoft Cor			Certificate Templates	Remove
Active Directory Site	Microsoft Cor			Certificates (Local Computer)	Remove
Active Directory Use	Microsoft Cor			is Certification Authority (Local)	
📥 ActiveX Control	Microsoft Cor				Move Up
🖉 ADSI Edit	Microsoft Cor				
Authorization Manager	Microsoft Cor				Move Down
🖳 Certificate Templates	Microsoft Cor		Add >		
Certificates	Microsoft Cor				
Certification Authority	Microsoft Cor				
Component Services	Microsoft Cor				
Computer Managem	Microsoft Cor				
Device Manager	Microsoft Cor				
DHCP	Microsoft Cor				Adverse 1
🚅 Disk Management	Microsoft and	•]	Advanced
corintion					
scripcion;					
Illows you to configure cert	tification authority	prop	perties and to n	nanage certificates issued by this CA.	

Step 6: On the Add or Remove Snap-ins dialog box, in the Available snap-ins list, choose Certificate Templates. The RAS/IAS template is added.

Step 7: Click OK. This completes the process of adding snap-ins.

Step 8: Expand Certificates (Local Computers) > Personal, right-click Certificates, and then click Request new certificate.

Eonsole 1 - [Console Root\Certificates (L	.ocal Computer)\Personal]				- 🗆 ×
a File Action View Favorites Window	Help				_ 8 ×
🗢 ⇒ 🖄 🗊 📋 💁 📓 🖬					
Per Actor Vew Parartes Window Personal Control Parameters Personal Control Parame	Cohect Type Contractors Cohect Type Contractors	Al Task Alt Task Plew Window from Here Parfesh Help	Reguest Here Certificate Import Advanced Operations	Actions Personal More Actions Certificates More Actions	× 3 × 4
Request a new certificate from a certification author	ority (CA) in your domain			1	

Procedure 3 Enro

Enroll certificates

Step 1: Follow the instructions in Certificate Enrollment wizard. Note the following:

On the Select Certificate Enrollment Policy page, select Active Directory Enrollment Policy as the Enrollment policy for this certificate request.

Field Action Wew Favorites Window Holp Field Action	Console1 - [Console Root\Certificates (Lo	ocal Computer)\Personal]		- 🗆 ×
Control Certificate Enrollment Policy Certificate Enrollment Certificate	File Action View Favorites Window	Help		_ 17 ×
Constructions (and Computer) Conflictuates (🗇 🔿 🙍 🗊 📋 🙆 😖 🚺 📆			
Configured by you	Corroll Cond Consult Red Consult Red Consu	Celificate Enrollment Celificate Enrollment Certificate Enrollment Certificate Enrollment Policy Certificate Enrollment Policy Certificate Enrollment Policy Certificate Enrollment Policy Certificate Sectory Enrollment Policy Certificate Sectory Enrollment Policy Certificate E	Actions Personal Mere Actions Certificates Mere Actions	, , ,
	<u>د ا</u>			

• On the Request Certificates page, select **Domain Controller** and **Domain Controller Authentication** as the type of certificates that are being requested, and then click **Enroll**.

Console1 - [Console Root\Certificates (L	Computer)\Personal]				_ 🗆 ×
🔚 File Action View Favorites Window)				_181 ×
🗢 🔿 🔰 📅 📋 🙆 😹 🚺 📷					
Console Root	ert Tune			Actions	
Certificates (Local Computer)	Certificate Enrollment			Personal	
Trusted Root Certification Authorities	📮 Certificate Enrollment			More Actions	•
Enterprise Trust Intermediate Certification Authorities Trusted Debletare	Request Certificates			Certificates	
Untrusted Certificates Trid-Party Root Certification Authorit	You can request the following types of cer	tificates. Select the certificates you want to requ	est, and then dick Enroll.	More Actions	•
Invisted People Remote Desktop	Active Directory Enrollment F	olicy			
Certificate Enrolment Requests Smart Card Trusted Roots	Directory Email Replication	(1) STATUS: Available	Details 🛞		
Trusted Devices Gertification Authority (Local)	Domain Controller	STATUS: Available	Details 🛞		
🗉 🧟 Certificate Templates	Domain Controller Authentication	😲 STATUS: Available	Details 🛞		
	IPSec (Offline request)	STATUS: Available	Details 🛞		
	A More information is required in	o enroll for this certificate. Click here to configure	settings.		
	Web Server	STATUS: Available	Details 🛞		
	A More information is required I	o enroll for this certificate. Click here to configure	e settings.		
	C Show all templater				
	Learn more about certificates			1	
			Enroll Cancel		
					_
Personal store contains 6 certificates.					

Step 2: Navigate to **Certificate Authority (Local) > Issued Certificates**, and then verify that the Certificate Templates folder appears.

\begin{bmatrix} certsrv - [Certification Authority	(Local)\ADy\]	ssued Certificates	6]		×
File Action View Help					
🗢 🔿 🙎 🗟 🔒 👔					
Certification Authority (Local)	Request ID	Requester Name	Binary Certificate	Certificate Template	Ser
🖃 🧓 ADy	2	CISCO\ADY\$	BEGIN CERTI	Domain Controller Authentication (1.3.6.1.4	571
Revoked Certificates	3	CISCO\ADY\$	BEGIN CERTI	Domain Controller (DomainController)	578
Issued Certificates					
Pending Requests					
Falled Requests					
Certificate l'emplates					
			N		
			13		
1					

Step 3: Right-click the Certificate Templates folder, and in the right pane, right-click RAS and IAS Server, and then click Duplicate Template.

Certificate Templates (Directory Email Replication	Windows Server 2003 Ent	115	Certificate Templat	
	🗵 Domain Controller	Windows 2000	4.1		
	Domain Controller Authentication	Windows Server 2003 Ent	110	More Actions	
	🗟 EFS Recovery Agent	Windows 2000	6.1	DAE and TAE Someon	
	🚇 Enrollment Agent	Windows 2000	4.1	KAS aliu IAS Server	
	🗟 Enrollment Agent (Computer)	Windows 2000	5.1	More Actions	▶
	🗟 Exchange Enrollment Agent (Offline request)	Windows 2000	4.1		
	🗟 Exchange Signature Only	Windows 2000	6.1		
	🗟 Exchange User	Windows 2000	7.1		
	🗵 IPSec	Windows 2000	8.1		
	🚇 IPSec (Offline request)	Windows 2000	7.1		
	Rerberos Authentication	Windows Server 2003 Ent	110		
	🚇 Key Recovery Agent	Windows Server 2003 Ent	105		
	OCSP Response Signing	Windows Server 2008 Ent	101		
	RAS and TAC Comment	Windows Server 2003 Ent	101		
	Root Ce	Windows 2000	5.1		
	Router Reenroll AINCertificate Holders	Windows 2000	4.1		
	🖳 Smartca 🛛 All Tasks 🔹 🕨	Windows 2000	6.1		
	Rearter Smarter	Windows 2000	11.		
	Subordi Properties	Windows 2000	5.1		
	🖳 Trust Li Help	Windows 2000	3.1		
	🖳 User	Windows 2000	3.1		
	🚇 User Signature Only	Windows 2000	4.1		
	•		•		

Step 4: Select Windows Server 2008 Enterprise, and then click OK.



Step 5: In the Template display name box, enter a valid display name, select Publish Certificate in Active Directory, click Apply, and then close the MMC console.

Properties of New Template				
Issuance Requirements Superseded Templates Extensions Security General Request Handling Cryptography Subject Name Server				
Template display name: Copy of RAS and IAS Server for NPS				
Minimum Supported CAs: Windows Server 2008 Enterprise				
Template name: CopyofRASandIASServerforNPS				
Validity period: Renewal period: 1 years 6 weeks				
 Publish certificate in Active Directory Do not automatically reenroll if a duplicate certificate exists in Active Directory 				
For automatic renewal of smart card certificates, use the existing key if a new key cannot be created				
OK Cancel Apply Help				

Procedure 4 Register Server in Active Directory

Step 1: Open the Network Policy Server administrative console by navigating to Start > Administrative Tools > Network Policy Server.

Step 2: Right-click the parent node NPS (Local), click Register server in Active Directory, click OK to authorize this computer to read users' dial-in properties from the domain, and then click OK.

sNetwork Policy Server			
File Action View Help			
NP5 (Local) NP5 (Local) Import Configuration Import Configuration Import Configuration Export Configuration Import Configuration Start NP5 Service	rted Palicy Server (NPS) allows you to create and enforce organization-wide network access policies for client health, connection uthentication, and connection request authorization.		
Properties	nfiguration		
View	Introduction scenario from the list and then click the link below to open the scenario wizard		
Help			
Network Access Protection (NAP) Network Access Protection (NAP) When you configure NPS as a NAP health policy server, you create health policies that allow NPS to validate the configuration of NAP-coable cient computers before they connect to your network. Clients that are not compliant with health policy can be placed on a restricted network and automatically updated to bring them into compliance. Configure NAP Learn more			
Advanced	Configuration •		
Register server in Active Directory			

Step 3: With the NPS (Local) node still selected, select RADIUS server for 802.1X Wireless or Wired Connections, and then click Configure 802.1X.

🞭 Network Policy Server	
File Action View Help	
Impact International Internatina International International International International Intern	NPS (Local) Getting Started Image: Started started Image: Started started started Standard Configuration and connection request authorization. Standard Configuration Select a configuration scenario from the list and then click the link below to open the scenario wizard. RADIUS server for 802 TX Wireless or Wired Connections Network Access Protection (NAP) RADIUS server for 802 TX Wireless or Wired Connections RADIUS server for 802 TX Wireless or Wired Connections RADIUS server for 802 TX Wireless or Wired Connections RADIUS server for 802 TX Wireless or Wired Connections RADIUS server for 802 TX Wireless or Wired Connections RADIUS server for 802 TX Wireless or Wired Connections RADIUS server for 802 TX Wireless or Wired Connections RADIUS server for 802 TX Wireless or Wired Connections RADIUS server for 802 TX Wireless or Wired Connections RADIUS server for 802 TX Wireless or Wired Connections Cate and authorize connections from wireless access points and authenticating switches (also called RADIUS clients).
	Configure 802.1X Advanced Configuration Templates Configuration

Step 4: In the Configure 802.1X wizard, under Type of 802.1X connections, select **Secure Wireless Connections**, and in the **Name** box, enter an appropriate name for the policies that you want to create, and then click **Next**.

NPS (Local)	
Getting Started	
Network Policy Server (NPS) allows you to create and enforce organization-wide network access policies client health, connection request authentication, and connection request authorization.	for
Standard Configuration	
Select a configuration scenario from the list and then click the link below to open the scenario wizard.	
RADIUS server for 802.1X Wireless or Wired Connections	
Configure 802.1X	ls
Select 802.1X Connections Type	
 Type of 802.1X connections: Secure Wireless Connections When you deploy 802.1X wireless access points on your network, NPS can authenticate and authorize connection requests made by wireless clients connecting through the access points. Secure Wired (Ethernet) Connections When you deploy 802.1X authenticating switches on your network, NPS can authenticate and authorize connection requests made by Ethernet clients connecting through the switches. Name: This default text is used as part of the name for each of the policies created with this wizard. You can use the default text or modify it 	•
Secure Wireless Connections	ole CAs o
Previous Next Finish Cancel	

Next, add each of the wireless LAN controllers as RADIUS clients.

Step 5: In the **Friendly name** box, click **Add**, enter a name for the controller (Example: WLC5508), provide the IP address or DNS entry for the controller, provide the Shared Secret (Example: SecretKey), and then click **OK**.

ettings Select en existing template: Name and Address Friendly name: WLC5508 Address (IP or DNS): 10.4.46.64 Verify Shared Secret Select an existing Shared Secrets template: None To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive. Manual Generate Shared secret: OK Cancel	RADIUS Client			
Select an existing template: Name and Address Friendly name: (WLC5508 Address (IP or DNS): 10.4.46.64 Verify Shared Secret Select an existing Shared Secrets template: None To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive. Image: Manual Generate Shared secret:	ettings			
Select an existing template: Name and Address Friendly name: WLC5508 Address (IP or DNS): 10.4.46.64 Verify Shared Secret Select an existing Shared Secrets template: None To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive. Image: Manual Shared secret: Image: Manual Shared secret: <				
Name and Address Friendly name: WLC5508 Address (IP or DNS): 10.4.46.64 Verify Shared Secret Select an existing Shared Secrets template: None To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive. Manual G Generate Shared secret: Confirm shar	Select an existing	:emplate:		
Name and Address Friendly name: WLC5508 Address (IP or DNS): 10.4.46.64 Verify Shared Secret Select an existing Shared Secrets template: None To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive. Manual Generate Shared secret: Confirm shared				7
Friendly name: WLC5508 Address (IP or DNS): 10.4.46.64 Verify Shared Secret Select an existing Shared Secrets template: None T o manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive. Image: Manual Configure the Shared secret: Image:	Name and Address			
WLC5508 Address (IP or DNS): 10.4.46.64 Verify Shared Secret Select an existing Shared Secrets template: None To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive. Image: Manual Comparison of Generate Shared secret: Image: Manual Comparison of Gener	Friendly name:			
Address (IP or DNS): 10.4.46.64 Verify Shared Secret Select an existing Shared Secrets template: None To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive. Manual Generate Shared secret: Confirm shared secret: OK Cancel 	WLC5508			
I0.4.46.64 Verify Shared Secret Select an existing Shared Secrets template: None Image: Comparison of the secret s	Address (IP or DNS):			
Shared Secret Select an existing Shared Secrets template: None To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive. Manual G Generate Shared secret: Confirm shared secret: CON	10 4 46 64			Verifu
Shared Secret Select an existing Shared Secrets template: None To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive. Manual G Generate Shared secret: Confirm shared secret: OK Cancel	12014140104			
Select an existing Shared Secrets template: None To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive. Manual Generate Manual Generate Shared secret: Confirm shared secret: Manual Generate Manual Generate Mared secret: Mared secret: Mared secret: Mared secret: Mared secret: 	Shared Secret			
None Image: Constraint of the same shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive. Image: Manual image:	Select an existing Sh	ared Secrets template:		
To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive.	None			-
Confirm shared secret: OK Cancel	To manually type a si secret, click Generat secret entered here. Manual Shared secret:	nared secret, click Manual, e. You must configure the I Shared secrets are case-se O Generate	To automatically ge RADIUS client with t ensitive.	enerate a shared the same shared
Confirm shared secret:	•••••			
OK Cancel	Confirm shared secre	t		
OK Cancel	•••••			
OK Cancel				

Step 6: Click Next.

Step 7: On the Configure an Authentication Method page, in the Type box, select Microsoft: Protected EAP (PEAP), and then click Configure.

Configure 802.1X					x
Config	jure an Authenti	ication Metho	d		
Select the EAP type for this	policy.				
Type (based on method	of access and network	k configuration):			
Microsoft: Protected EAP (PEAP)			Configure	
			*//		
	Previou	us Next	Finish	Cancel	

Step 8: In the Certificate issued list, ensure that the certificate you enrolled in Step 6 is selected, and then click OK.

Edit Protected EAP Pro	perties	×
Select the certificate the A certificate that is conf Policy will override this c	e server should use to prove its identity to the a igured for Protected EAP in Connection Reques rertificate.	:lient. t
Certificate issued	AD.cisco.local	_
Friendly name:		
Issuer:	AD.cisco.local	
Expiration date:	3/15/2016 2:26:19 PM	
 Enable Fast Reconne Disconnect Clients wi Eap Types 	ect ithout Cryptobinding	
Secured password (EAP	-MSCHAP v2)	Yove Up ove Down
Add Ec	dit Remove OK	Cancel

Step 9: If you would like to use a group that you have already created, in Specify User Groups, click **Add**, select the desired group, and then skip to Step 11.

If you would like to create a new group, continue with this procedure.

Step 10: Navigate to **Start > Administrative Tools > Active Directory Users and Computers**. In the Active Directory Users and Computers window, right-click **cisco.local**, and then navigate to **New > Group**. Create a group called **Wireless-Users-Group**.

Active Directory Users and Computers			
File Action View Help			
🗢 🔿 🔰 🖬 📋 🗎 🖌	1 🔧 🐮 👕 🍸 🔟 🎉		
A Create in: dsco.local/ Group name: Wreless-Users-Group Group name (cre-Windows 2000); Wreless-Users-Group Group name (create in: dsco.local/ Gr	Image: Security	Type bulkinDomain Organizational Unit Container Container Container Organizational Unit Security Group - Global Container Organizational Unit	Description Default container for upgraded computer acco Default container for domain controllers Default container for security identifiers (SIDs Default container for managed service accour) Default container for upgraded user accounts
	OK Cancel		
	1		

Step 11: In the Active Directory Users and Computer management console, create a wireless user (Example: Wireless User) by selecting the **Action > New > User**.

📔 Active Directory Users and	Computers			
File Action View Help				
Delegate Control	K 🗉 🧟 🗟 🛛 🖬 🗏 🍇	s 🛅 🍸 🗾 🍇		
A	mputers [AD.cisci Name 🔶		Туре	Description 🔺
🕀 🧯 New 🕨 🕨	Computer		User	
🖃 🗿 All Tasks 🔹 🕨	Contact		User	
+ Refresh	Group		User	
+ Export List	InetOrgPerson		User	
	msExchDynamicDistributionList		User	
* Properties	msImaging-PSPs		User	
Help	MSMQ Queue Alias		User	
+ Microsoft Exchange S	Printer		User	
F CLUSERS	User	hoorthy	User	
	Shared Folder		User	
🔐 Wireless-Users-Group	🦓 vpn-administrat	or	Security Group - Global	
	🛛 🍇 vpn-employee	:	Security Group - Global	
	Vpn-partner		Security Group - Global	_
[•]				•
Create a new object				
Step 12: Provide the necessary user information, and then click Next..

New Object - User	×
👗 Create in:	cisco.local/Users
<u>F</u> irst name:	Wireless Initials:
Last name:	User
Full n <u>a</u> me:	Wireless User
User logon name: WirelessUser	@cisco.local
User logon name (pre	- <u>W</u> indows 2000):
CISCO\	WirelessUser
	< <u>B</u> ack <u>N</u> ext > Cancel

Step 13: Enter a password, and then click Next.

New Object - User	×
Create in: cisco.local/Users	
Password: •••••• Confirm password: •••••••	
 User must change password at next logon User cannot change password Password never expires Account is disabled 	
< <u>B</u> ack <u>N</u> ext >	Cancel

Step 14: Review the information about the new user being added, and click Finish.

New Object - User		×
🤱 Create in: cisco.loc	cal/Users	
When you click Finish, the follow	ing object will be created:	
Full name: Wireless User		<u>^</u>
User logon name: WirelessUser(@cisco.local	
The password never expires.		
J		<u> </u>
	< <u>B</u> ack Finish	Cancel

Step 15: Within the Active Directory Users and Computer management console, select the users folder.

Step 16: Locate the wireless user (Example: Wireless User) that you want to add to the newly created Wireless-Users-Group, and then right click on the user and select **Add to a group...**

Active Directory Users and Computers					
File Action View Help					
(= =) 🖄 🛅 🦌 🗎 🔀 🗟 🗟	🛛 🖬 🐮 🕯	8 🗄 🝸 🗾 🗞			
Active Directory Users and Computers [AD.cisc	Name 🔺			Туре	Descriptio 🔺
🕀 🧰 Saved Queries	🍇 Schema Admin	s		Security Group - Universal	Designate
🖻 🏭 cisco.local	💄 Stuart Higgins			User	
🕀 🛄 Builtin	👃 🗞 SystemMailbo>	:{1f05a927-cfb7-4ca4-a039-4	437d0c471	User	
E CitrixXen	🕹 SystemMailb	Copy 78-	-e6c29d823	User	
Computers	👃 Taylor Smith	Add to a group		User	
EoreignSecurityPrincipals	👗 TJ Schuler 🛛	Disable Account		User	
Mapaged Service Accounts	👗 User One	Reset Password		User	
Manages betwee Accounts Microsoft Exchange Security Groups	🏅 vdi-finance-1	Move		User	
	🕹 vdi-finance-2	Open Home Page		User	
	👗 vdi-hr-1	Send Mail		User	
& Wireless-Users-Group	🕹 vdi-hr-2	Find		User	
_	👗 vdi-it-1 👘	Oll Tacks		User	
	👗 vdi-it-2			User	
	🏅 vdi-research	Cut		User	
	🏅 vdi-research	Delete		User	
	🏅 Vignesh Sath	Rename		User	
	S VPN ASA552	Refresh		User	
	🔏 vpn-administ 🗌	Properties		Security Group - Global	
	💑 vpn-employe	Toperaes		Security Group - Global	
	🚜 vpn-partner	Help		Security Group - Global	
	🍝 Wireless User			User	
٠	•				
Allows you to add the selected objects to a group you	u select.				

Step 17: Enter the name of the Wireless-Users-Group, and then click Check Names.

Select Groups		? ×
Select this object type:		
Groups or Built-in security principals		Object Types
From this location:		
cisco.local		Locations
Enter the object names to select (examples):		
Wireless-Users-Group		Check Names
		_
Advanced	ОК	Cancel

Step 18: Click OK. This completes the process of adding the user to the wireless group.

Select Groups		? ×
Select this object type:		
Groups or Built-in security principals	<u>O</u> bject Type	s
Erom this location:		
cisco.local	Locations	
Enter the object names to select (<u>examples</u>):		
Wireless-Users-Group	<u>C</u> heck Nam	es
<u>A</u> dvanced	OK Cance	



Step 19: On the next step of the Network Policy Server (NPS (Local)) wizard, configure VLAN information or accept the default settings, and then click **Next**.

Step 20: Click Finish. This completes the configuration of 802.1X.

Configure 802.	1X	×					
	Completing New IEEE 802.1X Secure Wired and Wireless Connections and RADIUS clients						
You have succe • To view the c • To change the • To save the c	You have successfully created the following policies and configured the following RADIUS clients. • To view the configuration details in your default browser, click Configuration Details. • To change the configuration, click Previous. • To save the configuration and close this wizard, click Finish.						
Connection F Secure Wireless Network Polie Secure Wireless	Request Policy: s Connections 2 cies: s Connections 2						
	Previous Next Finish Cancel						

Step 21: Restart the Network Policy Server service, and then navigate to NPS (Local) > Policies.

Note that the wizard has created a Connection Request Policy and a Network Policy containing the appropriate settings in order to authenticate your wireless connection.

🛸 Network Policy Server	
File Action View Help	
🗢 🔿 🔁 🖬 🚺 🖬	
NPS (Local) RADIUS Clients and Servers RADIUS Clients Remote RADIUS Server G Policies Connection Request Polici Network Policies Health Policies Network Access Protection	Network Policies Network policies allow you to designate who is authorized to connect to the network and the circumstances under which they can or cannot connect. Policy Name Status Processing Order Access Type S Secure Wireless Connections to Microsoft Routing and Remote Access server Enabled 1 Grant Access U
Accounting Templates Management	Conditions - If the following conditions are met: Condition Value NAS Port Type Wireless - Other OR Wireless - IEEE 802.11 Windows Groups CISCO\SBA-Users
	Settings - Then the following settings are applied: Setting Value Extensible Authentication Protocol Configuration Configured

Step 22: If you want to remove the less secure authentication methods and increase the encryption methods in the network policy, continue with this procedure.

If you would like to use the default authentication and encryption methods, skip to the next process.

Step 23: Under the Network Policies node, open the properties of the newly created policy.

Step 24: On the Constraints tab, under Less secure authentication methods, clear all of the check boxes.

Secure Wireless Connections Properties		×
Overview Conditions Constraints Setting		
Overview Conditions Constraints Setting Configure the constraints for this network politing all constraints are not matched by the constraints: Constraints Constraints Authentication Methods Image: Constraints Mathentication Methods Image: Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Called Timeout Session Timeout Constraints Called Station ID Constraints Constraints Called Station ID Constraints Constraints NAS Port Type NAS Port Type Constraints	by: ection request, network access is denied. Allow access only to those clients that authenticate with the specified methods. EAP types are negotiated between NPS and the client in the order in which they are listed. EAP Types: Microsoft: Protected EAP (PEAP) Move Up Move Down Add Edit Remove Less secure authentication methods: Microsoft Encrypted Authentication version 2 (MS-CHAP-v2) User can change password after it has expired Microsoft Encrypted Authentication (CHAP) User can change password after it has expired Encrypted authentication (CHAP) Add Hereorypted authentication (PAP, SPAP) Allow clients to connect without negotiating an authentication method	-
	OK Cancel Apply	

Step 25: On the Settings tab, click Encryption, clear all check boxes except Strongest encryption (MPPE 128bit), and then click OK.

Overview Conditions Constraints Settings Configure the settings for this network policy. If conditions and constraints match the connection request and the policy grants access, settings are applied. Settings: Image: Conditions and constraints match the connection request and the policy grants access, settings are applied. Settings: Image: Conditions and constraints match the connection request and the policy grants access, settings are applied. Vendor Specific Image: Conditions and Constraints NAP Enforcement Image: Condition and Constraints Image: Conditions and Remote Access Image: Condition access clients to the network access server is not secured by encryption. This configuration is not recommended. Image: Conditions and Remote Access Image: Condition access clients to the network access server is not secured by encryption. This configuration is not recommended. Image: Condition Protocol (BAP) Image: Condition Protocol (BAP) Image: Condition Protocol (BAP) Image: Condition Protocol (MPPE 128-bit) Image: Condition Protocol (BAP) Image: Condition Protocol (MPPE 128-bit) Image: Condition Protocol (BAP) Image: Condition Protocol (MPPE 128-bit) Image: Condition Protocol (BAP) Image: Condition Protocol (MPPE 128-bit) Image: Condition Protocol (Condition Protocol (Condition) Image: Condition) <	Secure Wireless Connections Properties		×
Configure the settings for this network policy. Conditions and constraints match the connection request and the policy grants access, settings are applied. Settings	Overview Conditions Constraints Setting	s	
No encryption	Overview Conditions Constraints Setting: Configure the settings for this network policy, if conditions and constraints match the connormality of conditions and constraints match the connormatic settings: Settings: RADIUS Attributes Image: Standard Image: Vendor Specific Network Access Protection Image: Extended State Routing and Remote Access Image: UP Filters Image: Encryption Image: Encryption		_
OK Cancel Apply	K Settings	No encryption	

Step 26: Restart the Network Policy Server service.



In an on-site local-mode deployment, the wireless LAN controller and access points are co-located. The wireless LAN controller is connected to a LAN distribution layer at the site, and traffic between wireless LAN clients and the LAN is tunneled in Control and Provisioning of Wireless Access Points (CAPWAP) protocol between the controller and the access point.

If you are deploying remote access points using FlexConnect, skip this section and proceed to the FlexConnect section of the guide.

This design guide supports both Cisco 5500 and 2500 Series WLCs for use in an on-site local-mode design. When installing 5500 Series WLCs, a high availability feature known as access point stateful switchover (AP SSO) is available. In this high availability mode, the resilient, or *secondary*, WLC uses the redundancy port in order to negotiate with its configured primary WLC and assumes the AP license count along with the configuration of the primary WLC.

In AP SSO mode, configuration synchronization and keep-alive monitoring occurs over a dedicated redundancy port (labeled as RP) using a dedicated straight through Ethernet cable.

The Cisco 2500 Series WLCs do not support the AP SSO feature and instead must be peered by using a mobility group in order to achieve resiliency. Unlike AP-SSO paired Wireless LAN Controllers, each Cisco 2500 Series WLC has a unique IP address on the management interface.

Table 2 - Cisco on-site wireless controller parameters checklist

Parameter	CVD values primary controller	CVD values resilient controller (optional)	Site-specific values
Controller parameters	1	1	
Switch interface number	1/0/3, 2/0/3	1/0/4, 2/0/4	
VLAN number	146	146	
Time zone	PST -8 0	PST -8 0	
IP address	10.4.46.64/24	10.4.46.65/242	
Default gateway	10.4.46.1	10.4.46.1	
Redundant management IP address (AP SSO)1	10.4.46.741	10.4.46.75 ¹	
Redundancy port connectiv- ity (AP SSO) ¹	Dedicated Ethernet cable ¹	Dedicated Ethernet cable ¹	
Hostname	WLC-1	WLC-2 ²	
Local administrator username and password	admin/C1sco123	admin/C1sco123	
Mobility group name	CAMPUS	CAMPUS	
RADIUS server IP address	10.4.48.15	10.4.48.15	
RADIUS shared key	SecretKey	SecretKey	
Management network (optional)	10.4.48.0/24	10.4.48.0/24	
TACACS server IP address 10.4.48.15 (optional)		10.4.48.15	
TACACS shared key (optional)	SecretKey	SecretKey	
Wireless data network parame	ters		
SSID	WLAN-Data	WLAN-Data	
VLAN number	116	116	
Default gateway	10.4.16.1	10.4.16.1	
Controller interface IP address	10.4.16.5/22	10.4.16.6/22	
Wireless voice network parame	eters		
SSID	WLAN-Voice	WLAN-Voice	
VLAN number	120	120	
Default gateway	10.4.20.1	10.4.20.1	
Controller interface IP address	10.4.20.5/22	10.4.20.6/22	

Notes:

- 1. AP SSO is only supported on the Cisco 5500 Series WLC.
- 2. The resilient Cisco 2500 Series WLC will require an IP address, as AP SSO is not supported on this platform.

Step 1: On the LAN distribution switch, create the wireless VLANs that you are connecting to the distribution switch. The management VLAN can contain other Cisco appliances and does not have to be dedicated to the WLCs.

vlan 116 name WLAN_Data vlan 120 name WLAN_Voice vlan 146 name WLAN_Mgmt

Step 2: Configure a switched virtual interface (SVI) for each VLAN. This enables devices in the VLAN to communicate with the rest of the network.

```
interface Vlan116
description Wireless Data Network
ip address 10.4.16.1 255.255.252.0
no shutdown
!
interface Vlan120
description Wireless Voice Network
ip address 10.4.20.1 255.255.252.0
no shutdown
!
interface Vlan146
description Wireless Management Network
ip address 10.4.46.1 255.255.255.0
no shutdown
```

Step 3: On both the server room distribution and access switches, create the wireless management and data VLANs.

```
vlan 116
name WLAN_Data
vlan 120
name WLAN_Voice
vlan 146
name WLAN Mgmt
```

Step 4: On the server room distribution switch, configure two uplink ports and an EtherChannel trunk to the server room access switches.

```
interface Port-channel12
description EtherChannel Link to Server Room Switch
switchport
switchport trunk allowed vlan 116,120,146
switchport mode trunk
logging event link-status
flowcontrol receive on
no shutdown
interface range tenGigabitEthernet [port 1],tenGigabitEthernet [port 2]
description Link to Server Room Switch
switchport trunk allowed vlan 116,120,146
switchport mode trunk
channel group 12
logging event link-status
logging event trunk-status
no shutdown
```

Step 5: On the server room access switches, configure two ports and an EtherChannel trunk that connects to the server room distribution switch.

```
interface range GigabitEthernet1/1/1, GigabitEthernet2/1/1
description Link to Distribution Switch
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 116,120,146
switchport mode trunk
logging event link-status
logging event trunk-status
logging event bundle-status
macro apply EgressQoS
channel-protocol lacp
channel-group 1 mode active
no shutdown
interface Port-channel1
description EtherChannel Link to Distribution Switch
switchport trunk encapsulation dotlq
switchport trunk allowed vlan 116,120,146
switchport mode trunk
logging event link-status
no shutdown
```

Step 6: Configure an 802.1Q trunk to be used for the connection to the WLCs. This permits Layer 3 services to all the networks defined on the WLC. The VLANs allowed on the trunk are limited to only the VLANs that are active on the WLC.

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

```
interface GigabitEthernet [port 1]
description To WLC Port 1
interface GigabitEthernet [port 2]
description To WLC Port 2
Т
interface range GigabitEthernet [port 1], GigabitEthernet [port 2]
  switchport
 macro apply EgressQoS
  channel-group [number] mode on
  logging event link-status
  logging event trunk-status
  logging event bundle-status
1
interface Port-channel [number]
description To WLC
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 116,120,146
 switchport mode trunk
logging event link-status
no shutdown
```

Procedure 2 Connecting the redundancy port

If you are using a Cisco 2500 Series WLC, skip this procedure. If you are using a Cisco 5500 Series WLC and you wish to enable the high availability AP SSO feature, continue with this procedure. When using the high availability feature known as access point stateful switchover (AP SSO), a dedicated special-purpose port is available on the Cisco 5500 Series WLC. This port is located on the in the lower left of the front panel.



Step 1: Connect an ordinary Ethernet cable between the primary and standby WLC, as shown below.

Procedure 3 Configure the WLC platform

After the WLC is physically installed and powered up, you will see the following on the console. If you do not see this, press "-" a few times to force the wizard to back to the previous step.

Welcome to the Cisco Wizard Configuration Tool Use the '-' character to backup

Step 1: Terminate the autoinstall process.

Would you like to terminate autoinstall? [yes]: YES

Step 2: Enter a system name. (Example: WLC-1)

System Name [Cisco 7e:8e:43] (31 characters max): WLC-1

Step 3: 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 4: If you are deploying a Cisco 5500 Series Wireless LAN Controller, use DHCP for the service port interface address.

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

Step 5: Enable the management interface.

```
Enable Link Aggregation (LAG) [yes][NO]: YES
Management Interface IP Address: 10.4.46.64
Management Interface Netmask: 255.255.255.0
Management interface Default Router: 10.4.46.1
Management Interface VLAN Identifier (0 = untagged): 146
```

Tech Tip

1

If you are configuring the Cisco 2500 Series Wireless LAN Controllers, you will need to configure both WLCs individually as they do not support AP-SSO and are therefore managed and configured separately. (Examples: 10.4.46.64 for WLC-1 and 10.4.46.65 for WLC-2)

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, enable AP SSO in order to enable high availability.

Enable HA [yes][NO]: YES Configure HA Unit [PRIMARY][secondary]: PRIMARY Redundancy Management IP Address: 10.4.46.74 Peer Redundancy Management IP Address: 10.4.46.75

Step 8: The virtual interface is used by the WLC for mobility DHCP relay, guest web authentication and intercontroller communication. Enter an IP address that is not used in your organization's network. (Example: 192.0.2.1)

Virtual Gateway IP Address: 192.0.2.1

Step 9: If you are configuring a Cisco 2500 Series Wireless LAN Controller, enter a multicast address for delivery of IP multicast traffic by using the multicast-multicast method. This multicast address will be used by each AP in order to listen for incoming multicast streams from the wireless LAN controller. (Example: 239.1.1.)

Multicast IP Address: 239.1.1.1

Step 10: Enter a name for the default mobility and RF group. (Example: CAMPUS)

Mobility/RF Group Name: CAMPUS

Step 11: Enter an SSID for the WLAN 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: Enable DHCP snooping.

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

Step 13: Do not configure the RADIUS server now. You will configure the RADIUS server later by 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 restarts without saving the configuration, and you have to complete this procedure again. Please wait for the "Configuration saved!" message before power-cycling the Wireless LAN Controller.

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 by using the credentials defined in Step 3. (Example: https://wlc-1.cisco.local/)

Procedure 4 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.

սիսիս							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	<u>F</u> EEDBACK
Commands	Set Time						Set	Date and [•]	Time Set Timezone
Download File Upload File Rebeat	Current Ti	me	Tue May 31 11:07	:38 2011					
Config Boot	Date							_	
Scheduled Reboot			Month		May	•			
Reset to Factory Default			Day Year		31 ¥ 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 Cana	ida) 🔻		
	Foot Notes	5							
	1. Automatica	ally sets de	aylight savings tim	e where used.					



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.

							Sa <u>v</u> e Cor	nfiguration <u>P</u> ing	Logout <u>R</u> efresh
cisco	MONITOR V	MLANs		WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP FEEDBAC	ж
Management	SNMP v1 / v	v2c Co	mmunity > N	ew				< Back	Apply
Summary SNMP General SNMP V3 Users Communities Trap Receivers Trap Logs HTTP-HTTPS Telnet-SSH Serial Port	Community I IP Address IP Mask Access Mode Status	Name	cisco 10.4.48.0 255.255.255.0 Read Only V Enable V						
Local Management User's Cessions > Logs Mgmt Via Wireless > Software Activation > Tech Support									

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.

սիսիս							Sa <u>v</u> e Cor	nfiguration <u>P</u> ing Logout <u>R</u> efres
cisco	MONITOR	<u>W</u> LANs	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP FEEDBACK
Management	SNMP v1	/ v2c Co	ommunity > N	ew				< Back Apply
Summary Summary SMMP General SNNP V3 Users Communities Trap Receivers Trap Logs HTTP-HTTPS Telnet-SSH Serial Port Local Management Users User Sessions Logs	Communit IP Address IP Mask Access Mc Status	ty Name s	cisco123 10.4.48.0 255.255.255.0 Read/Write • Enable •					< back Appny
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 string. You should have only the read-write and read-only community strings, as shown in the following screenshot.

սիսիս							Sa <u>v</u> e Co	nfiguration	n <u>P</u> ing	Logout <u>R</u> efresh
cisco	MONITOR	<u>W</u> LANs		WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	FEEDBAC	ск
Management	SNMP v1	/ v2c Co	ommunity							New
Summary										
▼ SNMP	Communit	y Name		IP Address	IP Mask	Access	Mode Status	;		
General	cisco			10.4.48.0	255.255.2	55.0 Read-Or	ly Enable			
SNMP V3 Users	cisco123			10.4.48.0	255.255.2	55.0 Read-Wi	ite 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										

(Optional)

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

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

Step 2: Enter an access control list name (Example: ACL-Rules), select **IPv4** as the ACL type, and then click **Apply**.

Step 3: In the list, choose the name of the access control 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

արտիս							Sa <u>v</u> e Co	nfiguratio	n <u>P</u> ing Lo	gout <u>R</u> efre
cisco	MONITOR	WLANs	CONTROLLER	WIRELESS	SECURITY	MANAGEMEN	COMMANDS	HELP	FEEDBACK	
Security	Access C	ontrol L	ists > Rules >	New					< Back	Apply
AAA	Sequence		1							
Local EAP Priority Order	Source		IP Address	•	IP Addr 10.4.4	ess 8.0	Netmask 255.255.255.0			
Certificate	Destination		Any	-						
 Access Control Lists Access Control Lists 	Protocol		TCP	•						
CPU Access Control Lists FlexConnect ACLs	Source Port		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 using the configuration details in the following table.

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

Table 3 - Access rule configuration values

ululu cisco	MONI	ITOR	<u>W</u> LANs		OLLER WIRELES		MANAGEMENT	C <u>O</u> MMANDS	HELP	EEEDBACK			Sa <u>v</u> e Cont	iguration	<u>Ping Logout R</u> efresh
Security	Acce	ess Co	ontrol l	.ists > Ec	lit								< Bac	k 📃	Add New Rule
AAA Local EAP Priority Order Certificate Access Control Lists Access Control Lists CPU Access Control Lists	Gene Acces Deny Seq	eral Is List N Counte Action	ame rs n Sou	ACL-R 0 rce IP/Ma	ules sk	Destination IP/Mask	1	Protoc	ol	Source Port	Dest Port	DSCP	Direction	Number of Hits	
Lists FlexConnect ACLs	1	Permit	t 10.4	.48.0	/ 255.255.255.0	0.0.0	/ 0.0.0.0	TCP		Anγ	HTTPS	Any	Any	0	
Wireless Protection	2	Permit	t 10.4	.48.0	/ 255.255.255.0	0.0.0.0	/ 0.0.0.0	TCP		Any	22	Any	Any	0	
Policies	3	Deny	0.0.	0.0	/ 0.0.0.0	0.0.0	/ 0.0.0.0	TCP		Any	HTTPS	Any	Any	0	
▶ Web Auth	4	Deny	0.0.	0.0	/ 0.0.0.0	0.0.0.0	/ 0.0.0.0	TCP		Any	22	Any	Any	0	
TrustSec SXP	5	Permit	t 0.0.	0.0	/ 0.0.0.0	0.0.0.0	/ 0.0.0.0	Any		Anγ	Αηγ	Any	Any	0	
Advanced															

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 7 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.

1 1		Save Configuration Ping Longuit Refresh
cisco	MONITOR WLANS CONTROLLE	ER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Security	RADIUS Authentication Service	vers > New Apply
AAA General KADIUS Authentication Accounting Failback TACACS+ LDAP Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies	Server Index (Priority) Server IP Address Shared Secret Format Shared Secret Confirm Shared Secret Key Wrap Port Number Server Status	1 • 10.4.48.15
Local EAP	Server Timeout	2 seconds
 Priority Order Certificate Access Control Lists Wireless Protection Policies Web Auth TrustSec SXP Advanced 	Network User Management IPSec	 Enable Enable Enable

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										Logout <u>R</u> efresh
cisco	MONITOR	<u>W</u> LANs		WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACk	(
Security AAA General RADIUS Authentication Accounting Fallback TACACS+ LOAP Local Net Veers MAC Filtering Disabled Clients User Login Policies AD Relieve	RADIUS / Server In Server IP Shared Se Shared Se Confirm S Port Num Server St Server Tir	dex (Priorit Address ecret Forma ecret ishared Secr ber atus meout	() 1 () 1 .	New .48.15 I .]			- Back	Apply
Password Policies Local EAP Priority Order	IPSec	Jser	E	nable Enable						
Certificate										
 Access Control Lists Wireless Protection Policies Web Auth TrustSec SXP Advanced 										

(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 to Procedure 9.

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, it controls all management access to the network infrastructure devices (SSH and HTTPS).



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)

alialia –							nfiguration <u>P</u> ing	Logout <u>R</u> efresh
cisco	MONITOR WLANS		WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP FEEDBACH	ĸ
Security	TACACS+ Authe	entication Serv	ers > New				< Back	Apply
AAA General FRADUS TACACS+ Authentication Accounting Authonization LoaP Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies Password Policies	Server Index (Prioi Server IP Address Shared Secret Forr Shared Secret Confirm Shared Se Port Number Server Status Server Timeout	rity) nat	1 • 10.4.48.15 ASCII • ••••••• 49 Enabled • 5 second	Is				
Local EAP								
Priority Order								
Certificate								
Access Control Lists								
Wireless Protection Policies								
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)

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)

ahaha									n <u>P</u> ing Lo <u>g</u> out <u>R</u> efre	
CISCO	MONITOR	<u>W</u> LANs		WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK	
Security	TACACS+	+ Author	ization Serve	rs > New					< Back Apply	
General RADIUS TACACS+ Authentication	Server IP Shared Se	Address cret Forma	it	10.4.48.15 ASCII 👻						
Accounting Authorization LDAP	Shared Se Confirm Si Port Numb	cret hared Secr	et	•••••						
Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies Password Policies	Server Sta	atus neout		Enabled • 5 secon	ds					
Local EAP										
Priority Order										
Certificate										
Access Control Lists										
 Wireless Protection Policies 										
▶ Web Auth										
IrustSec 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.

սիսիս							Sa <u>v</u> e Cor	nfiguratior	ı <u>P</u> ing Lı	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	Priority C	order > N	lanagement l	Jser						Apply
Security AAA Local EAP Certificate Access Control Lists Wireless Protection Policies Web Auth TrustSec SXP Advanced	Authentic Not RADIL	ation Used US + elected as f first prior	second priority the	ISET Order U In user will be	sed for Auther	ntication Up Down	0			Apply

Procedure 9 Enable multicast support

Some data and voice applications require the use of multicast in order to provide a more efficient means of communication typical in one-to-many communications. The local mode design model tunnels all traffic between the AP and WLC. As a result, the WLC issues all multicast joins on behalf of the wireless client.

Step 1: In Controller > Multicast, select Enable Global Multicast Mode and Enable IGMP Snooping, and then click Apply.

ahaha										Logout <u>R</u> efresh
cisco		<u>W</u> LANs		WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK	_
Controller	Multicast]	Apply
General Inventory Interfaces Interface Groups Multicast Network Routes Redundancy Internal DHCP Server Mobility Management Ports	Enable G Enable I IGMP Tin IGMP Qu Enable M MLD Tim MLD Que	lobal Multic GMP Snoopi neout (seco ery Interva LD Snoopin eout (secon ry Interval	ast Mode version of the second							
 CDP PMIPv6 IPv6 Advanced 										



Step 3: If you are using Cisco 5500 Series wireless LAN controllers, in the **AP Multicast Mode** list, choose **Multicast**, and then in the box, enter the multicast IP address that is to be used for multicast delivery (example: 239.1.1.1), and then click **Apply**.

If you are using a Cisco 2500 Series wireless LAN controller, in the **AP Multicast Mode** box, enter the multicast IP address that was configured in Step 8 of the "Configure the WLC platform" procedure, and then click **Apply**.

								Sa <u>v</u> e Co		ng Logout <u>R</u> efresh
CISCO	MONITOR	<u>W</u> LANs	<u>C</u> ONTROLLER	WIRELESS	<u>S</u> ECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK	
Controller	General									Apply
Controller General Inventory Interfaces Interface Groups Multicast Network Routes Redundancy Internal DHCP Server Nobility Management Ports NTP CDP CDP PMIPv6 IPv6 MDNS Advanced	General Name 802.3x Fl LAG Mod Broadcas AP Multic AP Fallba Fast SSI Default M RF Group User Idle ARP Timo Web Rad Operatin Internal WebAuth Gibbal IP	low Control e on next re t Forwardin ast Mode & lok D change Nome Timeout (s eout (secon ius Authent g Environm Proxy Redi Proxy Redi	Mode eboot ng nain Name ieconds) ds) ication ent Limits irection Port	WLC-1-Prime Disabled • Enabled • Disabled • Disabled • Disabled • CAMPUS CAMPUS 300 300 PAP Commercial 0 to 65 C Disabled • 0 Enabled •	239.1.1.1	Multicast G	(LAG Mode is cu	irrently er	nabled).	Apply

Procedure 10 Create the WLAN data interface

Configure the WLC 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.

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: 116)

alialia –							Sa <u>v</u> e Co	nfiguration <u>P</u> in	g Logout <u>R</u> efresh
cisco	MONITOR	<u>W</u> LANs		WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP FEED	ВАСК
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-data						

Step 4: If you are deploying a Cisco 2500 Series Wireless LAN Controller, in the **Port Number** box, enter the number of the port that is connected to the LAN distribution switch. (Example: 1)

Step 5: In the IP Address box, enter the IP address assigned to the WLC interface. (Example: 10.4.16.5)

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 Procedure 1. (Example: 10.4.16.1)

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

սիսիս							Sa <u>v</u> e Cor	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 FEEDBAC	ж
Controller	Interfaces	s > Edit						< Back	Apply
CISCO Controller General Inventory Interfaces Interface Groups Multicast Network Routes Internal DHCP Server Mobility Management Ports NTP COP Advanced	MONITOR Interfaces General I Interface Mac Addr Guest Lan Quarantin Quarantin Quarantin Quarantin Physical I The interf Enable Oy Managem Interface VLAN Ider IP Address Netmask Gateway DHCP Info Primary D Secondary Access Co	WLANS WLANS S > Edit Name ess tion f e e Van Id nformat ace is attan Address Address comation HCP Serve y DHCP Serve anto Lis	CONTROLLER ion wireless 00:24: 0 ion ion ion ion ion ion ion ion	s-data 97:69:dd:6f 52.0	SECURITY	MANAGEMENT	CQMMANDS	HELP FEEDBAC	Apply
	ACL Name		-	none 🔻					
	Note: Chang temporarily o some clients.	ing the Inte disabled an	erface parameters d thus may result	causes the WL in loss of conn	ANs to be ectivity for	-			

Tech Tip

1

To prevent DHCP from assigning wireless clients addresses that conflict with the WLC's addresses, exclude the addresses you assign to the WLC interfaces from DHCP scopes.

Procedure 11 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: 120)

							Sa <u>v</u> e Cor	nfiguration <u>P</u> ing L	.ogout <u>R</u> efresh
cisco	MONITOR	<u>W</u> LANs	<u>C</u> ONTROLLER	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 v	vireless-voice 20						

Step 4: If you are deploying a Cisco 2500 Series Wireless LAN Controller, in the **Port Number** box, enter the number of the port that is connected to the LAN distribution switch. (Example: 1)

Step 5: In the IP Address box, enter the IP address assigned to the WLC interface. (Example: 10.4.20.5)

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 Procedure 1. (Example: 10.4.20.1)

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

CISCO MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HEIP FEEDBACK Controller Interfaces > Edit Apply General Interfaces > Edit Apply Interfaces Interface Name wireless-voice Apply Multicast Mac Address 00:24:97:69:dd:6f <	սիսիս	ili.				Sa <u>v</u> e Co	nfiguration <u>P</u> ing I	Logout <u>R</u> efresh
Controller Interfaces > Edit Apply General Inventory General Information Interfaces Interface Name wireless-voice Interface Groups MAC Address 00:24:97:69:dd:6f Match address 00:24:97:69:dd:6f Interface Network Routes Configuration Interface Ports Quarantine Quarantine Quarantine Quarantine Interface is attached to a LAG. Enable Dynamic AP Management Interface Address VAN Identifier	cisco	CO <u>M</u> ONITOR <u>W</u> LAN	<u>C</u> ONTROLLER WIR	eless <u>s</u> ecurity	MANAGEMENT	C <u>O</u> MMANDS	HELP FEEDBACK	(
General General Information Interfaces Interface Address Interface Groups MaC Address Maticast MaC Address Network Routes Configuration Interface Name wireless-voice Mobility Management Quarantine Ports Quarantine Quarantine Quarantine Interface is attached to a LAG. Enable Dynamic AP Management VAN Identifier	Controller	Interfaces > Ed	t				< Back	Apply
IP Address 10.4.20.5 Netmask 255.255.252.0 Gateway 10.4.20.1 DHCP Information Primary DHCP Server 10.4.48.10 Secondary DHCP Server 10.4.48.10 Access Control List ACL Name Note: Changing the Interface parameters causes the WLANs to be	Controller General Inventory Interfaces Interface Groups Multicast Network Routes Internal DHCP Server Mobility Management Ports NTP COP Advanced	s Groups Groups Groups Groups Groups Groups Guest Lan Guarantine Quarantine Quarantine Quarantine The interface is at Enable Dynamic A Management Interface Address Netmask Gateway DHCP Informati Primary DHCP Set Secondary	t tion wireless-voice 00:24:97:69: 0 tion ached to a LAG. b tion tion tion tion tion tion tion tion	id:6f			< Back	Apply

Tech Tip

i

To prevent DHCP from assigning wireless clients addresses that conflict with the WLC's addresses, exclude the addresses you assign to the WLC interfaces from DHCP scopes.

Procedure 12 Configure the data wireless LAN

Wireless data traffic can tolerate delay, jitter, and packet loss more efficiently than wireless voice traffic. Applications that require a one-to-many communication model may require the use of multicast-based transmission. Generally, for the data WLAN, it is recommended to 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 number of the SSID created in Procedure 3. (Example: WLAN-Data)

uluilu cisco	MONITOR WLANS CONTROLLER WIRELESS	Save Configuration Ping Logout & SECURITY MANAGEMENT COMMANDS HELP FEEDBACK	efresh
WLANs	WLANs	Entries 1 - 1 o	of 1
WLANS	Current Filter: None [Change Filter] [Clear F	Filter] Create New Go	
Advanced	WLAN ID Type Profile Name	Admin WLAN SSID Status Security Policies	
	1 WLAN WLAN-Data	WLAN-Data Enabled [WPA2][Auth(802.1X)]	

Step 3: On the General tab, in the **Interface/Interface Group(G)** list, choose the interface created in Procedure 10. (Example: wireless-data)

Step 4: If you want to enable multicast on the WLAN-Data wireless LAN, select **Multicast VLAN Feature**, and then in the **Multicast Interface** list, choose the WLAN data interface. (Example: wireless-data)

Step 5: Click Apply.

սիսիս					Sa <u>v</u> e Co	onfiguration <u>P</u> ing L	.ogout <u>R</u> efresh
cisco	<u>M</u> ONITOR <u>W</u> LANS <u>C</u> ONTROLL	LER WIRELESS	<u>S</u> ECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP FEEDBACK	
WLANs	WLANs > Edit 'WLAN-Data	l,				< Back	Apply
- WLANS							
WLANs	General Security Qos	6 Advanced					
Advanced	Profile Name	WLAN-Data					
	Туре	WLAN					
	SSID	WLAN-Data					
	Status	Enabled					
	Security Policies	[WPA2][Auth(80	2.1X)]	hah will annan af			
		(Modificacions done	under security	cab will appear ai	iter applying the	changes.)	
	Radio Policy	All 👻					
	Interface/Interface Group(G)	wireless-data 👻					
	Multicast Vlan Feature	Enabled					
	Multicast Interface	wireless-data 👻					
	Broadcast SSID	Enabled					
	Foot Notes						
	 Web Pointy Calmink De Gale in it of 2 FlexConnect Local Switching is r 3 When client exclusion is enable. Client MFP is not active unless V 5 Learn Client IP is configurable of 6 WMM and open or AES security 8 Value zero implies there is no n 9 MAC Filtering is not supported with 10 MAC Filtering should be enable 	on prinadon wed reserved of supported with 1 d, a Timeout Value o VPA2 is configured inly when FlexConne should be enabled t estriction on maxim vith FlexConnect Loc id.	or Prec, CRANITE : of zero means ir act Local Switchi to support highe um clients allow al authentication bould be dirable	authentication, O nfinity (will requir ng is enabled r 11n rates ed. 7	verride Interface e administrative	ACLs override to reset exclud	ded clients)
	12 Bas-associated-clients feature 13 VLAN based central switching i 14 Enabling gtk-randomize will pr 15 Fast Transition is supported wi 16 A value of zero (0) indicates th	is not supported with s not supported with event clients from a th WPA2 and open s hat the value specifi	ith FlexConnect Li h FlexConnect Li lecrypting broad security policy ied in the selecte	Local Authenticat. local Authenticatic loast and multica: ad QoS profile wil	ion. in. st packets. I take effect.		

Procedure 13 Configure the 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. Multicast may be required for some voice applications that require a one-to-many method of communication. One common example of a multicast voice use-case is a group-based push-to-talk, which is more efficient via multicast than over traditional unicast transmissions.

To configure the voice WLAN, change the default QoS settings to Platinum and segment the voice traffic onto the voice wired VLAN.

cisco	MONITOR								
		WLANS		WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	<u>F</u> EEDBACK
WLANs	WLANs								Entries 1 - 1 of 1
WLANS	Current Filt	er: Nor	ne [Change	Filter] [Clear F	ilter]	C	reate New	Go	l
Advanced	WLAN ID	Туре	Profile Nam	e	WLAN	SSID	Admin Status	Secu	urity Policies
	1	WLAN	WLAN-Data		WLAN-	Data	Enabled	H [WP	A2][Auth(802.1X)]

Step 1: On the WLANs page, in the list, choose Create New, and then click Go.

Step 2: Enter the Profile Name. (Example: Voice)

Step 3: In the SSID box, enter the voice WLAN name, and then click Apply. (Example: WLAN-Voice)

ahaha				figuration <u>P</u> ing Lo <u>q</u> out <u>R</u> efresh
cisco	<u>M</u> ONITOR <u>W</u> LANS <u>C</u> OI	ITROLLER WIRELESS SECURITY	MANAGEMENT COMMANDS	HELP <u>F</u> EEDBACK
WLANs	WLANs > New			< Back Apply
WLANS WLANS Advanced	Type Profile Name SSID ID	WLAN Voice WLAN-Voice 2		

Step 4: On the General tab, next to Status, select Enabled.

Step 5: In the **Interface/Interface Group(G)** list, choose the interface created in Procedure 11. (Example: wireless-voice)

Step 6: If you want to enable multicast on the WLAN-Voice wireless LAN, select **Multicast VLAN Feature**, and then in the **Multicast Interface** list, choose the WLAN voice interface. (Example: wireless-voice)

Step	7:	Click	Apply.
------	----	-------	--------

ahaha	Saye Configuration Ping Logout Befresh
cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP EEEDBACK
WLANs	WLANs > Edit 'WLAN-Voice' < Back Apply
▼ WLANS	
WLANs	General Security QoS Advanced
Advanced	Profile Name WLAN-Voice
	Type WLAN
	SSID WLAN-Voice
	Status 💟 Enabled
	Security Policies [WPA2][Auth(802.1X)]
	(Modifications done under security tab will appear after applying the changes.)
	Radio Policy All
	Interface/Interface Group(G) wireless-voice 🔻
	Multicast Vlan Feature 🛛 Enabled
	Multicast Interface wireless-voice 👻
	Broadcast SSID 🛛 Enabled
	Foot Notes
	1 Web Policy cannot be used in combination with IPsec
	2 FlexConnect Local Switching is not supported with IPsec, CRANLIE authentication, Override Interface ACLs 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 FlexConnect Local Switching is enabled
	6 WMM and open or AES security should be enabled to support higher 11n rates 8 Value zero implies there is no restriction on maximum clients allowed.
	9 MAC Filtering is not supported with FlexConnect Local authentication 10 MAC Filtering should be enabled.
	11 Guest tunneling, Local switching, DHCP Required should be disabled. 12 Max-associated-clients feature is not supported with FlexConnect Local Authentication.
	13 VLAN based central switching is not supported with FlexConnect Local Authentication. 14 Enabling atk-randomize will prevent clients from decrypting broadcast and multicast packets.
	15 Fast Transition is supported with WPA2 and open security policy 16 A value of zero (0) indicates that the value specified in the selected QoS profile will take effect.

Step 8: On the QoS tab, in the Quality of Service (QoS) list, choose Platinum (voice), and then click Apply.

ababa	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<="" th=""></back>
WLANs	General Security QoS Advanced
MLANS Advanced	
, navancea	Quality of Service (QoS) Platinum (voice)
	WMM
	WMM Policy Allowed -
	7920 AP CAC Enabled
	7920 Client CAC Enabled
	Foot Notes
	1 Web Policy cannot be used in combination with IPsec 2 H-REAP Local Switching is not supported with IPsec. CRANITE authentication
	3 When client exclusion is enabled, a Timeout Value of zero means infinity (will require administrative override to reset excluded clients)
	4 Client MEP is not active unless WPA2 is compared 5 Learn Client IP is configurable only when HREAP Local Switching is enabled
	6 WMM and open or AES security should be enabled to support higher 11n rates 7 Multicast Should Be Enabled For IPV6.
	8 Band Select is configurable only when Radio Policy is set to 'All'. 9 Value zero implies there is no sectricities on maximum clients allowed
	10 MAC Filtering is not supported with HREAP Local authentication
	11 MAC Filtering should be enabled. 12 Guest tunneling, Local switching, DHCP Required should be disabled.
	13 Max-associated-clients feature is not supported with HREAP Local Authentication.

Procedure 14 Configure the resilient controller

If you are configuring Cisco 2500 Series WLCs, AP SSO is not supported. You should therefore complete this procedure in order to join multiple controllers to a mobility group. If you are configuring Cisco 5500 Series WLCs, AP SSO is supported, and you should skip this procedure.

The local-mode design model can support lightweight access points across multiple floors and buildings simultaneously. In all deployment scenarios, you should deploy multiple controllers at each site, for resiliency.

This design, not based on AP SSO, uses two independently licensed controllers. The first is the primary controller to which access points normally register. The secondary controller, also called the *resilient controller*, provides resiliency in case the primary controller fails. Under normal operation, no access points register to the resilient controller.

Even when configured as a pair, controllers do not share configuration information as they do when using AP SSO, so you must configure each controller separately.

Because it is possible for a wireless client in your network to roam from an access point joined to one controller to an access point joined to another controller, both controllers should be deployed in the same mobility group.

A *mobility group* is a set of controllers, identified by the same mobility group name that defines the realm of seamless roaming for wireless clients. By creating a mobility group, you can enable multiple controllers in a network to dynamically share information and forward data traffic when intercontroller or intersubnet roaming occurs. Controllers in the same mobility group can share the context and state of client devices as well as their list of access points so that they do not consider each other's access points as rogue devices. With this information, the network can support intercontroller WLAN roaming and controller redundancy.

Step 1: Repeat Procedure 3 through Procedure 13 for the resilient controller.

Step 2: On the primary controller, navigate to **Controller > Mobility Management > Mobility Groups**. The MAC address, IP address, and mobility group name for the local controller are shown.

սիսիս							Sa <u>v</u> e Cor	nfiguration <u>P</u> ing	Logout <u>R</u> efresh
cisco	MONITOR	<u>W</u> LANs	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP FEEDBA	CK
Controller	Static Mo	bility Gı	roup Member	S				New	EditAll
General Inventory	Local Mo	obility Gro	CAMPU:	5					
Interfaces	MAC Add	dress	IP Address	Group N	ame M	lulticast IP	Status		
Interface Groups	00:24:97	7:69:dd:60	10.4.46.64	CAMPUS	0	.0.0.0	Up		
Multicast									
Network Routes									
Internal DHCP Server									
 Mobility Management Mobility Groups Mobility Anchor Config Multicast Messaging 									
Ports									
▶ NTP									
▶ CDP									
Advanced									

Step 3: On the resilient controller, navigate to Controller > Mobility Management > Mobility Groups, and then click New.

August 2013

Step 4: In the Member IP Address box, enter the IP address of the primary controller. (Example: 10.4.46.64)

Step 5: In the Member MAC Address box, enter the MAC address of the primary controller, and then click Apply.

սիսիս		Sa <u>v</u> e Configuration <u>P</u> ing Logout <u>R</u> efre					<u>R</u> efresh		
cisco	MONITOR	<u>W</u> LANs		WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP FEEDBACK	
Controller	Mobility (Group Me	ember > New					< Back A	pply
General Inventory Interfaces Interface Groups Multicast Network Routes Internal DHCP Server Mobility Management Mobility Anangement Multicast Messaging Ports NTP COP Advanced	Member Member Group Na	IP Address MAC Addre	10.4.46.6 90:24:97 Самриз	4 :69:d:60					

Step 6: On the primary controller, navigate to Controller > Mobility Management > Mobility Groups, and then click New.

Step 7: In the Member IP Address box, enter the IP address of the resilient controller. (Example: 10.4.46.65)

Step 8: In the Member MAC Address box, enter the MAC address of the resilient controller, and then click Apply.

CISCO MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HEIP FEEDBACK Controller Mobility Group Member > New < Back Apply General Inventory Member IP Address 00:24:97:69:37:20 Interfaces Group Name CAMPUS Interfaces Group Name CAMPUS CAMPUS Interfaces Interfaces Interface Groups Multicast Network Routes CAMPUS Interfaces Interface Mobility Groups Mobility Groups CAMPUS Interface Interface Interface Mobility Anagement Mobility Anagement Mobility Anagement Mobility Anagement Interface Mobility Anagement Mobility Anagement Mobility Anagement Interface Interface Mobility Anagement Mobility Anagement Mobility Anagement Interface Interface Mobility Anagement Mobility Anagement Interface Interface Interface Ports Advanced Interface Interface Interface Interface Advanced Interface Inte
Controller Mobility Group Member > New < Back
General Member IP Address 10.4.46.65 Interfaces Group Name 00:24:97:69:a7:20 Interface Groups Group Name CAMPUS Mutticast Method Server CAMPUS Mobility Management Mobility Anchor Config Mutticast Hessaging Ports NTP > CDP Advanced

Step 9: On each controller, click Save Configuration, and then click OK.

Step 10: Navigate to **Controller > Mobility Management > Mobility Groups** on each controller, and then verify that connectivity is up between all the controllers by examining the mobility group information. In the Status column, all controllers should be listed as **Up**.

սիսիս							nfiguration <u>P</u> in	g Logout <u>R</u> efresh
cisco	MONITOR WLANS		WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP FEED	BACK
Controller	Static Mobility Gro	oup Members	5				New	EditAll
General Inventory	Local Mobility Gro	up CAMPUS						
Interfaces	MAC Address	IP Address	Group Na	ime M	ulticast IP	Status		
Interface Groups	00:24:97:69:dd:60	10.4.46.64	CAMPUS	0.	0.0.0	Up		
Multicast Network Routes	00:24:97:69:a7:20	10.4.46.65	CAMPUS	0.	0.0.0	Up		
Internal DHCP Server								
 Mobility Management Mobility Groups Mobility Anchor Config Multicast Messaging 								
Ports								
▶ NTP								
► CDP								
Advanced								

Procedure 15 Configure controller discovery

You have three options to configure controller discovery, depending on the number of controller pairs and the type of DHCP server you've deployed.

If you have only one controller pair in your organization, complete Option 1 of this procedure. If you have deployed multiple controller pairs in your organization and you use Cisco IOS software in order to provide DHCP service, complete Option 2. If you have deployed multiple controller pairs in your organization and you use a Microsoft DHCP server, complete Option 3.

DHCP Option 43 maps access points to their controllers. Using DHCP Option 43 allows remote sites and each campus to define a unique mapping.





Option 1: Only one WLC pair in the organization

Step 1: Configure the organization's DNS servers (Example: 10.4.48.10) to resolve the **cisco-capwap-controller** host name to the management IP address of the controller. (Example: 10.4.46.64) The cisco-capwap-controller DNS record provides bootstrap information for access points that run software version 6.0 and higher.

Step 2: If the network includes access points that run software older than version 6.0, add a DNS record to resolve the host name **cisco-lwapp-controller** to the management IP address of the controller.

Option 2: Multiple WLC pairs in the organization: Cisco IOS DHCP server

In a network where there is no external, central-site DHCP server, you can provide DHCP service with Cisco IOS software. This function can also be useful at a remote site where you want to provide local DHCP service and not depend on the WAN link to an external, central-site DHCP server.

Step 1: Assemble the DHCP Option 43 value.

The hexadecimal string is assembled as a sequence of the Type + Length + Value (TLV) values for the Option 43 suboption, as follows:

- Type is always the suboption code 0xf1.
- Length is the number of controller management IP addresses times 4, in hexadecimal.
- Value is the IP address of the controller listed sequentially, in hexadecimal.

For example, suppose there are two controllers with management interface IP addresses 10.4.46.64 and 10.4.46.65. The type is 0xf1. The length is 2 * 4 = 8 = 0x08. The IP addresses translate to 0a042e40 (10.4.46.64) and 0a042e41(10.4.46.65). When the string is assembled, it yields **f1080a042e400a042e41**.

Step 2: On the network device, add Option 43 to the pre-existing data network DHCP Pool.

ip dhcp pool [pool name]
option 43 hex f1080a042e400a042e41

Option 3: Multiple WLC pairs in the organization: Microsoft DHCP server

This procedure shows how the Microsoft DHCP server is configured in order to return vendor-specific information to the lightweight Cisco Aironet 1600, 2600, and 3600 Series Access Points used in this design guide. The vendor class identifier for a lightweight Cisco Aironet access point is specific to each model type. To support more than one access point model, you must create a vendor class for each model type.

Access point	Vendor class identifier
Cisco Aironet 1600 Series	Cisco AP c1600
Cisco Aironet 2600 Series	Cisco AP c2600
Cisco Aironet 3600 Series	Cisco AP c3600

Table 4 - Vendor class identifiers

Step 1: Open the DHCP Server Administration Tool or MMC.

Step 2: Navigate to DHCP > ad.cisco.local, right-click IPv4, and then click Define Vendor Classes.

Name	Actions	
IPv4	ad.cisco.local	<u>ــــــــــــــــــــــــــــــــــــ</u>
10 Th A D	More Actions	+
	Nome	Nome Actions Prv4 actions Prv6 More Actions

Step 3: In the DHCP Vendor Classes dialog box, click Add.

D	HCP Vendor Classes		? ×]
	Name Microsoft Windows 20 Microsoft Windows 98 Microsoft Options	Description Microsoft vendor-specific option Microsoft vendor-specific option Microsoft vendor-specific option	Add Edit <u>R</u> emove	
			Close	

Step 4: In the New Class dialog box, enter a Display Name. (Example: Cisco Aironet 1600 AP)

Step 5: In the ASCII section, enter the vendor class identifier for the appropriate access point series from Table 4, and then click **OK**. (Example: Cisco AP c1600)

Step 6: In the DHCP Vendor Classes dialog box, click Close.

🖞 DHCP	_ 🗆 ×
File Action View Help	
🗢 🔿 🗡 📰 🗶 🖹 🖻 🔹 📝 🗊	
P DHCP Name	Actions
ad.cisco.local	ad.cisco.local 🔺
E PV6	More Actions
DHCP Vendor Classes	? 🗙
Available classes:	
Name Description	Add
Mir Mir Mir	Edit
Mir Display name:	Bemove
Cis Cisco Aironet 1600 AP	
Cis Description:	
Cis ID: Binary ASCI	
0000 43 69 73 63 6F 20 41 50 Cisco AF	Close
OK Cano	el

Step 7: Right-click the IPV4 DHCP server soot, and then click Set Predefined Options.

Step 8: In the Option Class list, choose the class created in Step 4, and then click Add.

Predefined Options a	nd ¥alues	? ×
Option class:	Cisco Aironet 1600 AP	_
Option name:		-
	Add Edit	Delete
Description:		
	0K	Cancel

Step 9: In the Option Type dialog box, enter a Name. (Example: Option 43)

Step 10: In the Data Type list, choose IP Address.

Step 11: Select Array.

Step 12: In the Code box, enter 241, and then click OK.

Change Option	Name	? ×
Class:	Cisco Aironet 1600 AP	
<u>N</u> ame:	Option 43	
<u>D</u> ata type:	IP Address 🔽 🗹 Array	
<u>C</u> ode:	241	
D <u>e</u> scription:		
	OK Cano	el

The vendor class and suboption are now programmed into the DHCP server. Now, you need to define the vendor-specific information for the DHCP scope.

Step 13: Choose the DHCP scope that you will be installing Access Points on, right-click **Scope Options**, and then click **Configure Options**.

Step 14: Click the Advanced tab, and in the Vendor class list, choose the class created in Step 4.

Step 15: Under Available Options, select 241 Option 43.

Step 16: In the **IP address** box, enter the IP address of the primary controller's management interface, and then click **Add**. (Example: 10.4.46.64)

×

Step 17: If you are not using the AP SSO feature, repeat Step 13 through Step 16 for the resilient controller, and then click **Apply**. (Example: 10.4.46.65)

Procedure 16 Connect the access points

On the LAN access switch, the switch interfaces that are connected to the access points use the standard access switchport configuration, with the exception of the QoS policy that you configure in this procedure.

Step 1: Configure the interface where the access point will be connected to trust the QoS marking from the access point.

```
interface GigabitEthernet [port]
  description Access Point Connection
  switchport access vlan 100
  switchport voice vlan 101
  switchport host
  macro apply EgressQoS
  switchport port-security maximum 11
  switchport port-security
  switchport port-security aging time 2
  switchport port-security aging type inactivity
  switchport port-security violation restrict
  ip arp inspection limit rate 100
  ip dhcp snooping limit rate 100
  ip verify source
```
Procedure 17 Configure access points for resiliency

Step 1: For access points that are connecting to a WLC that is not using AP-SSO, it is necessary to configure these access points with the IP addresses of each of the non AP-SSO controllers. If you are installing access points that will connect to a pair of WLC's using AP-SSO, please skip this procedure.

Step 2: On the primary controller, navigate to Wireless, and then select the desired access point.

Step 3: Click the High Availability tab.

Step 4: In the **Primary Controller** box, enter the name and management IP address of the primary controller. (Example: WLC-1 / 10.4.46.64)

Step 5: In the **Secondary Controller** box, enter the name and management IP address of the resilient controller, and then click **Apply**. (Example: WLC-2 / 10.4.46.65)

սիսիս					Sa <u>v</u> e Confi	iguration <u>P</u> ing l	.ogout <u>R</u> efresh
cisco	<u>M</u> ONITOR <u>W</u> LANS <u>O</u>	ONTROLLER WIRELE	SS <u>S</u> ECURITY M <u>A</u> I	NAGEMENT C	OMMANDS	HELP FEEDBACK	
Wireless	All APs > Details for	A4507-1141N				< Back	Apply
Access Points	General Credent	ials Interfaces	High Availability	Inventory	Advanced	i	
 Access Points All APs Kadios S02.11a/n S02.11b/g/n Global Configuration Advanced Mesh HREAP Groups S02.11a/n S02.11a/	General Credent Primary Controller Secondary Controller Tertiary Controller AP Failover Priority	Auls Interfaces	High Availability Managemee 10.4.46.64 10.4.46.65	Inventory nt IP Address	Advanced		
	Foot Notes						
	1 DNS server IP Address	and the Domain name c	an be set only after a val	lid static IP is pus	shed to the AP.		



There are two methods of deploying remote site wireless LAN controllers, shared and dedicated:

- A *shared WLC* has both remote-site access points and local, on-site access points connected to it concurrently. Use a shared WLC when the number of access points matches the available capacity of the co-located WLCs near the WAN headend, and the WAN headend is co-located with a campus.
- A *dedicated WLC* only has remote-site access points connected to it. Use a dedicated WLC pair, such as Cisco Flex 7500 Series Cloud Controller using AP SSO, when you have a large number of access points or remote sites. Alternately, for smaller deployments, the use of the vWLC is a cost-effective option, provided that you do not exceed 200 APs across two or more Cisco FlexConnect groups or exceed 3000 wireless clients per vWLC. You also use this option when the co-located WLCs near the WAN headend don't have the necessary capacity or the WAN headend is not co-located with a campus.



If you are using a shared WLC, this design guide assumes that you have already deployed the WLC following the instructions in the "Configuring On-Site Wireless Controllers" process. To deploy remote-site wireless in a shared controller deployment, skip to Procedure 15.

If you are using a dedicated WLC, perform all the procedures in this process in order to deploy remote-site wireless.

Parameter	CVD values primary controller	CVD values resilient controller not using AP SSO	Site-specific values
Controller parameters	<u>`</u>		
Switch interface number	1/0/3, 2/0/3	1/0/4, 2/0/4	
VLAN number	146	146	
Time zone	PST -8 0	PST -8 0	
IP address	10.4.46.68/24	10.4.46.69/24	
Default gateway	10.4.46.1	10.4.46.1	
Hostname	WLC-RemoteSites-1	WLC-RemoteSites-2	
Mobility group name	REMOTES	REMOTES	
RADIUS server IP address	10.4.48.15	10.4.48.15	
RADIUS shared key	SecretKey	SecretKey	
Management network (optional)	10.4.48.0/24	10.4.48.0/24	
TACACS server IP address (optional)	10.4.48.15	10.4.48.15	
TACACS shared key (optional)	SecretKey	SecretKey	
Remote site parameter	TS		
Wireless data SSID	WLAN-Data	WLAN-Data	
Wireless data VLAN number	65	65	
Wireless voice SSID	WLAN-Voice	WLAN-Voice	
Wireless voice VLAN number	70	70	
Default gateway	10.4.20.1	10.4.20.1	
Controller interface IP address	10.4.20.5/22	10.4.20.6/22	

Table 5 - Cisco remote-site wireless controller parameters checklist

Procedure 1 Install the vWLC for FlexConnect designs

The virtual Wireless LAN controller (vWLC) is ideal for small to medium deployments where virtualized compute services are available within the data center and the AP design model is using local switching using Cisco FlexConnect.

Tech Tip

The vWLC requires two physical network interface cards (NICs), one dedicated to the management interface and one for wireless client traffic. To provide full switch fabric redundancy, four physical NICs are required and are grouped into two pairs by using NIC teaming.

If you are installing a virtual wireless LAN controller (vWLC), you must complete the following steps in order to install it using the downloaded Open Virtual Archive (OVA) file available online from Cisco. If you are using another WLC to support your remote sites, you can skip to Procedure 5 "Configure the LAN distribution switch."

Step 1: Begin by preparing the VMware host machine networking environment. On the physical host machine, in vCenter, create three virtual switches (vSwitch0, vSwitch1, and vSwitch2), as follows:

- On vSwitch0, allocate two physical NIC interfaces. These will be used to provide management access to the vWLC (Example: management network mapped to VLAN ID: 148)
- On vSwitch1 allocate two physical interfaces that will be used to provide wireless VLAN access for each WLAN created on the vWLC. (Example: wireless VLANs mapped to VLAN ID: All 4095)
- On vSwitch2, no physical interfaces need to be allocated unless the service port will be used in the future. Failure to define this interface may result in the wrong interface's vSwitches being used for the wireless data VLANs. The configuration of the service port is required in the event that the service port needs to be used for maintenance and support functions during the controller's lifecycle.

File Edit View Inventory Administra	ation Plug-ins Help		
🖸 🔝 🔥 Home 🕨 👩 Inv	rentory 🕨 🎁 Hosts and Clusters		Search Inventory
htter dato bela 18 18 19 19 19 19 19 19 19 19 19 19	r200 examplication back VM-over EXX, 52 Erating strategies and the second VM-over EXX, 52 Processes Memory Strategies Adaptes Advanced Strategies Nover Management Strategies Adaptes Advanced Strategies Advanced Strategies Nover Management Usersel Frahement Default Nachina Surfaug/Adaptes Advanced Strategies Nover Management Mana	DB, G25801 [Vehicken (25 days remained) Per Parameter 2005000; Performance Configuration Tests & Dennis Allenni Permessare Market Statement Handware Statement Networking Parameter Marks Performance Parameter Marks Performance Performa	

Next, you install the vWLC OVA file obtained from Cisco.

Step 2: In vCenter, select the physical machine, click File, and then click Deploy OVF Template.

🖗 vCenter.cisco.local - vSphere Client				
Ele Edit View Inventory Administration	ion Plug-ins Help			
New +	ntory 🕨 🎁 Hosts and Clusters	eð - Sear		
Deploy OVF Template	rs200.esvi2 cisco local VMware ESXI 5	D.D. 623860 Evaluation (25 days remaining)		
Export +	Seller Control Control Interaction			
Report +	deconglocarced (ourman) (wrodanniach	а пле Акаласкимскота нагодинист Солдонала раза и стата Акала Сталара на сталара на сталала стала и раза стала ста В стала на стала на стала на стала стала стала стала стала		
Browse VA Marketplace	Hardware	View: vSphere Standard Switch vSphere Distributed Switch		
Date Maps > Ext	Processes Hennory Storage Noto-Charles Storage Adgetes Noto-Charles Software Learned Features The Confluctions The Confluctions Dever Minagement Multi-Marker Startup/Endown What Marker Startup/Endown What Marker Startup/Endown Society India Software Marker Startup/Endown Society India Software Besource Alcoden Advenced Settrage	Retworking Scadard Switch vSwitch Person Markan Verwer WAL Private Adaptas Verwer Walk Private Adaptas Verwer Verwer Verwer Private Adaptas Verwer Ver		

Step 3: Complete the Deploy OVF Template wizard. Note the following:

- On the Source page, select the downloaded vWLC OVA file that you obtained from Cisco.
- On the Name and Location page, provide a unique name for the virtual Wireless LAN controller. (Example: vWLC-1)

Deploy OVF Template		_ 🗆 🗙
Name and Location Specify a name and locat	ion for the deployed template	
Source OVF Template Details Name and Location Storage Disk Format Network Mapping Ready to Complete	Name: WHLC-1] The name can contain up to 80 characters and it must be unique within the inventory folder. Inventory Location: RS200 Data Center	
Help	≤Back Next ≥	Cancel

Step 4: On the Storage page, select the storage destination of the virtual machine.

Deploy OVF Template		
Storage Where do you want to s	tore the virtual machine files?	
Source OVF Template Details Name and Location	Select a destination storage for the virtual machine files:	
Storage	Name Drive Type Capacity Provisioned Free Type Thin	Prov
Disk Format Network Mapping	Openfiler(Soft Unknown 9.09 TB 6.07 TB 3.04 TB NFS Supp	orte
	Disable Storage DRS for this virtual machine Select a datastore:	Þ
	Name Drive Type Capacity Provisioned Free Type Thin P	rovis
Help	≤Back Next ≥ Cance	1

Step 5: On the Disk Format page, select Thick Provision Lazy Zeroed.

Deploy OVF Template					_ 🗆 ×
Disk Format In which format do you wa	nt to store the virtual disks?				
Source OVF Template Details Name and Location Storage Disk Format Network Mapping Ready to Complete	Datastore: Available space (GB): Thick Provision Lazy 20 Thick Provision Eager 2 Thin Provision	R5200-E5X/2_Local			
Help	<u> </u>		<u><</u> Back	Next >	Cancel

Step 6: On the Network Mapping page, in the **Destination Networks** list, choose the network defined on the VM host machine that will be used on the vWLC management interface. (Example: Server VLAN 1)

Deploy OVF Template		
Network Mapping		
What networks should th	ne deployed template use?	
Source	_	
OVF Template Details	Map the networks used in this OVF	template to networks in your inventory
Name and Location		
Storage	Source Networks	Destination Networks
<u>Disk Format</u>	VM Network	Server VLAN 1
Ready to Complete		Server VLAN 1
coddy co complete		Server VLAN 2
		Wireless VLANs
	Description:	
	The VM Network	
	1	1
Help		≤Back Next ≥ Cancel

Step 7: On the Ready to Complete page, review the settings, and then press **Finish**. Deployment of the OVA file begins, and it may take a few minutes to complete.

🚱 Deploy OVF Template 👘		
Ready to Complete		
Are these the options yo	u want to use?	
Source	_	
OVF Template Details	When you click Finish, the deplo	yment task will be started.
Name and Location	Deployment settings:	
<u>Storage</u>	OVF file:	C:\AS CTVM 7 4 1 42.ova
Disk Format	Download size:	161.7 MB
Network Mapping	Size on disk:	8.2 GB
Ready to Complete	Name:	VWLC-1
	Folder:	RS200 Data Center
	Host/Cluster:	rs200-esxi2.cisco.local
	Datastore:	RS200-ESXi2_Local
	Disk provisioning:	Thick Provision Lazy Zeroed
	Network Mapping:	"VM Network" to "Server VLAN 1"
	Power on after deployment	
Help		≤ Back Finish Cancel

Procedure 2 Configure the console port on the vWLC

When the vWLC starts, the Console tab within vSphere will display a repetitive message stating to press any key in order to make the Console tab the default terminal for console messages from the vWLC. If a key is not pressed during the vWLC startup, console communication to the vWLC through the vSphere client's console window will not be possible. This can be a problem when troubleshooting IP connectivity issues, for example, and console access is required. For this reason, in this procedure, you create a virtual serial port. This will ensure access to the vWLC console through the use of a standard Telnet client.

Step 1: In vCenter, select the newly added vWLC (Example: vWLC-1), click **Edit virtual machine settings**, and then in the Virtual Machine Properties dialog box, click **Add**.



Step 2: Complete the Add Hardware wizard. Note the following:

• On the Device Type page, select Serial Port.

💋 vWLC-1 - Virtual Machine Prope	rties	
Hardware Options Resources Prof	iles vServices	Virtual Machine Version: 7
Ha Device Type What sort of device do you Device Type Select Port Type Select Port Type Select Output File Ready to Complete	u wish to add to your virtual machin Choose the type of device you v	Memory Configuration
	☐ Floppy Drive ☑ CD/DVD Drive ☑ USB Controller ☑ USB Device (unavailable) I USB Device (unavailable) I Ethernet Adapter I Hard Disk ☑ SCSI Device	Source can be back to this in technicit.
		OK Cancel

• On the Select Port Type page, select Connect via Network.



 On the Network Backing page, select Server (VM listens for connection), and then in the Port URI box, enter telnet://[Host Machine IP Address]:[Unique TCP Port]. (Example: telnet://10.5.24.101:9292) This configures IP address and TCP port number that are used access the console port via Telnet.

@ -	WLC-1 - Virtual Machine Prope	rties
Har	dware Options Resources Prof	iles vServices Virtual Machine Version: 7
		Memory Configuration
Ha	Add Hardware Network Serial Port Settin How should this serial port	gs connect via network?
	Device Type	Network Backing
Ī	Select Port Type	 Server (VM listens for connection)
E	Ready to Complete	C Client (VM initiates connection)
		Port URI: telnet://10.5.24.101:9292
		Use Virtual Serial Port Concentrator vSPC URI: Device Status Connect at power on I/O Mode Vield CPU on poll Allow the guest operating system to use this serial port in polled mode rather than in interrupt mode.
L		
	Help	OK Cancel

• On the Ready to Complete page, review the settings, and then click Finish.

Step 3: On the Virtual Machine Properties dialog box, click **OK**. The new serial port has been successfully configured.

🚱 vWLC-1 - Virtual Machine Properties	
Hardware Options Resources Profiles vServices	Virtual Machine Version: 7
WULC-1 - Virtual Machine Properties Hardware Options Resources Profiles VServices Image: Summary Add R Hardware Summary Image: Summary Add R Hardware Summary Image: Summary 2048 MB Image: CPUs 1 Video card Video card VMCI device Restricted SCSI controller 0 LSI Logic Parallel Hard disk 1 Virtual Disk CD/DVD drive 1 [RS200-E5X82_Loc Network adapter 1 Server VLAN 1 Image: Network adapter 2 Server VLAN 1 Image: Picppy drive 1 Floppy 1	
ICD/DVD drive 1 IRS200-ESX2_Loc Network adapter 1 Server VLAN 1 Floppy drive 1 Floppy drive 1 Floppy 1 New Serial Port (adding) telnet://10.5.2*	Al V C Use named pipe: Pipe Name: Pipe Na
Help	I/O Mode Vield CPU on poll OK Cancel

Procedure 3 Configure the vWLC network adapters

Configure the network adapters that will be used for the WLAN service port and the wireless VLAN interfaces. In this procedure, four physical NIC interfaces are used in two EtherChannel pairs, and each interface in a pair connects to separate redundant switches.

Step 1: In the Virtual Machine Properties dialog box, select Network adapter 1, and then in the Network label list, choose WLAN Service Port.

🚱 vWLC-1 - Virtual Machine Properties _ 🗆 🗙 Hardware Options Resources Profiles VServices Virtual Machine Version: 7 Device Status Show All Devices Add... Remove Connected 🔽 Connect at power on Hardware Summary Memory 2048 MB Adapter Type 🔲 CPUs 1 E1000 Current adapter: 📃 Video card Video card 🔲 VMCI device Restricted MAC Address SCSI controller 0 LSI Logic Parallel 00:50:56:a2:5d:84 Virtual Disk 😑 🛛 Hard disk 1 CD/DVD drive 1 Automatic O Manual [RS200-ESXi2_Local] v... Network adapter 1 (edite... WLAN Service Port DirectPath I/O Network adapter 2 (edite... Wireless VLANs Not supported 🕤 Eloppy drive 1 Status: Floppy 1 Serial port 1 telnet://10.5.24.101:92... Network Connection Network label: Wireless VLANs Server VLAN 1 Wireless VLANs LAIN SE <u>H</u>elp OK Cancel

Step 2: Select Network adapter 2, and in the Network label list, choose Wireless VLAN, and then press OK.

Step 3: In the left column, start the virtual wireless LAN controller for the first time by selecting the virtual machine you just installed, and then clicking the **Power on the virtual machine** option shown within the console tab.

Within the Console tab you are prompted to "Press any key to use this terminal as the default terminal." However, you do not need to press any key because access via the serial port that was created in Procedure 2 will be used.

🔗 vCenter.cisco.local - vSphere Client		
Ble Edit View Igventory Administration Blug-ins Help		
💽 🔯 👌 Home 🕨 🚮 Inventory 🕨 🎁 Hosts and Clusters		🚮 • Search Inventory 🔍
Venter acaded Venter	And Managa Ang	
Recent Tasks		Name, Target or Status contains: - Elecr ×
Name Taroet Status Details	Initiated by Venter Server Requested Start Tu., V Start Time	Completed Time
Power On virtual mach WLC-1 Completed	CISCOlythigg. 12 Center.cisco.L. 10/31/2012 12:50:01 10/31/2012 12:50:01 PM	10/31/2012 12:50:01



Using a Telnet client, such as Putty, access the vWLC console port by connecting via Telnet to the IP address and TCP port defined in the Add Hardware wizard in the previous procedure.

🕵 PuTTY Configuration	
Representation	Basic options for your PuTTY session Specify the destination you want to connect to Host Name (or IP address) Port 10.5.24.101 9292 Connection type: Raw I lehet Rlogin Serial
Appearance Behaviour Translation Selection Colours Connection Data Proxy Telnet Rogin	Load, save or delete a stored session Sav <u>e</u> d Sessions Default Settings Load Save Delete
About	Close window on e <u>x</u> it: Always Never Only on clean exit <u>Open</u>

Procedure 4 Configure the data center switches

When using a dedicated design controller model with the Cisco Flex 7500 Series Cloud Controller, the controller resides within the data center. This procedure configures the data center Cisco Nexus switch for connectivity to the redundant Flex 7500 Series Cloud Controllers using redundant Ethernet ports configured for link aggregation (LAG). For the virtual Wireless LAN Controller, these steps are performed for the VM host machine during the deployment of the VM environment.

Step 1: On the primary data center Cisco Nexus switch (Example: DC5596UPa), create the wireless management VLAN that you are going to use to connect the redundant Cisco Flex 7500 Series Cloud Controller.

Vlan 146 name WLAN Mgmt

Step 2: On the primary data center Cisco Nexus switch (Example: DC5596UPa), create wireless port channels for the primary and resilient Cisco Flex 7500 Series Cloud Controller.

```
interface port-channel65
  description Link to WLC7500-1
  switchport mode trunk
  switchport trunk allowed vlan 146
  no shutdown
interface port-channel66
  description Link to WLC7500-2
  switchport mode trunk
  switchport trunk allowed vlan 146
  no shutdown
```

Step 3: Configure a switched virtual interface (SVI) for the VLAN. This enables devices in the VLAN to communicate with the rest of the network.

```
interface Vlan146
  no shutdown
  description Wireless Management Network
  no ip redirects
  ip address 10.4.46.2/24
  ip router eigrp 100
  ip passive-interface eigrp 100
  ip pim sparse-mode
  hsrp 146
    priority 110
    ip 10.4.46.1
```

Step 4: Configure two ports on the data center switch as a trunk port. These two ports will be connected to the redundant ports on the primary Cisco Flex 7500 Series Cloud Controller.

```
interface Ethernet103/1/1
  description Links to 7500-1
  switchport mode trunk
  switchport trunk allowed vlan 146
  channel-group 65
  no shutdown
interface Ethernet104/1/1
  description link to 7500-1
  switchport mode trunk
  switchport trunk allowed vlan 146
  channel-group 65
  no shutdown
```

Step 5: Configure two ports on the data center switch as a trunk port. These two ports will be connected to the redundant ports on the resilient Cisco Flex 7500 Series Cloud Controller.

```
interface Ethernet103/1/2
  description link to 7500-2
  switchport mode trunk
  switchport trunk allowed vlan 146
  channel-group 66
  no shutdown
interface Ethernet104/1/2
  description link to 7500-2
  switchport mode trunk
  switchport trunk allowed vlan 146
  channel-group 66
  no shutdown
```

Step 6: Repeat this procedure for the redundant Cisco Nexus data center switch (Example: DC5596UPb). Failure to define these on both Cisco Nexus switches results in a configuration inconsistency and prevents the ports from coming active.

Procedure 5 Configure the LAN distribution switch

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

vlan 146 name WLAN Mgmt

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

```
interface Vlan146
description Wireless Management Network
ip address 10.4.46.1 255.255.255.0
no shutdown
```

Step 3: For interface configuration in this procedure, 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 of the networks defined on the WLC. The VLANs allowed on the trunk are reduced to only the VLANs that are active on the WLC.

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

If you are deploying a Cisco Flex 7500 Series Cloud Controller, configure a 10-Gigabit distribution switch interface as a trunk. Note that when deploying a Cisco Flex 7500 Series Cloud Controller, it should not be connected to a Cisco Catalyst 3750-X Series distribution switch.

```
interface TenGigabitEthernet [number]
description To WLC port 1
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 146
switchport mode trunk
macro apply EgressQoS
logging event link-status
logging event trunk-status
no shutdown
```

If you are deploying a Cisco 5500 Series Wireless LAN Controller, configure at least two distribution switch interfaces as an EtherChannel trunk.

```
interface GigabitEthernet [port 1]
description To WLC Port 1
interface GigabitEthernet [port 2]
description To WLC Port 2
1
interface range GigabitEthernet [port 1], GigabitEthernet [port 2]
  switchport
 macro apply EgressQoS
  channel-group [number] mode on
  logging event link-status
 logging event trunk-status
 logging event bundle-status
Т
interface Port-channel [number]
description To WLC
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 146
 switchport mode trunk
logging event link-status
no shutdown
```

Procedure 6 Connecting the redundancy port

If you are using a Cisco vWLC, skip this procedure. If you are using a Cisco 7500 Series WLC and you wish to enable the high availability AP SSO feature, continue with this procedure. When using the high availability feature known as access point stateful switchover (AP SSO), a dedicated special-purpose port is available on the Cisco 7500 Series WLC. This port is located on the rear panel.

Seri ,		Cisco Flex 7500 Series viniti- Wreiess Controller
Redundancy	Port	
Sector		Cisco Flex 7500 Series

Step 1: Connect an Ethernet cable between the primary and standby WLC, as shown below.

Procedure 7 Configure the WLC platform

If you are installing a vWLC, the console port may be accessed by using a Telnet client as configured in Procedure 2. Alternately, you can use the VMware Console tab within vSphere in order to access the vWLC if the vSphere console was selected as the default terminal when the vWLC was started.

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

Welcome to the Cisco Wizard Configuration Tool Use the '-' character to backup

Step 1: Terminate the autoinstall process.

Would you like to terminate autoinstall? [yes]: YES

Step 2: Enter a system name. (Example: WLC-RemoteSites-1)

System Name [Cisco d9:3d:66] (31 characters max): WLC-RemoteSites-1

Step 3: Enter an administrator username and password.



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

If you are deploying a Cisco 5500 Series WLC or Cisco Flex Series Cloud Controller, configure at least two interfaces as an EtherChannel trunk.

Enable Link Aggregation (LAG) [yes][NO]: YES Management Interface IP Address: 10.4.46.68 Management Interface Netmask: 255.255.255.0 Management interface Default Router: 10.4.46.1 Management Interface VLAN Identifier (0 = untagged): 146

If you are deploying a virtual Wireless LAN Controller, select port 1 as the management interface port.

Management Interface Port Num [1 to 1]: 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 7500 Series Wireless LAN Controller as a primary WLC in an AP-SSO redundant pair, complete the following steps. This enables AP SSO on the primary.

Enable HA [yes][NO]: YES Configure HA Unit [PRIMARY][secondary]: PRIMARY Redundancy Management IP Address: 10.4.46.78 Peer Redundancy Management IP Address: 10.4.46.79

Step 8: If you are deploying a Cisco 7500 Series Wireless LAN Controller as a secondary WLC in an AP-SSO redundant pair, complete the following steps. This enables AP SSO on the secondary

Enable HA [yes][NO]: YES Configure HA Unit [PRIMARY][secondary]: secondary Redundancy Management IP Address: 10.4.46.79 Peer Redundancy Management IP Address: 10.4.46.78

Step 9: The virtual interface is used by the WLC for mobility DHCP relay and intercontroller communication. Enter an IP address that is not used in your organization's network. (Example: 192.0.2.1)

Virtual Gateway IP Address: 192.0.2.1

Step 10: Enter a name for the default mobility and RF group. (Example: REMOTES)

Mobility/RF Group Name: REMOTES

Step 11: Enter an SSID for the WLAN 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: Enable DHCP snooping.

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

Step 13: Do not configure the RADIUS server now. You will configure the RADIUS server later by 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 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 restarted, access the console port on the WLC and configure it to automatically convert the APs to Cisco FlexConnect mode as they register.

config ap autoconvert flexconnect

Step 20: Log in to the Cisco Wireless LAN Controller Administration page by using the credentials defined in Step 2. (Example: https://WLC-RemoteSites-1.cisco.local/)

Procedure 8 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.
---------	-------	-----	-----------

սիսիս						Sa <u>v</u> e Co	nfiguration	<u>P</u> ing Logout <u>R</u> efresh			
cisco	MONITOR WLA	ANS <u>C</u> ONTROLLER	WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP F	EEDBACK			
Commands	Set Time					Set	Date and T	ime Set Timezone			
Download File Upload File	Current Time	Tue May 31 11:0	7:38 2011								
Reboot Config Boot	Date						_				
 Scheduled Reboot 		Month		Мау	-						
Reset to Factory Default		Year		31 ¥ 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 Cana	ida) 🔻					
	Foot Notes										
	1. Automatically s	1. Automatically sets daylight savings time where used.									



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.

							Save Col	ingulation Ping Log	out <u>R</u> efresh
cisco	MONITOR	<u>W</u> LANs	<u>C</u> ONTROLLER	WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP FEEDBACK	
Management	SNMP v1	/ v2c Cc	ommunity > N	ew				< Back	Apply
Management Summary SNMP General SNNP V3 Users Communities Trap Receivers Trap Logs HTTP-HTTPS Telnet-SSH Serial Port Local Management Users User Sessions J Logs Mgmt Via Wireless Software Activation J Tech Support	SNMP v1 Communit IP Addres IP Mask Access Mc Status	/ v2c Cc	cisco 10.4.48.0 255.255.255.0 Read Only ♥ Enable ♥	ew				< Back	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. You should have only the read-write and read-only community strings, as shown in the following screenshot.

							Sa <u>v</u> e Co	nfiguration	Ping Logout <u>R</u> efresh
cisco	MONITOR	<u>W</u> LANs	CONTROLLER	WIRELESS	SECURITY	MANAGEMEN	COMMANDS	HELP FER	DBACK
Management	SNMP v1	/ v2c Co	ommunity						New
Summary									
▼ SNMP	Communit	y Name		IP Address	IP Mask	Access	Mode Status	5	
General	<u>cisco</u>			10.4.48.0	255.255.25	55.0 Read-0	nly Enable		
Communities	cisco123			10.4.48.0	255.255.25	55.0 Read-W	rite Enable		
Trap Receivers									
Trap Controls									
Talact COU									
Teinet-SSH									
Serial Port									
Local Management Users									
User Sessions									
▶ Logs									
Mgmt Via Wireless									
Software Activation									
Tech Support									
Serial Port Local Management User Sessions Logs Mgmt Via Wireless Software Activation Tech Support									

Procedure 10 Limit which networks can manage the WLC

(Optional)

In networks where network operational support is centralized you can increase network security by using an access control list in order to limit the networks that can access your controller. In this example, only devices on the 10.4.48.0/24 network are able to access the controller via SSH or SNMP.

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

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

Step 3: In the list, choose the name of the access control 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 Configuration Ping Logout <u>R</u> efree						
cisco	MONITOR	<u>W</u> LANs		WIRELESS	SECURITY	MANAGEMEN	COMMANDS	HELP	<u>F</u> EEDBACK		
Security	Access C	ontrol L	ists > Rules >	New					< Back	Apply	
 AAA Local EAP 	Sequence		1 IP Address]	IP Addr 10.4.4	ess 8.0	Netmask 255.255.255.0	_			
 Priority Order Certificate 	Destination		Any	•							
 Access Control Lists Access Control Lists CPU Access Control Lists 	Protocol		ТСР	•							
FlexConnect ACLs Wireless Protection Policies	Destination P	Port	HTTPS	•							
▶ Web Auth	DSCP		Any	•							
TrustSec SXP Advanced	Direction		Any	·							
	Action		Permit	·							

Sequence	Source Destination Protocol		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	ТСР	Other/22	Deny	
5	Any	Any	Any	Any	Permit	

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

li.ili. cisco	MON	ITOR	<u>W</u> LANs		OLLER WIRELESS	SECURITY	MANAGEMENT	COMMANDS	нецр	EEEDBACK			Sa <u>v</u> e Cont	iguration	<u>P</u> ing Logout <u>R</u> efre
Security	Acc	ess C	ontrol L	.ists > E	dit								< Bac	k	Add New Rule
AAA Local EAP Priority Order Certificate Access Control Lists Access Control Lists	Gen Acces Deny	eral Is List N Counte	ame rs	ACL-F	ules	Destination			s	ource	Dest			Number	
CPU Access Control	Seq	Actio	n Sou	rce IP/Ma	isk	IP/Mask		Protoco	I P	ort	Port	DSCP	Direction	of Hits	
FlexConnect ACLs	1	Permi	t 10.4	.48.0	/ 255.255.255.0	0.0.0	/ 0.0.0.0	TCP	A	ny	HTTPS	Any	Any	0	
Wireless Protection	2	Permi	t 10.4	.48.0	/ 255.255.255.0	0.0.0	/ 0.0.0.0	TCP	A	ny	22	Any	Any	0	
Policies	3	Deny	0.0.0	1.0	/ 0.0.0.0	0.0.0.0	/ 0.0.0.0	TCP	A	ny	HTTPS	Any	Any	0	
Web Auth	4	Deny	0.0.0	1.0	/ 0.0.0.0	0.0.0	/ 0.0.0.0	TCP	A	ny	22	Any	Any	0	
TrustSec SXP	5	Permi	t 0.0.0	1.0	/ 0.0.0.0	0.0.0	/ 0.0.0.0	Any	A	ny	Any	Any	Any	0	
Advanced															

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 just created, and then click Apply.

Procedure 11 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.

սիսիս							nfiguratior		Logout <u>R</u> efresh
cisco	MONITOR WLANS		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 LOAP LOAD Net Users MAC Filtering Disabled Clients User Login Policies AP Policies Password Policies Local EAP Priority Order Access Control Lists Wirelees Protection Policies Web Auth TrustSec SXP Advanced 	Server Index (Priorit Server IP Address Shared Secret Form Shared Secret Confirm Shared Secret Key Wrap Port Number Server Status Support for RFC 357 Server Timeout Network User Management IPSec	y) it et	1 v 10.4.48.15 ASCII v Cosigned for 1812 Enabled v Enabled v Enable Enable Enable	or FIPS custome	ers and requires a k	wy wrap complia	nt RADIUS	S 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)

Procedure 12 Configure management authentication

(Optional)

You can use this procedure to deploy centralized management authentication by configuring an authentication, authorization and accounting (AAA) service. If you prefer to use local management authentication, skip to Procedure 13.

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 Authentication, Authorization and Accounting (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, it controls all management access to the network infrastructure devices (SSH and HTTPS).

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)

սիսիս						Sa <u>v</u> e Cor	nfiguratior	n <u>P</u> ing	Logout <u>R</u> efresh
cisco	MONITOR W	LANS <u>C</u> ONTROLLER	WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	FEEDBAC	<
Security	TACACS+ A	uthentication Ser	vers > New				<	< Back	Apply
 AAA General RADUS RADUS TACACS+ Authentication Accounting Authentization LDAP Local Net Users MAC Filtering Disabled Clients User Login Policies Password Policies Priority Order Access Control Lists Wireless Protection Policies Web Auth TrustSec SXP Advanced 	Server Index Server IP Add Shared Secret Shared Secret Confirm Share Port Number Server Status Server Timeo	(Priority) Iress t Format t ed Secret	1 • 10.4.48.15 ASCII • 49 Enabled • 5 secon	ds					

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)

								Logout <u>R</u> efresh
cisco	MONITOR WLANS		WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP FEEDBA	ск
Security AAA General > RADIUS < TACACS+ Authentication Accounting Authorization	TACACS+ Accou Server Index (Priorit Server IP Address Shared Secret Form Shared Secret	y) 1 • 10.4 at ASC	3 > New .48.15 II ▼]		< Back	Apply
LDAP Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies Password Policies	Confirm Shared Sec Port Number Server Status Server Timeout	et •••• 49 Enat 5	oled 💌					
Local EAP								
Priority Order								
Certificate Certi								

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)

սիսիս						Sa <u>v</u> e Cor	nfiguration <u>P</u> ing	Logout <u>R</u> efresh
CISCO	MONITOR WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP FEEDB	ACK
Security	TACACS+ Author	ization Serve	rs > New				< Back	Apply
 AAA General RADIUS TACACS+ Authentation Accounting Authorization LDAP Local Net Users MAC Filtering Disabled Clients User Logn Policies Local EAP Priority Order Ccertificate Access Control Lists Wireless Protection Policies Web Auth TrustSec SXP Advanced 	Server Index (Priorit Server IP Address Shared Secret Confirm Shared Secr Port Number Server Status Server Timeout	y) it et	1 • 10.4.48.15 ASCII • • • • 49 5 second	is .				

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.

										done Vene
cisco	MONITOR	<u>W</u> LANs		WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	FEEDBACK	
Security	Priority C	Order > N	lanagement l	Jser						Apply
AAA										
Local EAP	Authentic	ation								
 Priority Order Management User 	Not	Used		Order L	Ised for Authe	ntication				
Certificate	RADIU	JS 🔺	>		TACACS+ *	Up				
Access Control Lists		~	<		*	Down	1			
Wireless Protection Policies										
Web Auth	If LOCAL is s	selected as	second priority the	en user will be	authenticated a	igainst				
TrustSec SXP	LOCAL only	if first prior	ity is unreachable.							
Advanced										

Procedure 13 Configure the resilient WLC

This design uses two WLCs. The first is the primary WLC, and the access points register to it. The second WLC provides resiliency in case the primary WLC fails. Under normal operation, there will not be any access points registered to this WLC.

Step 1: Configure the resilient AP-SSO secondary WLC by repeating Procedure 5 through Procedure 10.



In the event that you are using two WLCs using AP SSO mode of operation (Cisco 5500 Series WLCs or Cisco Flex 7500 Series Cloud Controllers), you should skip this procedure. If you are using two or more WLCs without AP SSO (vWLCs), then complete this procedure in order to create a mobility group.

Step 1: On the primary controller, navigate to **Controller > Mobility Management > Mobility Groups**. The MAC address, IP address, and mobility group name for the local controller are shown on the Static Mobility Group Members page.

սիսիս						Sa <u>v</u> e Cor	nfiguration <u>P</u> ing	Logout <u>R</u> efresh
cisco	MONITOR WL	ANS <u>C</u> ONTROLLE	R WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP FEEDBAC	ж
Controller	Static Mobili	ty Group Memb	ers				New	EditAll
General Inventory	Local Mobili	ty Group REM	DTES					
Interfaces	MAC Addres	IP Address	Group N	ame Mi	ulticast IP	Status		
Interface Groups	40:55:39:f6:	1d:40 10.4.46.68	REMOTES	s 0.	0.0.0	Up		
Multicast								
Network Routes								
Internal DHCP Server								
 Mobility Management Mobility Groups Mobility Anchor Config Multicast Messaging 								
Ports								
▶ NTP								
► CDP								
Advanced								
	-							

Step 2: On the resilient controller, navigate to Controller > Mobility Management > Mobility Groups, and then click New.

Step 3: In the Member IP Address box, enter the IP address of the primary controller. (Example: 10.4.46.68)

Step 4: In the Member MAC Address box, enter the MAC address of the primary controller, and then click Apply.

սիսիս							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	EEEDBAC	к
Controller	Mobility (Group Me	mber > New					<	Back	Apply
General Inventory Interfaces Interface Groups Multicast Network Routes Internal DHCP Server Mobility Management Mobility Anangement Mobility Anahor Config Multicast Messaging Ports NTP COP Advanced	Member Member Group Ni	IP Address MAC Addre ame	10.4.46.6 \$\$ 40:55:39 REMOTES	8 :f6:1d:40					Julk	сору

Step 5: On the primary controller, navigate to Controller > Mobility Management > Mobility Groups, and then click New.

Step 6: In the Member IP Address box, enter the IP address of the resilient controller. (Example: 10.4.46.69)

Step 7: In the Member MAC Address box, enter the MAC address of the resilient controller, and then click Apply.

արտիս					Sa <u>v</u> e Cor	nfiguration <u>P</u> ing Lo	gout <u>R</u> efresh
cisco	<u>M</u> ONITOR <u>W</u> LANS <u>C</u>	ONTROLLER WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP <u>F</u> EEDBACK	
Controller	Mobility Group Men	iber > New				< Back	Apply
General Inventory Interfaces Interface Groups Multicast Network Routes Internal DHCP Server Mobility Management Mobility Anacher Config	Member IP Address Member MAC Address Group Name	10.4.46.69 00:24:97:69:a8:a0 REMOTES					
Ports							
▶ NTP							
► CDP							
Advanced							

Step 8: On each controller, click Save Configuration, and then click OK.

Step 9: Navigate to Controller > Mobility Management > Mobility Groups, and then verify that connectivity is up between all the controllers by examining the mobility group information. In the Status column, all controllers should be listed as Up.

սիսիս						nfiguration <u>P</u> ing	Logout <u>R</u> efresh
cisco	MONITOR WLANS	CONTROLLER	WIRELESS SECU	IRITY MANAGEMENT	C <u>O</u> MMANDS	HELP FEEDBACH	<
Controller	Static Mobility Gr	oup Members	1			New	EditAll
General Inventory	Local Mobility Gro	up REMOTE	s				
Interfaces	MAC Address	IP Address	Group Name	Multicast IP	Status		
Interface Groups	40:55:39:f6:1d:40	10.4.46.68	REMOTES	0.0.0.0	Up		
Multicast	00:24:97:69:a8:a0	10.4.46.69	REMOTES	0.0.0.0	Up		
Internal DHCP Server							
 Mobility Management Mobility Groups Mobility Anchor Config Multicast Messaging 							
Ports							
▶ NTP							
► CDP							
Advanced							

Procedure 15 Configure the data wireless LAN

Wireless data traffic can handle delay, jitter, and packet loss more efficiently than wireless voice traffic. For the data WLAN, 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 number of the data SSID.

Step 3: On the General Tab, to the right of Status, select Enabled, and then click Apply.

սիսիս	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 Entries 1 - 1 of 1
WLANS	Current Filter: None [Change Filter] Create New Go
Advanced	WLAN Admin ID Type Profile Name WLAN SSID Status Security Policies
	1 WLAN WLAN-Data WLAN-Data Enabled [WPA2][Auth(802.1X)]

Step 4: On the Advanced tab, disable mDNS Snooping as this is not supported with FlexConnect Local Switching.



սիսիս		Sa <u>v</u> e	Configuration Ping Logout Refresh
cisco	MONITOR WLANS CONTROLLER WIRELESS	SECURITY MANAGEMENT COMMANDS HELP	EEDBACK
WLANs	WLANs > Edit 'WLAN-Data-RS201'		< Back Apply
 ₩LANS ¥LANS Advanced 	General Security Qos Advanced (15-100000) 000 Bytes Off-Lannel Scaning Defer Scan Defer Priority 0 1 2 3 5 6 7 Scan Defer Priority 0 1 2 3 4 5 6 7 Scan Defer Priority 0 1 2 3 4 5 6 7 Scan Defer Priority 100 Time(mses) 100 100 100 100 100 FlexConnect FlexConnect Local Image: Construct Local Imag	Media Session Snooping Re-anchor Roamed Voice Clients KTS based CAC Policy Client Profiling DHCP Profiling HTTP Profiling mDNS mDNS Snooping	Enabled Finabled
	•		

Procedure 16

Configure the voice wireless LAN

Wireless voice traffic is unique among other types of data traffic in that it cannot effectively handle delay and jitter or packet loss. To configure the voice WLAN, change the default QoS settings to Platinum and segment the voice traffic onto the voice wired VLAN.

cisco	MONITOR WLANS CONTROLLER WIRELESS SEA	
WLANs	WLANs	Entries 1 - 1 of 1
WLANS	Current Filter: None [Change Filter] [Clear Filter]	Create New Go
Advanced	ID Type Profile Name	Admin WLAN SSID Status Security Policies
	1 WLAN WLAN-Data	WLAN-Data Enabled [WPA2][Auth(802.1X)]

Step 1: On the WLANs page, in the list, choose Create New, and then click Go.

Step 2: Enter the Profile Name. (Example: Voice)

Step 3: In the SSID box, enter the voice WLAN name, and then click Apply. (Example: WLAN-Voice)

սիսիս									n <u>P</u> ing Lo <u>g</u> out <u>R</u> efresł
cisco	MONITOR	<u>W</u> LANs		WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK
WLANs	WLANs >	New							< Back Apply
WLANS WLANS Advanced	Type Profile Na SSID ID	me	WLAI Voice WLA1 2	N Vice					

Step 4: On the Advanced tab, disable mDNS Snooping as this is not supported with FlexConnect Local Switching.

Step 5: Enable FlexConnect Local Switching by selecting Enabled, and then click Apply.

ululu cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT	Save Configuration ping Logout Befresh COMMANDS HELP <u>F</u> EEDBACK
vilsio VLANS ♥ WLANS ₩LANS ₩LANS ₩LANS ₩LANS ₩LANS	MONTOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT WLANS Edit "Volce" General Security QOS Advanced J000000 Image: Security Image: Security Image: Security General Security QOS Advanced J0000000 Image: Security Image: Security Image: Security Off Channel Scanning Defer Image: Security Image: Security Image: Security Off Channel Scanning Defer Image: Security Image: Security Image: Security Off Channel Scanning Defer Image: Security Image: Security Image: Security Plack Connect Local Auth Image: Enabled Image: Security Image: Security Via hased Cortrol Image: Security Image: Security Image: Security Via hased Cortrol Image: Security Image: Security Image: Security Security Image: Security Image: Security Image: Security Via hased Cortrol Image: Security Image: Security Image: Security Central Dirth/PCP Procession Image: Security Image: Security Image: Security	Save Configuration Eng Logarit Befresh COMMANIOS HELP EEEDBACK
	VVernde DNS Enabled NAT-PAT Enabled	, , ,

Step 6: On the QoS tab, in the Quality of Service (QoS) list, choose Platinum (voice), and then click Apply.

cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MONAGEMENT COMMANDS HELP EEEDBACK	
√s	WLANs > Edit 'Voice'	Apply
/LANs WLANs	General Security QoS Advanced	
dvanced	Quality of Service (QoS) Platinum (voice) Application Visibility Enabled Avc Profile non e Netflow Monitor non e	
	Override Per-User Bandwidth Contracts (kbps) 14 DownStream UpStream	E
	Average Data Rate 0 0 Burst Data Rate 0 0	
	Average Real-Time Rate 0 0	
	Clear	
	Override Per-SSID Bandwidth Contracts (kbps) #	
	DownStream UpStream	
	Average Data Rate 0 0	
	Burst Data Rate 0 0	

Step 7: On the General tab, to the right of Status, select Enabled, and then click Apply.

cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP EEEDBACK	Sage Configuration ging Logout Befresh
WLANs	WLANs > Edit 'Voice'	< Back Apply
 WLASs WLASs WAvanced 	Vice Profile Name Voice Type WLAN SSID WLAN- Status Enabled Security Policies [WPA2[[Auth(@20.1x)]] (Modifications done under security tab will appear after applying the changes.) Redio Policy All Interferse2/Interface Group(C) management Multicast Vian Feature Enabled Brodscast SSID Enabled Multicast Vian Feature Enabled	

Procedure 17 Configure controller discovery

You have three options to configure controller discovery, depending on the number of controller pairs and the type of DHCP server you've deployed.

If you have only one controller pair in your organization, complete Option 1 of this procedure.

If you have deployed multiple controller pairs in your organization and you use Cisco IOS software in order to provide DHCP service, complete Option 2. If you have deployed multiple controller pairs in your organization and you use a Microsoft DHCP server, complete Option 3.





Option 1: Only one WLC pair in the organization

If AP SSO is being used, the WLC pair is represented by a single IP address, that being the management address of the primary WLC. The resilient secondary controller will assume the IP address of the primary in the event the primary WLC fails.

Step 1: Configure the organization's DNS servers (Example: 10.4.48.10) to resolve the **cisco-capwap-controller** host name to the management IP address of the controller. (Example: 10.4.46.64) The cisco-capwap-controller DNS record provides bootstrap information for access points that run software version 6.0 and higher.

Step 2: If the network includes access points that run software older than version 6.0, add a DNS record to resolve the host name **cisco-lwapp-controller** to the management IP address of the controller.

Option 2: Multiple WLC pairs in the organization: Cisco IOS DHCP server

In a network where there is no external central site DHCP server you can provide DHCP service with Cisco IOS software. This function can also be useful at a remote-site where you want to provide local DHCP service and not depend on the WAN link to an external central-site DHCP server.

Step 1: Assemble the DHCP Option 43 value.

The hexadecimal string is assembled as a sequence of the Type + Length + Value (TLV) values for the Option 43 suboption, as follows:

- *Type* is always the suboption code 0xf1.
- Length is the number of controller management IP addresses times 4 in hex.
- · Value is the IP address of the controller listed sequentially in hex.

For example, suppose there are two controllers with management interface IP addresses, 10.4.46.64 and 10.4.46.65. The type is 0xf1. The length is 2 * 4 = 8 = 0x08. The IP addresses translate to 0a042e44 (10.4.46.68) and 0a042e45(10.4.46.69). When the string is assembled, it yields **f1080a042e440a042e45**.

Step 2: On the network device, add Option 43 to the pre-existing data network DHCP Pool.

ip dhcp pool [pool name]
 option 43 hex [f1080a042e440a042e45]

Option 3: Multiple WLC pairs in the organization: Microsoft DHCP server

This procedure shows how the Microsoft DHCP server is configured to return vendor-specific information to the lightweight Cisco Aironet 1600, 2600, and 3600 Series Access Points used in this design guide. The vendor class identifier for a lightweight Cisco Aironet access point is specific to each model type. To support more than one access point model, you must create a vendor class for each model type.

Table 6 -	Vendor class identifiers	

Access point	Vendor class identifier
Cisco Aironet 1600 Series	Cisco AP c1600
Cisco Aironet 2600 Series	Cisco AP c2600
Cisco Aironet 3600 Series	Cisco AP c3600

Step 1: Open the DHCP Server Administration Tool or MMC.

Step 2: Navigate to DHCP > ad.cisco.local, right-click IPv4, and then click Define Vendor Classes.

9 DHCP			_ 8 ×
File Action View Help			
(= =) 🖄 📰 🗙 🖾 🧟 💀 📓 🖬			
P DHCP	Name	Actions	
E ad.dsco.local	IPv4	ad.cisco.local	
Display Statistics	₽V6	More Actions	•
New Scope			
New Superscope			
New Multicast Scope			
Define User Classes			
Denne Vendor Ciases			
Reconcile All Scopes			
Set Predefined Options			
Refresh			
Properties			
Help			
Define vendor specific option classes			

Step 3: In the DHCP Vendor Classes dialog box, click Add.

D	HCP Vendor Classes		? ×
	Name Microsoft Windows 20 Microsoft Windows 98 Microsoft Options	Description Microsoft vendor-specific option Microsoft vendor-specific option Microsoft vendor-specific option	Add
			Close

Step 4: In the New Class dialog box, enter a Display Name. (Example: Cisco Aironet 1600 AP)

Step 5: In the ASCII section, enter the vendor class identifier for the appropriate access point series from Table 6, and then click **OK**. (Example: Cisco AP c1600)

File Action View Help
Yes Name Actions
ad.cisco.local
DHCP Vendor Classes
Available classes:
Name Description Add
Min New Class
Mir Display name:
Cisc Aironet 1600 AP
Cis Cis Description:
Cis De Binaro: ASCII:
0000 43 69 73 63 6F 20 41 50 Cisco AP
OK Cancel

Step 6: In the DHCP Vendor Classes dialog box, click Close.

Step 7: Right-click the IPV4 DHCP server root, and then click Set Predefined Options.

Predefined Options and Values			
Option class:	Cisco Aironet 1600 AP	•	
Option name:		•	
	Add Edit	Delete	
Description:			
Value			
	DK	Cancel	

Step 8: In the Option Class list, choose the class you just created, and then click Add.

Step 9: In the Option Type dialog box, enter a Name. (Example: Option 43)

Step 10: In the Data Type list, choose IP Address.

Step 11: Select Array.

Step 12: In the Code box, enter 241, and then click OK.

Change Option Name ? 🗙			
Class:	Cisco Aironet 1600 AP		
<u>N</u> ame:	Option 43		
<u>D</u> ata type:	IP Address 💌 🗹 Array		
<u>C</u> ode:	241		
D <u>e</u> scription:	1		
	OK Cancel		

The vendor class and suboption are now programmed into the DHCP server. Now, you need to define the vendor-specific information for the DHCP scope.

Step 13: Choose the DHCP that you will be installing access points on, right-click Scope Options, and then click Configure Options.

Step 14: Click the **Advanced** tab, and then in the **Vendor class** list, choose the class you created in this procedure. (Example: Cisco Aironet 1600 AP)

Step 15: Under Available Options, select 241 Option 43.

Step 16: In the IP address box, enter the IP address of the primary controller's management interface, and then click Add. (Example: 10.4.46.68)

Scope Options	? 🗙
General Advanced	
Vendor class:	Cisco Aironet 1600 AP
User class:	Default User Class
Available Options	Description
241 Option 43	
d Data entry)
Server name:	
	Resolve
IP address:	
	Add
10.4.46.68	Remove
	Up
	Down
	OK Cancel Apply

Step 17: If you are not using AP-SSO, it is necessary to repeat Step 16 for the resilient controller, and then click **Apply**. (Example: 10.4.46.69)



Procedure 18 Configure the remote-site router

Remote-site routers require additional configuration in order to support wireless VLANs. If you have a single WAN remote-site router, complete Option 1 of this procedure. If you have dual remote-site routers, complete Option 2.

Option 1: Single WAN remote-site router

Step 1: Create wireless data and voice sub-interfaces on the router's interface that connects to the access layer switch. The interface will be a physical interface when the connection is a single link, and it will be a logical port-channel interface when the connection is EtherChannel.

```
interface GigabitEthernet0/2.65
description Wireless Data
encapsulation dot1Q 65
ip address 10.5.42.1 255.255.255.0
ip helper-address 10.4.48.10
ip pim sparse-mode
!
interface GigabitEthernet0/2.70
description Wireless Voice
encapsulation dot1Q 70
ip address 10.5.43.1 255.255.255.0
ip helper-address 10.4.48.10
ip pim sparse-mode
```

Step 2: If application optimization is deployed at the remote site as described in the Application Optimization Using Cisco WAAS Design Guide, configure Web Cache Communication Protocol (WCCP) redirection on the router's wireless data interface.

```
interface GigabitEthernet0/2.65
description Wireless Data
ip wccp 61 redirect in
```

Step 3: If the network does not have a central-site DHCP server, configure the Cisco IOS software DHCP service on the router.

```
ip dhcp excluded-address 10.5.42.1 10.5.42.10
ip dhcp excluded-address 10.5.43.1 10.5.43.10
ip dhcp pool WLAN-Data
network 10.5.42.0 255.255.255.0
default-router 10.5.42.1
domain-name cisco.local
dns-server 10.4.48.10
ip dhcp pool WLAN-Voice
network 10.5.43.0 255.255.255.0
default-router 10.5.43.1
domain-name cisco.local
dns-server 10.4.48.10
```
Option 2: Dual WAN remote-site routers

Step 1: On the primary router, create wireless data and voice sub-interfaces on the interface that connects to the access layer switch. The interface will be a physical interface when the connection is a single link, and it will be a logical port-channel interface when the connection is EtherChannel.

```
interface GigabitEthernet0/2.65
description Wireless Data
encapsulation dot1Q 65
ip address 10.5.42.2 255.255.255.0
ip helper-address 10.4.48.10
ip pim dr-priority 110
ip pim sparse-mode
standby version 2
standby 1 ip 10.5.42.1
standby 1 priority 110
standby 1 preempt
standby 1 authentication md5 key-string cisco123
standby 1 track 50 decrement 10
1
interface GigabitEthernet0/2.70
description Wireless Voice
encapsulation dot1Q 70
ip address 10.5.43.2 255.255.255.0
ip helper-address 10.4.48.10
ip pim dr-priority 110
ip pim sparse-mode
standby version 2
standby 1 ip 10.5.43.1
standby 1 priority 110
standby 1 preempt
standby 1 authentication md5 key-string cisco123
standby 1 track 50 decrement 10
```

Step 2: On the secondary router, create wireless data and voice sub-interfaces on the interface that connects to the access layer switch. The interface will be a physical interface when the connection is a single link, and a logical port-channel interface when the connection is EtherChannel.

```
interface GigabitEthernet0/2.65
description Wireless Data
encapsulation dot1Q 65
ip address 10.5.42.3 255.255.255.0
ip helper-address 10.4.48.10
ip pim dr-priority 105
ip pim sparse-mode
standby version 2
standby 1 ip 10.5.42.1
standby 1 priority 105
standby 1 preempt
```

```
standby 1 authentication md5 key-string ciscol23
!
interface GigabitEthernet0/2.70
description Wireless Voice
encapsulation dot1Q 70
ip address 10.5.43.3 255.255.255.0
ip helper-address 10.4.48.10
ip pim dr-priority 105
ip pim sparse-mode
standby version 2
standby 1 ip 10.5.43.1
standby 1 priority 105
standby 1 preempt
standby 1 authentication md5 key-string ciscol23
```

Step 3: If application optimization is deployed at the remote site as described in the Application Optimization Using Cisco WAAS Design Guide, configure WCCP redirection on both the primary and secondary router.

interface GigabitEthernet0/2.65
description Wireless Data
ip wccp 61 redirect in

Procedure 19 Configure the remote-site switch for APs

Before remote-site switches can offer the appropriate trunk behavior to access points configured for Cisco FlexConnect wireless switching, you must reconfigure the switch interfaces connected to the access points. For consistency and modularity, configure all WAN remote sites that have a single access switch or switch stack to use the same VLAN assignment scheme.

Step 1: On the remote-site switch, create the data and voice wireless VLANs.

vlan 65 name WLAN_Data vlan 70 name WLAN Voice

Step 2: Configure the existing interface where the router is connected to allow the wireless VLANs across the trunk. If there are two routers at the site, configure both interfaces.

interface GigabitEthernet 1/0/24
switchport trunk allowed vlan add 65,70

Step 3: Reset the switch interface where the wireless access point will connect to its default configuration.

default interface GigabitEthernet 1/0/23

Step 4: Configure the interface to which the access point will connect to allow a VLAN trunk for remote-site VLANs.

Tech Tip

The Inter-Switch Link trunking protocol is supported on Cisco Catalyst 3750-X Series Switches but not supported on Cisco Catalyst 2960s and 4500 Series Switches. As such, you do not need to specify the trunk encapsulation type on Catalyst 2960 and 4500 Series switches, but you do need to specify it on Catalyst 3750 Series switches.

interface GigabitEthernet 1/0/23 description FlexConnect Access Point Connection switchport trunk encapsulation dot1q switchport trunk native vlan 64 switchport trunk allowed vlan 64,65,70 switchport mode trunk switchport port-security maximum 255 spanning-tree portfast trunk macro apply EgressQoS

Procedure 20 Enable licensing on the vWLC

The Wireless LAN Controller virtual Appliance OVA includes a temporary 60-day license that includes 200 access points. You can activate the demo license included with the vWLC deployment by completing the following steps. After you acquire a permanent license from licensing@cisco.com, you must install and activate it, using the same steps below.

Caution

If you do not activate the demo licenses, you will be unable to register the access point with the vWLC.

Step 1: On the vWLC, navigate to Management > Software Activation > Licensing.

Step 2: Change the Priority to High by using the Set Priority button, and then click Apply.

Step 3: Accept the License, click OK, and then click Apply.

Step 4: Reboot the vWLC by navigating to Commands > Reboot > Save and Reboot.

Procedure 21 Configure the AP for Cisco FlexConnect

Step 1: Connect the access point to the remote-site switch, and then wait for the light on the access point to turn a solid color.

Step 2: On the WLC's web interface, navigate to Wireless > Access Points.

Step 3: Select the AP Name of the access point you want to configure.

Step 4: If the access points were not previously registered to the WLC prior to issuing the **autoconvert** command in Step 18 of Procedure 7, skip this step.

If the access points were registered to the WLC prior to issuing the **autoconvert** command, on the General tab, in the **AP Mode** list, choose **FlexConnect**, and then click **Apply**. Wait for the access point to reboot and reconnect to the controller. This should take approximately three minutes.

uluulu cisco	MONITOR WLANS CONT	TROLLER WIRELESS SECURIT	Sa <u>v</u> e Config TY M <u>A</u> NAGEMENT C <u>O</u> MMANDS F	uration <u>P</u> ing Logout <u>R</u> efre HELP <u>F</u> EEDBACK
Wireless	All APs > Details for Al	P44d3.ca42.309d		< Back Apply
Access Points All APs Radios 802.11a/n 802.11b/g/n Global Configuration Advanced Mesh RF Profiles	General General AP Name Location AP MAC Address Base Radio MAC Admin Status	Interfaces High Availa AP44d3.ca42.309d default location 44:d3:ca:42:30:9d 64:d9:89:42:28:e0 Enable	bility Inventory Advanced Versions Primary Software Version Backup Software Version Predownloads Status Predownload Version Predownload Hext Retry Time	7.2.104.16 0.0.0.0 None None
FlexConnect Groups FlexConnect ACLs 9 802.11a/n 9 802.11b/g/n 9 Media Stream Country Timers	AP Mode AP Sub Mode Operational Status Port Number Venue Group Venue Type	FlexConnect FlexConnect FlexC	Predownload Retry Count Boot Version IOS Version Mini IOS Version IP Config IP Address	NA 12.4.2.4 12.4(20120312:184417)\$ 7.0.114.214
▶ QoS	Venue Name Language Network Spectrum Interface Key	18551F89B90500F6FC39DDA82790	Static IP C16D6 Time Statistics UP Time Controller Associated Time Controller Association Latency	0 d, 00 h 46 m 45 s 0 d, 00 h 45 m 35 s 0 d, 00 h 01 m 09 s
	Hardware Reset Perform a hardware reset Reset AP Now	on this AP C	to Factory Defaults Jear configuration on this AP and reset it t lefaults Clear All Config Clear Config Except Static IP	o factory
	Foot Notes 1 DNS server IP Address and	d the Domain name can be set only a	fter a valid static IP is pushed to the AP.	

Step 5: In Wireless > Access Points, select the same access point as in Step 3.

Step 6: On the FlexConnect tab, select VLAN Support.

Step 7: In the Native VLAN ID box, enter the trunk's native VLAN number as configured in Procedure 17, and then click Apply. (Example: 64)

CISCO MONITOR MLANS CONTROLLER WIPELESS SECURITY MANAGEMENT CQMMANDS HEIP EEEDBACK Wireless All APs > Details for RS201-CAP36021 < Back Apply All APs Ceneral Cedentials Interfaces High Availability Inventory FlexConnect Advanced Mesh RF Profiles FlexConnect VLAN Imprings FlexConnect Advanced Mesh RE Profiles FlexConnect Net Configured Preduthentication ACcess Control Lists External Webdufaentication ACLs B02.11b/g/n OfficeExtend AP Enable Least Latency Control B02.11b/g/n Finable Least Latency Control Control OgS Fort Notes Interfaces and the Domain name can be set only after a valid state IP is pushed to the AP. Fort Notes	ahaha		Save Configuration Ping Logout Refresh
Wireless AI APs > Details for RS201-CAP36021 Lock Apply Access Points Alaps Boold and and and and and and and and and an	CISCO	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT	C <u>o</u> mmands he <u>l</u> p <u>f</u> eedback
 Access points Al Access points Al Access points Al Access points Solution Solution Solution Solution Solution Solution Solution Advanced Mish RF Profiles FecConnect Croups FecConnect Acces Solution Solution	Wireless	All APs > Details for RS201-CAP3602I	< Back Apply
	 Access Points All AP is Radios 802.11a/n 802.11a/n Global Configuration Advanced Mesh RF Profiles FlexConnect Groups FlexConnect ACLs 802.11a/n 802.11a/n 802.11b/g/n Media Stream Country Timers QoS 	General Credentials Interfaces High Availability Inventory VLAN Support Image: Support Supp	FlexConnect Advanced

Step 8: Click VLAN Mappings.

Step 9: For the data WLAN, in the VLAN ID box, enter the VLAN number from Procedure 17. (Example: 65)

Step 10: For the voice WLAN, in the **VLAN ID** box, enter the VLAN number from Procedure 17, and then click **Apply**. (Example: 70)

alaha sa								Sa <u>v</u> e Config	uration	Ping Log	qout <u>R</u> efresh
cisco	MONITOR	<u>W</u> LAN	s <u>c</u> o	NTROLLER	WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBAC	к
Wireless	All APs	> RS201	-CAP	3602l > VL	AN Mappir.	igs			< Back	A	oply
Access Points All APs Radios	AP Name		RS201	-CAP3602I							
802.11a/n	Base Ra	dio MAC	64:d9:	:89:47:14:20							
802.11b/g/n Global Configuration	WLAN Id	SSID				VLAN ID					
Advanced	1	WLAN-Da	ita			65					
Mesh RE Profiles	2	WLAN-Vo	ice			70					
FlexConnect Groups	Centrally	switche	d Wlar	ns							
802 11a/n	WLAN Id	l.	:	SSID	VLAN ID						
802.11b/g/n	AP level	VLAN AC	L Map	pina							
Media Stream	Vlan Id	In	gress /	ACL	Egress A	CL					
Country	146	no	one 🔻		none 🔻						
Timers	Group le	vel VLAN		Mapping							
▶ QoS	Vlan Id	In	gress /	ACL	Egress A	CL					



Procedure 22 Configure access points for resiliency

If you are using the AP SSO high availability feature on a Cisco 5500 Series WLC or Cisco Flex 7500 Series Cloud Controller, skip this procedure, as the resilient controller automatically tracks the primary controller and assumes its IP address in the event of a failure. The AP SSO feature is not available on the virtual wireless LAN controller (vWLC).

Step 1: On the primary WLC, navigate to **Wireless**, and then select the desired access point. If the access point is not listed, check the resilient WLC.

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-RemoteSites-1 / 10.4.46.68)

Step 4: In the **Secondary Controller** box, enter the name and management IP address of the resilient WLC, and then click **Apply**. (Example: WLC-RemoteSites-2 / 10.4.46.69)

	IR WIANC ((NTROLLER WIREL		MANAGEMENT		
Wireless All AP	e > Detaile for F	S201_CAP3602		MERICEMENT		Pack Apply
AIAI	s > Details for i	(3201-CAI 30021				Баск Аррлу
Access Points All APs Gene	eral Credentia	ls Interfaces	High Availability	Inventory	FlexConnect	Advanced
Radios 802.11a/n						
802.11b/g/n		Name	Mana	agement IP Add	ress	
Global Configuration Print	mary Controller	WLC-RemoteSites-1	10.4	.46.68		
Moch Ter	rtiary Controller	wEC-Remotesties-2	10.4	.40.09		
RE Profiles	controller					
FlexConnect ACLs FlexConnect ACLs 9 802.11a/n 9 802.11b/g/n 9 Media Stream Country Timers 9 QoS	Failover Priority	Low				
Foot 1 DNS	Notes S server IP Address	and the Domain name	can be set only after	a valid static IP is	pushed to the AP.	



Procedure 23 Configure Cisco FlexConnect groups

Step 1: On the WLC, navigate to Wireless > FlexConnect Groups, and then click New.

Step 2: In the Group Name box, enter a name that will allow you to associate the group with the remote site, and then click Apply. (Example: Remote-Site 1)

- Step 3: Under Group Name, click the group you just created.
- Step 4: Under Add AP, select Select APs from current controller.
- Step 5: In the AP Name list, choose an access point that is located at the site, and then click Add.
- Step 6: Repeat the previous step for every access point at the site.
- Step 7: Under AAA, enter the Server IP Address and Shared Secret, click Add, and then click Apply.

Step 8: Repeat Procedure 23 for each remote site.

Configuring Guest Wireless: Shared Guest Controller

- 1. Configure the distribution switch
- 2. Configure the firewall DMZ interface
- 3. Configure Network Address Translation
- 4. Configure guest network security policy
- 5. Create the guest wireless LAN interface
- 6. Configure the guest wireless LAN
- 7. Create the lobby admin user account
- 8. Create guest accounts

Procedure 1 Configure the distribution switch

The VLAN used in the following configuration examples is:

Guest Wireless-VLAN 1128, IP: 192.168.28.0/22

Step 1: On the LAN distribution switch, for Layer 2 configuration, create the guest wireless VLAN.

vlan **1128**

name Guest_Wireless

PROCESS



Step 2: Configure the interfaces that connect to the Internet edge firewalls by adding the wireless VLAN.

```
interface GigabitEthernet1/0/24
description IE-ASA5540a Gig0/1
!
interface GigabitEthernet2/0/24
description IE-ASA5540b Gig0/1
!
interface range GigabitEthernet1/0/24, GigabitEthernet2/0/24
switchport trunk allowed vlan add 1128
```

Step 3: Configure the interfaces that connect to the WLCs by adding the wireless VLAN.

```
interface Port-channel [WLC #1 number]
description WLC-1 LAG
!
interface Port-channel [WLC #2 number]
description WLC-2 LAG
!
interface range Port-channel [WLC #1 number], Port-channel [WLC #2 number]
switchport trunk allowed vlan add 1128
```

Procedure 2 Configure the firewall 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 guest DMZ is connected to Cisco Adaptive Security Appliances (ASA) on the appliances' internal Gigabit Ethernet 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 internal distribution switch's VLAN interface does not have an IP address assigned for the DMZ VLAN.

Table 7 - C	Cisco ASA	DMZ interface	information
-------------	-----------	---------------	-------------

Interface Label	IP Address & Netmask	VLAN	Security Level	Name
GigabitEthernet0/0.1128	192.168.28.1/22	1128	10	dmz-guests

Step 1: Login to the Internet Edge firewall using Cisco Adaptive Security Device Manager (Cisco ASDM).

Step 2: Navigate to Configuration -> Device Setup ->Interfaces.

Step 3: On the Interface pane, click Add > Interface.

Step 4: In the **Hardware Port** list, choose the interface that is connected to the internal LAN distribution switch. (Example: GigabitEthernet0/0)

Step 5: In the VLAN ID box, enter the VLAN number for the DMZ VLAN. (Example: 1128)



Step 6: In the Subinterface ID box, enter the VLAN number for the DMZ VLAN. (Example: 1128)

Step 7: Enter an Interface Name. (Example: dmz-guests)

Step 8: In the Security Level box, enter a value of 10.

Step 9: Enter the interface IP Address. (Example: 192.168.28.1)

Step 10: Enter the interface Subnet Mask, and then click OK. (Example: 255.255.252.0)

Add Interface		×
General Advance	ad IPv6	
Hardware Port:	GigabitEthernet0/1 👻	
VLAN ID:	1128	
Subinterface ID:	1128	
Interface Name:	dmz-guests	
Security Level:	10	
Dedicate this	interface to management only	
Channel Group:		
V Enable Interf	ace	
IP Address		
Ose Static	IP 💿 Obtain Address via DHCP 💿 Use PPPoE	
ID Address:	107 168 78 1	
Subnet Mad	~ 255 255 252 0	
Subnethildar		
Description:		
	OK Cancel Help	

Step 11: Navigate to Configuration > Device Management > High Availability > Failover.

Step 12: On the Interfaces tab, in the Standby IP address column, enter the IP address of the standby unit for the interface you just created. (Example: 192.168.28.2)

August 2013

Step 13: Select Monitored, and then click Apply.

Interface Name	Name	Active IP Address	Subnet Mask/ Prefix Length	Standby IP Address	Monitored	
GigabitEthernet0/0.300	inside	3 10.4.24.30	255.255.255.224	3 10.4.24.29		
GigabitEthernet0/1.1116	dmz-web	3 192.168.16.1	255.255.255.0	3 192.168.16.2		
L		🖳 2001:db8:	64	🖳 2001:db8:a:		
GigabitEthernet0/1.1117	dmz-email	🖳 192.168.17.1	255.255.255.0	📇 192.168.17.2		
GigabitEthernet0/1.1118	dmz-dmvpn	3, 192.168.18.1	255.255.255.0	3 192.168.18.2		
GigabitEthernet0/1.1119	dmz-wlc	🖳 192.168.19.1	255.255.255.0	4 192.168.19.2		
GigabitEthernet0/1.1123	dmz-management	4 192.168.23.1	255.255.255.0	3, 192.168.23.2		
GigabitEthernet0/1.1128	dmz-guests	🖳 192.168.28.1	255.255.252.0	192.168.28.2		
GigabitEthernet0/3.16	outside-16	🖳 172.16.13	255.255.255.0	🖳 172.16.130		
L		🖳 2001:db8:	64	📇 2001:db8:a::2		
GigabitEthernet0/3.17	outside-17	🖳 172.17.13	255.255.255.0	📇 172.17.130		
Management0/0	IPS-mgmt					

Step 14: At the bottom of the window, click Apply. This saves the configuration.

Procedure 3 Configure Network 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 guest clients to an outside public address.

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

Step 2: Click Add > Network Object.

Step 3: In the Add Network Object dialog box, in the **Name** box, enter a description for the guest network. (Example: dmz-guests-network-ISPa)

- Step 4: In the Type list, choose Network.
- Step 5: In the IP Address box, enter the guest DMZ network address. (Example: 192.168.28.0)
- Step 6: Enter the guest DMZ netmask. (Example: 255.255.252.0)
- **Step 7:** Click the two down arrows. The NAT pane expands.
- Step 8: Select Add Automatic Address Translation Rules.
- Step 9: In the Type list, choose Dynamic PAT (Hide).



Step 10: In the **Translated Addr** list, choose the interface name for the primary Internet connection. (Example: outside-16)

💁 Add Network	Object 💌
Name:	dmz-guest-network-ISPa
Туре:	Network
IP Version:	● IPv4 ○ IPv6
IP Address:	192.168.28.0
Netmask:	255.255.252.0
Description:	DMZ outside PAT address for ISPa
NAT	*
🔽 Add Autom	atic Address Translation Rules
Type:	Dynamic PAT (Hide) 👻
Translated A	ddr: outside-16
Use one-	to-one address translation
PAT Pool	Translated Address:
Round	Robin
Extend	PAT uniqueness to per destination instead of per interface
Transla	ate TCP and UDP ports into flat range 1024-65535 🗌 Include range 1-1023
Fall throu	igh to interface PAT(dest intf): IPS-mgmt 🚽
Use IPv6	for interface PAT
	Advanced
	OK Cancel Help

Step 11: Click Advanced.

Step 12: 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: 💌 🔻
Real Port:
Mapped Port:
OK Cancel Help

Step 13: In the Add Network Object dialog box, click OK.

Procedure 4 Configure guest network 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

First, you enable the guests to communicate with the DNS and DHCP servers in the data center.

Step 3: Click Add > Insert.

Step 4: In the Interface list, choose Any.

Step 5: In the **Source** list, choose the network object automatically created for the guest DMZ. (Example: dmz-guests-network/22)

Step 6: In the Destination list, choose the network object for the DNS server. (Example: internal-dns)

Step 7: In the Service list, enter udp/domain, tcp/domain, and then click OK.

insert Access	; Rule
Interface:	Any 🔻
Action: 🧿 Perr	nit 🕐 Deny
Source Criteria	
Source:	dmz-guests-network/22
User:	
Security Group:	
Destination Crite	
Destination:	internal-dns -
Security Group:	
Service:	udp/domain, tcp/domain
Description:	Allow Guest Wireless users to resolve DNS names.
📝 Enable Logg	ing
Logging Levi	əl: Default 👻
More Options	*
	OK Cancel Help

Step 8: Click Add > Insert.

Step 9: In the Interface list, choose Any.

Step 10: In the **Source** list, choose the network object automatically created for the guest DMZ. (Example: dmz-guests-network/22)



Step 11: In the Destination list, choose the network object for the DHCP server. (Example: internal-dhcp)

🔁 Add Access	Rule
Interface:	Any 🔹
Action: 🧿 Perr	nit 🔘 Deny
Source Criteria	
Source:	dmz-guests-network/22
User:	
Security Group:	· · · · · · · · · · · · · · · · · · ·
Destination Crite	eria
Destination:	internal-dhcp
Security Group:	
Service:	udp/bootps
Description:	Allow Hosts on DMZ Guest Network access to DHCP server for IP address assignment.
📝 Enable Logg	ing
Logging Levi	el: [Default +
More Options	*
	OK Cancel Help

Step 12: In the Service list, enter udp/bootps, and then click OK.

Next, you enable the guests to communicate with the web servers in the DMZ.

Step 13: Click Add > Insert.

Step 14: In the Interface list, choose Any.

Step 15: In the **Source** list, choose the network object automatically created for the guest DMZ. (Example: dmz-guests-network/22)

Step 16: In the **Destination** list, choose the network object automatically created for the web DMZ. (Example: dmz-web-network/24)

Step	17:	In the	Service	list,	enter	tcp/http,	tcp/https,	and then	click OK.
------	-----	--------	---------	-------	-------	-----------	------------	----------	-----------

📴 Insert Access	Rule
Interface:	Any 🔻
Action: 💿 Perr	nit 🕐 Deny
Source Criteria	
Source:	dmz-guests-network/22
User:	
Security Group:	
Destination Crite	ria
Destination:	dmz-web-network/24
Security Group:	
Service:	tcp/http, tcp/https
Description:	All wireless guest users access to DMZ based webservers, possibly for walled garden access
🔽 Enable Logg	ing
Logging Leve	al: Default 🗸
More Options	¥
	OK Cancel Help

Next, you remove the guest's ability communicate with other internal and DMZ devices.

- Step 18: Click Add > Insert.
- Step 19: In the Interface list, choose Any.
- Step 20: To the right of Action, select Deny.

Step 21: In the **Source** list, choose the network object automatically created for the guest DMZ. (Example: dmz-guests-network/22)

Step 22: In the **Destination** list, choose the network objects for the internal and DMZ networks, and then click **OK**. (Example: internal-network, dmz-networks)

둴 Edit Access F	Rule
Interface:	Any
Action: 🔘 Perr	nit 💿 Deny
Source Criteria	
Source:	dmz-guests-network/22
User:	
Security Group:	
Destination Crite	ria
Destination:	dmz-networks, internal-network
Security Group:	
Service:	ip 💮
Description:	Deny traffic from the wireless guest network to the internal and dmz resources
🔽 Enable Logg	ing
Logging Leve	el: Default 👻
More Options	*
	OK Cancel Help

Next, you enable the guests to communicate with the Internet.

Step 23: Click Add > Insert.

Step 24: In the Interface list, choose Any.

Step 25: In the **Source** list, choose the network object automatically created for the guest DMZ, click **OK**, and then click **Apply**. (Example: dmz-guests-network/22)

insert Access	Rule
Interface:	Any 🔻
Action: 💿 Perr	nit 🕜 Deny
Source Criteria	
Source:	dmz-guests-network/22
User:	
Security Group:	
Destination Crite	eria
Destination:	any
Security Group:	
Service:	ip
Description:	Allow Wireless DMZ users access to the internet
📝 Enable Logg	ing
Logging Levi	el: Default 👻
More Options	*
	OK Cancel Help

Procedure 5 Create the guest wireless LAN interface

The guest wireless interface is connected to the DMZ of the Cisco ASA 5500 Series Adaptive Security Appliances. This allows guest wireless traffic only to and from the Internet. All traffic, regardless of the controller that the guest initially connects to, is tunneled to the guest WLC and leaves the controller on this interface. To easily identify the guest wireless devices on the network, use an IP address range for these clients that are not part of your organization's regular network. This procedure adds an interface that allows devices on the guest wireless network to communicate with the Internet.

Step 1: In Controller>Interfaces, click New.

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

ahaha						Sa <u>v</u> e C	Configuration <u>P</u> i	ng Lo	gout <u>R</u> efresh
cisco	MONITOR	<u>W</u> LANs	<u>C</u> ONTROLLER	WIRELESS	<u>S</u> ECURITY	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK
Controller		Inter	faces > New	T			< Back		Apply
General Inventor Interfac	r y es	Int VL	erface Name AN Id	Wireless-Guest 1128					
Interfac Multicas Network	e Groups t : Routes								
Mobility	Managemer	it							
Ports NTP									
CDP									
▶ mDNS									
Advance	d								

Step 3: Enter the VLAN Id, and then click Apply. (Example: 1128)

Step 4: In the **IP Address** box, enter the IP address you want to assign to the WLC interface. (Example: 192.168.28.5)

Step 5: Enter the Netmask. (Example: 255.255.252.0)

Step 6: In the **Gateway** box, enter the IP address of the firewall's DMZ interface, defined in Procedure 2. (Example: 192.168.28.1)

Step 7: 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 L	.ogout <u>R</u> efresh
CISCO	MONITOR	<u>W</u> LANs	<u>CONTROLLER</u>	WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK
Controller	Interface	s > Edit					< Back		Apply
General Inventory Interfaces	General I	nformati	on						
Interface Groups	Interface	Name	wireless	-guest					
Multicast	MAC Add	ress	88:43:e	1:7e:11:cf					
Network Routes Internal DHCP Server 	Configura	ition							
Mobility Management	Guest La	n							
Ports	Quarantir	he							
▶ NTP	Quarantii	ne Vlan Id	0						
CDP	Physical 1	informati	on						
P IPV6	The inter	face is atta	ched to a LAG.						
F Advanced	Enable D	ynamic AP	Management 📄						
	Interface	Address							
	VLAN Ide	ntifier	112	28					
	IP Addres	55	192	2.168.28.5					
	Netmask		255	5.255.252.0					
	Gateway		193	2.168.28.1					
	DHCP Info	ormation							
	Primary I	DHCP Serve	er 1	0.4.48.10					
	Secondar	ry DHCP Se	rver						
	Access Co	ontrol Lis	t						
	ACL Nam	e		none 🔻					
	Note: Chang temporarily some clients	ing the Int disabled ar 5.	erface parameter nd thus may resul	s causes the Wl t in loss of conr	ANs to be ectivity for				

Tech Tip

1

To prevent DHCP from assigning addresses to wireless clients that conflict with the WLC's addresses, exclude the addresses you assign to the WLC interfaces from DHCP scopes.

Step 1: On the WLANs page, in the list, choose Create New, and then click Go.

WLANS WLANS Current Filter: None Current Filter: </th <th>տիտիս cisco</th> <th>Saye Configuration Ping Logou MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK</th> <th>t <u>R</u>efres</th>	տիտիս cisco	Saye Configuration Ping Logou MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK	t <u>R</u> efres
WLANS WLANS Current Filter: None Chance filter] Create New Go Advanced UNAN TD Type Profile Name WLAN SSID Status 2 WLAN WLAN-Data WLAN-Data Enabled [WPA2][Auth(802.1X)] 2 WLAN Voice WLAN-Voice Enabled [WPA2][Auth(802.1X)]	WLANs	WLANS Entries 1	- 2 of 2
Mdvanced WLAN Type Profile Name WLAN SSID Admin Status Security Policies 1 WLAN WLAN-Data Enabled [WPA2][Auth(802.1X)] 2 WLAN Voice WLAN-Poice Enabled [WPA2][Auth(802.1X)]	WLANS	Current Filter: None [Change Filter] Create New - Go	
WLAN Voice WLAN-Voice Enabled [WPA2][Auth(802.1X)]	Advanced	WLAN Admin ID Type Profile Name WLAN SSID Status Security Policies 1 WLAN WLAN-Data Fenabled [WP42][Juth/602.133]	
		2 WLAN Voice Enabled [WPA2][Auth(00212)]	

Step 2: Enter the Profile Name. (Example: Guest)

Step 3: In the SSID box, enter the guest WLAN name, and then click Apply. (Example: Guest)

CISCO MONTOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK WLANS WLANS WLANS VULANS VULANS Type Profile Name Guest SSID ID 3 V	սիսիս						nfiguration <u>P</u> ing I	.ogout <u>R</u> efresh
WLANs WLANs Type WLAN Mulans Advanced SID Guest </th <th>CISCO</th> <th>MONITOR WLANS</th> <th><u>CONTROLLER</u> WIRELE</th> <th>55 <u>S</u>ECURITY</th> <th>MANAGEMENT</th> <th>COMMANDS</th> <th>HELP FEEDBACK</th> <th></th>	CISCO	MONITOR WLANS	<u>CONTROLLER</u> WIRELE	55 <u>S</u> ECURITY	MANAGEMENT	COMMANDS	HELP FEEDBACK	
VLANs Type WLAN Pofile Name Guest SSD Guest ID 3	WLANs	WLANs > New					< Back	Apply
	WLANS WLANS WLANS Advanced	WLANS > New Type Profile Name SSID ID	WLAN Cuest Guest 3				< Back	Αρρίγ

Step 4: On the General tab, in the **Interface/Interface Group(G)** list, choose the interface created in Procedure 5. (Example: wireless-guest)

ահահ				Sa <u>v</u> e Configuration <u>P</u> ing	Logout <u>R</u> efresh
CISCO	MONITOR WLANS CON	TROLLER WIRELESS SE	CURITY MANAGEMENT	COMMANDS HELP FEEDBA	АСК
WLANs	WLANs > Edit 'Guest			< Back	Apply
wi ANc					
WLANs	General Security	QoS Advanced			
Advanced					
	Profile Name	Guest			
	Туре	WLAN			
	SSID	Guest			
	Status	Enabled			
	Security Policies	[WDAD][Auth(800.1X)]			
	Security Policies	(Modifications done under sec	urity tab will appear after ap	plying the changes.)	
	Dadia Daliau	411			
	Radio Policy	All			
	Group(G)	wireless-guest 💌			
	Multicast Vlan Feature	Enabled			
	Broadcast SSID	V Enabled			
	broddedae obro				
	Foot Notes				
	1 Web Policy cannot be use	d in combination with IPsec			
	2 H-REAP Local Switching is	not supported with IPsec, CRA	NITE authentication		
	3 When client exclusion is e 4 Client MFP is not active ui	napieg, a Timeout Value of zen nless WPA2 is configured	o means infinity (will require	administrative override to reset exc	luaed clients)
	5 Learn Client IP is configur	able only when HREAP Local Sv	vitching is enabled		
	6 WMM and open or AES se 7 Multicast Should Be Enable	curity snould be enabled to sup led For IPV6.	port nigner 11n rates		
	8 Band Select is configurable	le only when Radio Policy is set	to 'All'.		
	9 Value zero implies there i 10 MAC Filtering is not supp	s no restriction on maximum cli ported with HREAP Local authen	ents allowed. tication		
	11 MAC Filtering should be	enabled.			
	12 Guest tunneling, Local s 13 Max-associated-clients fi	witching, DHCP Required should eature is not supported with HR	t be disabled. IEAP Local Authentication.		

Step 5: Click the Security tab, and then on the Layer 2 tab, in the Layer 2 Security list, choose None.

cisco	Save Configuration Ping Logout Betrear MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
WLANs	WLANs > Edit 'Guest' Apply
WLANS	General Security QoS Advanced
Advanced	Layer 2 Layer 3 AAA Servers
	Leyer 2 Security ⁹ None •
	Foot Notes 1 Web Policy cannot be used in combination with IPsec 2 H-REA 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 MED is not stolin wither WID3 is enablement
	4 Client MPF is not active unless WPA2 is configured 5 Learn Client IP is configurable only when HRAP Local Switching is enabled 6 WIM and open or AES security should be enabled to support higher 11n rates 7 Multicast Should Be Enabled for IPV6. 8 Band Select is configurable only when Radio Policy is set to 'AI'. 9 Value zero implies there is no restriction on maximum clients allowed. 10 MAC Filtering is not supported with HRAP Local authentication 11 MAC Filtering is not able anabled. 12 Guest turneling, Local switching, DHCP Required should be disabled. 13 Mareasscieted-clients fatture is not supported with HRAP Local Authentication.



Step 6: On the Layer 3 tab, select Web Policy, and then click OK.

Step 7: On the QoS tab, in the Quality of Service (QoS) list, choose Bronze (background), and then click Apply.

iliulu cisco	Saye Configuration Ping Logout <u>R</u> efresh MONITOR <u>W</u> LANS <u>C</u> ONTROLLER WIRELESS <u>S</u> ECURITY MANAGEMENT C <u>O</u> MMANDS HELP <u>F</u> EEDBACK
WLANs	WLANs > Edit 'Guest' <back apply<="" th=""></back>
WLANS	General Security QoS Advanced
➤ Advanced	Quality of Service (QoS) Bronze (background) • WMM Policy Allowed • 7920 AP CAC Enabled 7920 Client CAC Enabled
	Foot Notes 1 Web Policy cannot be used in combination with IPsec 2 H-REAP Local Switching is not supported with IPsec, CRANITE authentication 3 When clear texclusion is enabled, a Timeout Value of zero means infinity (will require administrative override to reset excluded clients) 4 Client MPF is not active unless WPA2 is configured 5 Learn Client IP is configurable only when HREAP Local Switching is enabled 6 WMM and open or AES security should be enabled to support higher 11n rates 7 Multicast Should be Enabled for IPr6. 8 Band Select is configurable only when HREAP Local Switching is enabled 10 MAC Filtering is no t supported with HREAP Local Switching is enabled. 11 MAC Filtering is not supported with HREAP Local authentication 12 KGC Intering Should be enabled. Local authentication.

Step 8: On the General tab, to the right of Status, select Enabled, and then click Apply.



Procedure 7 Create the lobby admin user account

Typically, the lobby administrator is the first person to interact with your corporate guests. The lobby administrator can create individual guest user accounts and passwords that last from one to several days, depending upon the length of stay for each guest.

Step 1: In Management > Local Management Users, click New.

Step 2: Enter the username. (Example: Guest-Admin)

Step 3: Enter and confirm the password. (Example: C1sco123)

Step 4: In the User Access Mode list, choose LobbyAdmin, and then click Apply.

սիսիս							Sa <u>v</u> e Co	nfiguration <u>P</u> ing Lo <u>q</u> out !	<u>R</u> efresh
cisco	MONITOR	<u>W</u> LANs		WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP FEEDBACK	
Management	Local Ma	nageme	nt Users > Ne	ew				< Back Ap	ply
Summary SNMP HTTP-HTTPS Telnet-SSH Serial Port Local Management User Sessions Logs Mgmt Via Wireless Software Activation Fech Support	User Nam	ie Password Iss Mode	Gue	at-Admin 					

Procedure 8 Create guest accounts

Now you can use the lobby administrator account to create usernames and passwords for partners, customers, and anyone else who is not normally granted access to your network.

Step 1: Using a web browser, open the WLC's web interface (for example, https://wlc-1.cisco.local/), and then log in using your LobbyAdmin account with the username **Guest-Admin** and password **C1sco123**.

Step 2: From the Lobby Ambassador Guest Management page, click New.

	Lobby Ambassador Guest Management	Logout Refresh Help
Guest Management	Guest Users List	New
	Items 0 User Name WLAN SSID Account Remaining Time Description	to 0 of 0

Step 3: Create a new username and password, or allow the system to create a password automatically by selecting **Generate Password**.

cisco	Lobby Ambassador Gues	Management	Logout	Refresh Help
Guest Management	Guest Users List > N	3W	< Back	Apply
	User Name Generate Password Password Confirm Password Lifetime Guest User Role WLAN SSID Description	partner		

Step 4: Click Apply. The new user name and password are created.

With a wireless client, you can now test connectivity to the guest WLAN. Without any security enabled, you should receive an IP address, and after opening a web browser, you should be redirected to a web page to enter a username and password for Internet access, which will be available to a guest user for 24 hours.

August 2013



Procedure 1

Configure the DMZ switch

The VLANs used in the following configuration examples are:

- · Guest Wireless-VLAN 1128, IP: 192.168.28.0/22
- · Wireless management-VLAN 1119, IP 192.168.19.0/24

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

vlan 1119 name WLAN_Mgmt vlan 1128 name Guest_Wireless 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-ASA5545a Gig0/1
!
interface GigabitEthernet2/0/24
description IE-ASA5545b Gig0/1
!
interface range GigabitEthernet1/0/24, GigabitEthernet2/0/24
switchport trunk encapsulation dot1q
switchport trunk allowed vlan add 1119, 1128
switchport mode trunk
macro apply EgressQoS
logging event link-status
logging event trunk-status
no shutdown
```

Step 3: This deployment uses Layer 2 EtherChannels in order to connect the WLCs to the DMZ switch. Connect the WLC EtherChannel uplinks to separate devices in the DMZ stack.

On the DMZ switch, the physical interfaces that are members of a Layer 2 EtherChannel are configured prior to configuring the logical port-channel interface. Doing the configuration in this order allows for minimal configuration because most of the commands entered to a port-channel interface are copied to its members' interfaces and do not require manual replication.

Configure two or more physical interfaces to be members of the EtherChannel. It is best if they are added in multiples of two.

```
Interface range GigabitEthernet1/0/13, GigabitEthernet2/0/13
description DMZ-WLC-Guest-1
!
Interface range GigabitEthernet 1/0/14, GigabitEthernet 2/0/14
description DMZ-WLC-Guest-2
Т
interface range GigabitEthernet 1/0/13, GigabitEthernet 2/0/13
channel-group 12 mode on
macro apply EgressQoS
logging event link-status
logging event trunk-status
 logging event bundle-status
interface range GigabitEthernet 1/0/14, GigabitEthernet 2/0/14
channel-group 13 mode on
macro apply EgressQoS
logging event link-status
logging event trunk-status
 logging event bundle-status
```

Step 4: Configure trunks.

An 802.1Q trunk is used for the connection to the WLC, which allows the firewall to provide the Layer 3 services to all the VLANs defined on the access layer switch. The VLANs allowed on the trunk are reduced to only the VLANs that are active on the WLC.

```
interface Port-channel12
description DMZ-WLC-Guest-1
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 1119,1128
switchport mode trunk
logging event link-status
no shutdown
interface Port-channel13
description DMZ-WLC-Guest-2
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 1119,1128
switchport mode trunk
logging event link-status
no shutdown
```

Procedure 2 Configure the firewall 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 appliances' Gigabit Ethernet 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.

Interface Label	IP Address & Netmask	VLAN	Security Level	Name
GigabitEthernet0/1.1119	192.168.19.1/24	1119	50	dmz-wlc
GigabitEthernet0/1.1128	192.168.28.1/22	1128	10	dmz-guests

Table 8 - Cisco ASA DMZ interface information

Step 1: Login to the Internet Edge firewall using Cisco ASDM.

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

Step 3: Click Edit.

Step 4: Select Enable Interface, and then click OK.

🔂 Edit Interface						
General Advanced IPv6						
Hardware Port: GigabitEthernet0/1 Configure Hardware Properties						
Security Level:						
Dedicate this interface to management only						
Channel Group:						
Enable Interface						
IP Address						
⊚ Use Static IP Obtain Address via DHCP O Use PPPoE						
IP Address:						
Description						
OK Cancel Help						

Step 5: On the Interface pane, click **Add > Interface**.

Step 6: In the Haruware Port list, choose the interface configured in Step 2. (Example, Gigabitethe	.nernetu	J/ I.
--	----------	-------

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

Step 8: In the Subinterface ID box, enter the VLAN number for the DMZ VLAN. (Example: 1119)

Step 9: Enter an Interface Name. (Example: dmz-wlc)

Step 10: In the Security Level box, enter a value of 50.

Step 11: Enter the interface IP Address. (Example: 192.168.19.1)

Edit Interface
General Advanced IPv6
Hardware Port: GigabitEthernet0/1.1119 VLAN ID: 1119 Subinterface ID: 1119 Interface Name: dmz-wlc Security Level: 50 Dedicate this interface to management only Channel Group: Image:
IP Address Use Static IP Obtain Address via DHCP Use PPPoE IP Address: 192.168.19.1 Subnet Mask: 255.255.255.0
Description: WLC DMZ Trunk to DMZ Switch OK Cancel Help

Step 12: Enter the interface Subnet Mask, and then click OK. (Example: 255.255.255.0)

Step 13: Navigate to Configuration > Device Management > High Availability and Scalability > Failover.

Step 14: On the Interfaces tab, in the Standby IP address column, enter the IP address of the standby unit for the interface you just created. (Example: 192.168.19.2)

Step 15: Select Monitored, and then click Apply.

Interrace Name	Name	Active IP Address	Prefix Length	Standby IP Address	Monicored	
GigabitEthernet0/0.300	inside	🖳 10.4.24.30	255.255.255.224	🖳 10.4.24.29		
GigabitEthernet0/1.1116	dmz-web	🖳 192.168.16.1	255.255.255.0	🖳 192.168.16.2		
L		💐 2001:db8:	64	💐 2001:db8:a:		
SigabitEthernet0/1.1117	dmz-email	🖳 192.168.17.1	255.255.255.0	4 192.168.17.2		
SigabitEthernet0/1.1118	dmz-dmvpn	🖳 192.168.18.1	255.255.255.0	4 192.168.18.2		
SigabitEthernet0/1.1119	dmz-wlc	192.168.19.1	255.255.255.0	192.168.19.2		
SigabitEthernet0/1.1123	dmz-management	4 192.168.23.1	255.255.255.0	4 192.168.23.2		
SigabitEthernet0/1.1128	dmz-guests	🖳 192.168.28.1	255.255.252.0	4 192.168.28.2		
GigabitEthernet0/3.16	outside-16	🖳 172.16.13	255.255.255.0	4 172.16.130		
L		🖳 2001:db8:	64	🖳 2001:db8:a::2		
SigabitEthernet0/3.17	outside-17	릨, 172.17.13	255.255.255.0	鸟 172.17.130		
Management0/0	IPS-mgmt					

Step 16: At the bottom of the window, click Apply. This saves the configuration.

Step 17: Repeat Step 5 through Step 12 for the dmz-guests interface.

Procedure 3 Configure Network 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 guest clients to an outside public address.

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

Step 2: Click Add > Network Object.

Step 3: In the Add Network Object dialog box, in the **Name** box, enter a description for the guest network. (Example: dmz-guests-network-ISPa)

Step 4: In the Type list, choose Network.

Step 5: In the IP Address box, enter the guest DMZ network address. (Example: 192.168.28.0)

Step 6: Enter the guest DMZ netmask. (Example: 255.255.252.0)

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

Step 8: Select Add Automatic Address Translation Rules.

Step 9: In the Type list, choose Dynamic PAT (Hide).

Step 10: In the **Translated Addr** list, choose the interface name for the primary Internet connection. (Example: outside-16)

🔄 Add Network	: Object					
Name:	dmz-guest-network-ISPa					
Туре:	Network					
IP Version:	● IPv4					
IP Address:	192.168.28.0					
Netmask:	255.255.252.0 🗸					
Description:	DMZ outside PAT address for ISPa					
NAT	*					
🚺 Add Autom	atic Address Translation Rules					
Type:	Dynamic PAT (Hide) 👻					
Translated A	ddr: outside-16					
Use one-	-to-one address translation					
PAT Poo	Translated Address:					
Round	IRobin					
Extend	d PAT uniqueness to per destination instead of per interface					
Transl	ate TCP and UDP ports into flat range 1024-65535 📃 Include range 1-1023					
Fall through to interface PAT(dest intf): IPS-mgmt						
Use IPv6 for interface PAT						
Advanced						
	OK Cancel Help					

Step 11: Click Advanced.

Step 12: In the **Destination Interface** list, choose the interface name for the primary Internet connection, and then click **OK**. (Example: outside-16)

Advanced NAT Settings	— X—				
Translate DNS replies for rule					
Interface	_				
Source Interface: Any	•				
Destination Interface: outside-16					
OK Cancel Help					

Step 13: In the Add Network Object dialog box, click OK.

Procedure 4 Create network objects

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

First, add a network object for the every internal WLC in your organization.

Step 2: Click Add > Network Object.

Step 3: On the Add Network Object dialog box, in the **Name** box, enter a description of the WLC. (Examples: internal-wlc-5508, internal-wlc-flex-7500)

Step 4: In the Type list, choose Host.

Step 5: In the IP Address box, enter the WLC's management interface IP address, and then click OK. (Example: 10.4.46.64, 10.4.46.68)

둴 Edit Network	k Object	×
Name:	internal-wlc-5508	
Туре:	Host	•
IP Version:	IPv4	
IP Address:	10.4.46.64	
Description:	Internal 5508 WLC	
NAT		×
INAL		~
	OK Cancel Help	

Step 6: Repeat Step 2 through Step 5 for every WLC inside your organization.

📴 Edit Network	: Object
Name:	internal-wlc-flex-7500
Туре:	Host
IP Version:	
IP Address:	10.4.46.68
Description:	Internal FlexConnect 7500 WLC
NAT	*
	OK Cancel Help

Next, to simplify security policy configuration, you create a network object group that contains every WLC inside your organization.

Step 7: Click Add > Network Object Group.

Step 8: In the Add Network Object Group dialog box, in the **Group Name** box, enter a name for the group. (Example: internal-wlc-group)

🔂 Add Netw	vork Object Group							×
Group Name:	: internal-wlc-group							
Description:	n: Internal Wireless LAN Controllers							
Existing N	Network Objects/Groups:					Members in Group:		
Name	A 1	IP Address	Netmask			Name	IP Address	NetmaskPrefix Lenç
	dmz-dmvpn-2	192.168.18.11				💳 🖪 internal-wlc-flex-7500	10.4.46.68	
	dmz-guest-network-ISPa	192.168.28.0	255.255.252.0			🖵 🖳 internal-wlc-5508	10.4.46.64	
	dmz-ipv6-natpool	192.168.16.32-192						
	dmz-networks	192.168.16.0	255.255.248.0					
- 3	dmz-web-net-v6	2001:db8:a:1::	64					
	dmz-webserver-ISPa	192.168.16.100						
- 8	dmz-webserver-ispa-v6	192.168.16.111						
	dmz-webserver-ISPb	192.168.16.100						
	🛃 internal-network	10.4.0.0	255.254.0.0					
3	🛃 internal-network-ISPa	10.4.0.0	255.254.0.0					
3	🛃 internal-network-ISPb	10.4.0.0	255.254.0.0					
	oustide-webserver-isp	2001:db8:a::111		=				
🔙	🖪 outside-dmvpn-ISPa	172.16.130.1		-	Add >>			
- 8	🗓 outside-dmvpn-ISPb	172.17.130.1			<< Demove			
	🛃 outside-IPv6-all	::	0		<< Remove			
8	🖪 outside-webserver-ISPa	172.16.130.100						
	dutside-webserver-ISPb	172.17.130.100		Ŧ				
•	m		Þ					
🔘 Create ne	iew Network Object member	:						
Name: (o	optional)							
Type:	Host			•				
IP Version	o: @ IPv4 @ IPv6							
1 101010								
IP Addres	55:							
								•
			ОК		Cancel	Help		

Step 9: In the Existing Network Objects/Groups pane, select every internal WLC, click Add, and then click OK.

Next, you create a network object group that contains the private DMZ address of every WLC in the DMZ. (Example: 192.168.19.54)

Step 10: Click Add > Network Object Group.

cription:	Wireless LAN Controlle	rs in the DMZ						
Existing N	letwork Objects/Groups					Members in Group:		
ame	~1	IP Address	Netmask			Name	IP Address	NetmaskPrefix Le
- 🚜 e	Imz-wlc-network	192.168.19.0	255.255.255.0			- 🖳 dmz-wlc-5508	192.168.19.54	
ir 🚅 ir	nside-network	10.4.24.0	255.255.255.224			- 🔜 dmz-wlc-2504-1	192.168.19.56	
- <u>1</u>	outside-16-network	172.16.130.0	255.255.255.0			🛏 🖳 dmz-wlc-2504-2	192.168.19.57	
- 1	outside-16-network6	2001:db8:a::	64					
- 🚅 e	outside-17-network	172.17.130.0	255.255.255.0					
- 🖪 d	lmz-dmvpn-1	192.168.18.10						
- 🖪 d	Imz-dmvpn-2	192.168.18.11						
- 🚜 d	lmz-guest-network-ISPa	192.168.28.0	255.255.252.0					
- 📑 d	lmz-ipv6-natpool	192.168.16.32-192		Ε				
- 👼 d	Imz-networks	192.168.16.0	255.255.248.0					
- 👼 dmz-web-net-v6 🖳 dmz-webserver-ISPa 🖳 dmz-webserver-Ispa-v6		2001:db8:a:1::	64		Add >>			
		192.168.16.100						
		192.168.16.111						
- 🖪 d	mz-webserver-ISPb	192.168.16.100						
ir 🔊	nternal-network	10.4.0.0	255.254.0.0		<< Remove			
- 🛃 ir	nternal-network-ISPa	10.4.0.0	255.254.0.0					
- 🥵 ir	nternal-network-ISPb	10.4.0.0	255.254.0.0	-				
	· · ·		•					
- <u> </u>		h		-				
Create ne	ew Network Object mem	Der:						
Name: (o	ptional)							
Гуре:	Host			•				
IP Versior	n: 🔘 IPv4 🦳 I	Pv6						
IP Addres	55:							
						•	"	

Step 11: In the Add Network Object Group dialog box, in the **Group Name** box, enter a name for the group. (Example: dmz-wlc-group)

Step 12: In the Existing Network Objects/Groups pane, choose the primary WLC, and then click **Add**. (Example: 192.168.19.54). If you are using the 5508 as the anchor controller, only the IP address of the primary WLC needs to be configured because this WLC model supports AP-SSO and the redundant pair uses a single IP address.

Step 13: If using a 2504 as a guest anchor controller, both the primary and resilient WLC IP addresses are necessary because this WLC does not support AP-SSO. In the Existing Network Objects/Groups pane, choose the resilient WLC, click **Add**, and then click **OK**. (Example: 192.168.19.56). You will also add the IP address of the secondary WLC's (Example: 192.168.19.57)

When in standby mode and using AP-SSO, the resilient Wireless LAN Controller uses the redundancy port to communicate with the NTP server. Since either of the WLCs in AP-SSO mode could be in standby, we need to create a network object that is used to identify each of the redundancy ports.

Step 14: Create a Network Object for each of the WLCs in the DMZ (Example: 192.168.19.54) by clicking Add > Network Object.

Step 15: In the Add Network Object dialog box, in the Name box, enter a description of the WLC. (Example: dmz-wlc-primary-5508-RP)

Step 16: In the Type list, choose Host.

Step 17: In the IP Address box, enter the primary WLC's redundancy-port interface IP address, and then click OK. (Example: 192.168.19.154)

🚰 Add Networl	k Object	×
Name:	dmz-wlc-primary-5508-RP	
Туре:	Host	•
IP Version:	IPv4 O IPv6	
IP Address:	192.168.19.154	
Description:	Primary WLC Redundancy Port	
ΝΔΤ		*
		Ť
	OK Cancel Help	

Step 18: Repeat the steps in Procedure 4 for the resilient controller's redundancy port. (Example 192.168.19.155)

💁 Add Networ	k Object 🗾	
Name:	Imz-wlc-resilient-5508-RP	
Туре:	Host	
IP Version:	IPv4 O IPv6	
IP Address:	192.168.19.155	
Description:	Resilient WLC Redundancy Port	
NAT	*	
	OK Cancel Help	

Step 19: Create a Network Object Group to group the two redundancy ports on the WLCs.

up Name:	dmz-wlc-RP-group							
cription:	DMZ Wireless LAN Contro	ollers Redundancy Port G	oup					
Existing f	Network Objects/Groups:					Members in Group:		
Name	^1	IP Address	Netmask			Name	IP Address	NetmaskPrefix
	autside-16-network	172.16.130.0	255.255.255.0			🚽 🖳 dmz-wlc-primary-5508-RP	192.168.19.154	
	dutside-16-network6	2001:db8:a::	64			🖵 🖳 dmz-wlc-resilient-5508-RP	192.168.19.155	
	autside-17-network	172.17.130.0	255.255.255.0					
5	dmz-dmvpn-1	192.168.18.10						
🦉	🗓 dmz-dmvpn-2	192.168.18.11		_				
	🖶 dmz-guest-network-ISPa	192.168.28.0	255.255.252.0					
	e dmz-ipv6-natpool	192.168.16.32-192						
	dmz-networks	192.168.16.0	255.255.248.0	E				
	🛱 dmz-web-net-v6	2001:db8:a:1::	64					
[dmz-webserver-ISPa	192.168.16.100						
[dmz-webserver-ispa-v6	192.168.16.111		Add >>				
🦉	dmz-webserver-ISPb	192.168.16.100						
8	🖪 dmz-wlc-2504-1	192.168.19.56			Add >>			
8	📱 dmz-wlc-2504-2	192.168.19.57						
3	🗓 dmz-wlc-5508	192.168.19.54			<< Remove			
5	🗓 internal-aaa	10.4.48.15						
2	🗓 internal-dhcp	10.4.48.10		-				
•	III		+					
Create n	ew Network Object membe	r:						
Name: (o	ptional)							
Type:	Host			•				
IP Versio	n: 💿 IPv4 🔘 IPv	6						
IP Addre:	ss:							
						•		

Step 20: In the Add Network Object Group dialog box, click OK.

Procedure 5 Configure WLC 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 Insert Access Rule dialog box, in the Interface list, choose Any.

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

Step 6: In the **Source** list, choose the network object group created in Step 8, "Create network objects." (Example: wlc-group)

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

August 2013

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

💁 Add Access I	Rule	×
Interface:	Any 👻	
Action: 💿 Pern	nit 💿 Deny	
Source Criteria		
Source:	dmz-wlc-group	
User:		
Security Group:		
Destination Crite		_
Destination:	internal-aaa 💮	
Security Group:		
Service:	tcp/tacacs, udp/1812, udp/1813 -	
Description:	Allow DMZ based WLC's to communicate with the AAA/ACS Server on the internal network.	
🔽 Enable Logg	ing	
Logging Leve	el: Default 👻	
More Options		×
	OK Cancel Help	

Next, you must allow 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, choose Any.

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

Step 12: In the **Source** list, choose the network object group created in Step 11 of Step 13, "Create network objects." (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.
------	-----	----	-----	---------	-------	-------	----------	-----	------	-------	-----

📴 Edit Access F	Rule	
Interface:	Any	
Action: 💿 Perr	nič 🔘 Deny	
Source Criteria		-
Source:	dmz-wlc-group	
User:		
Security Group:		
Destination Crite	aria	-
Destination:	internal-ntp	
Security Group:		
Service:	udp/ntp ····	
Description:	Allow WLC's to communicate with the NTP server locate din the data center.	
📝 Enable Logg	ing	
Logging Leve	el: Default 🗸	
More Options	*	
	OK Cancel Help	

Next, you allow 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, choose Any.

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

Step 18: In the **Source** list, choose the network object group created in Step 11 of Step 13, "Create network objects." (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: 💿 Pern	nit 💿 Deny
Source Criteria	
Source:	dmz-wlc-group
User:	
Security Group:	
Destination Crite	ria
Destination:	any
Security Group:	
Service:	tcp/ftp, tcp/ftp-data
Description:	Allow the WLC's to communicate with any FTP server.
🚺 Enable Loggi	ing
Logging Leve	el: Default 🗸
More Options	*
	OK Cancel Help

Next, you enable the DMZ guest WLC to communicate with the WLCs inside the organization.

Step 20: Click Add > Insert.

Step 21: In the Interface list, choose Any.

Step 22: In the **Source** list, choose the network object group created in Step 11 of Step 13, "Create network objects." (Example: dmz-wlc-group)

Step 23: In the **Destination** list, choose the network object group created in Step 8 of Step 13, "Create network objects." (Example: internal-wlc-group)

Step 24: In the Service list, enter udp/16666, udp/5246, udp/5247, 97, and then click OK.

🚰 Add Access F	Rule
Interface:	Any 👻
Action: 💿 Pern	nit 💿 Deny
Source Criteria	
Source:	dmz-wlc-group
User:	
Security Group:	
Destination Crite	eria
Destination:	internal-wic-group
Security Group:	
Service:	udp/16666, udp/5246, udp/5247, 97
Description:	Allow DMZ based WLC's to communicate with the internal WLC's
📝 Enable Loggi	ing
Logging Leve	el: Default 🗸
More Options	*
	OK Cancel Help

Next, you enable the guest WLC to communicate with the DHCP server inside your organization.

Step 25: Click Add > Insert.

Step 26: In the Interface list, choose Any.

Step 27: In the **Source** list, choose the network object group created in Step 11 of Step 13, "Create network objects." (Example: dmz-wlc-group)

Step 28: In the **Destination** list, choose the network object group for the internal DHCP server. (Example: internal-dhcp)

Step 29: In the Service list, enter udp/bootps, click OK, and then click Apply.

📴 Edit Access F	tule
Interface:	Any
Action: 🧿 Pern	nit 🔘 Deny
Source Criteria	
Source:	dmz-wic-group 💮
User:	
Security Group:	
Destination Crite	ria
Destination:	internal-dhcp
Security Group:	
Service:	udp/bootps
Description:	Allow DMZ WLC's to obtain IP address via internal DHCP server
📝 Enable Loggi	ing
Logging Leve	el: Default 🗸
More Options	*
	OK Cancel Help

Finally, enable the guest WLC configured for AP-SSO (5500 series) in order to communicate with the internal NTP server using its redundancy port.

Step 30: Click Add > Insert.

Step 31: In the Interface list, choose Any.

Step 32: In the Source list, choose network group that was created for the WLC RP ports (Example: dmz-wlc-RP-group)

Step 33: In the Destination list, choose the network object group for the internal NTP server. (Example: internal-ntp)

Step 34: In the Service list, enter udp/ntp, click OK, and then click Apply.

📴 Edit Access R	tule	×
Interface:	Any	
Action: 💿 Perm	nit 🔘 Deny	
Source Criteria -		_
Source:	Imz-wic-RP-group	
User:		
Security Group:		
Destination Crite	ria	-
Destination:	internal-ntp	
Security Group:		
Service:	udp/ntp 💮	
Description:	Allow Standby AP-SSO WLC's to communicate to internal NTP server using RP Port	
🔽 Enable Loggi	ing	
Logging Leve	el: Default 👻	
More Options	¥	
	OK Cancel Help	

Procedure 6 Configure guest network security policy

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

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

First, you configure an access rule in the firewall in order to enable the guest wireless users to communicate with the internal DNS and DHCP servers in the data center.

IP iD

😣 Deny

Step 3: Click Add > Insert.

24 🔽 📑 dmz-networks

Step 4: In the Interface list, choose Any.

Step 5: In the **Source** list, select the network object automatically created for the guest DMZ. (Example: dmz-guests-network/22)

Step 6: In the Destination list, choose the network object for the DNS server. (Example: internal-dns)

August 2013

Step 7: In the Service list, enter udp/domain, tcp/domain, and then click OK.

📴 Insert Access	Rule
Interface:	Any 🗸
Action: 💿 Pern	nit 💿 Deny
Source Criteria	
Source:	dmz-guests-network/22
User:	
Security Group:	
Destination Crite	ria
Destination:	internal-dns
Security Group:	
Service:	udp/domain, tcp/domain
Description:	Allow Guest Wireless users to resolve DNS names.
🔽 Enable Logg	ing
Logging Leve	el: Default 🗸
More Options	*
	OK Cancel Help

Step 8: Click Add > Insert.

Step 9: In the Interface list, choose Any.

Step 10: In the **Source** list, choose the network object automatically created for the guest DMZ. (Example: dmz-guests-network/22)

Step 11: In the Destination list, choose the network object for the DHCP server. (Example: internal-dhcp)

Step 12: In the Service list, enter udp/bootps, and then click OK.

📴 Insert Access	Rule
Interface:	Any 🔹
Action: 💿 Pern	nit 💿 Deny
Source Criteria	
Source:	dmz-guests-network/22
User:	
Security Group:	
Destination Crite	ria
Destination:	internal-dhcp
Security Group:	
Service:	udp/bootps
Description:	Allow wireless guest users to obtain an IP address from the internal DHCP server
🔽 Enable Loggi	ing
Logging Leve	el: Default 🔹
More Options	*
	OK Cancel Help

Next, you enable the guests to communicate with the web servers in the DMZ.

Step 13: Click Add > Insert.

Step 14: In the Interface list, choose Any.

Step 15: In the **Source** list, choose the network object automatically created for the guest DMZ. (Example: dmz-guests-network/22)

Step 16: In the **Destination** list, choose the network object automatically created for the web DMZ. (Example: dmz-web-network/24)

Step 17: In the Service list, enter tcp/http, tcp/https, and then click OK.

📴 Insert Access	s Rule	×
Interface:	Any 👻	
Action: 💿 Pern	nit 💿 Deny	
Source Criteria		
Source:	dmz-guests-network/22	
User:		
Security Group:		
Destination Crite	eria	_
Destination:	dmz-web-network/24	
Security Group:		
Service:	tcp/http, tcp/https	
Description:	All wireless guest users access to DMZ based webservers, possibly for walled garden access	
🔽 Enable Loggi	ing	
Logging Leve	el: Default 👻	
More Options		*
	OK Cancel Help	

Next, you remove the guests' ability communicate with other internal and DMZ devices.

Step 18: Click Add > Insert.

Step 19: In the Interface list, choose Any.

Step 20: To the right of Action, select Deny.

Step 21: In the **Source** list, choose the network object automatically created for the guest DMZ. (Example: dmz-guests-network/22)

Step 22: In the **Destination** list, choose the network objects for the internal and DMZ networks, and then click **OK**. (Example: internal-network, dmz-networks)

둴 Edit Access F	kule 💌
Interface:	Any
Action: 🔘 Perr	nit 💿 Deny
Source Criteria	
Source:	dmz-guests-network/22 .
User:	
Security Group:	
Destination Crite	xia
Destination:	dmz-networks, internal-network
Security Group:	
Service:	ip
Description:	Deny traffic from the wireless guest network to the internal and dmz resources
🔽 Enable Logg	ing
Logging Leve	el: Default 🗸
More Options	*
	OK Cancel Help

Next, you enable the guests to communicate with the Internet.

Step 23: Click Add > Insert.

Step 24: In the Interface list, choose Any.

Step 25: In the **Source** list, choose the network object automatically created for the guest DMZ, click **OK**, and then click **Apply**. (Example: dmz-guests-network/22)

insert Access	Rule
Interface:	Any 🔻
Action: 🧿 Perr	nit 💿 Deny
Source Criteria	
Source:	dmz-guests-network/22
User:	
Security Group:	
Destination Crite	ria
Destination:	any
Security Group:	
Service:	ip
Description:	Allow Wireless DMZ users access to the internet
📝 Enable Logg	ing
Logging Leve	al: Default 🗸
More Options	*
	OK Cancel Help

Configure the DMZ wireless LAN controller by using the following values.

Deremeter	CVD values	CVD values resilient controller not	Site enecifie voluce		
Controller parameters	primary controller	using AP 550	Site-specific values		
Switch interface number	1/0/13 2/0/13	1/0/14 2/0/14			
	1110	1119			
	PST -8 0	PST -8 0			
IP address	192 168 19 54/24	102 168 10 55/2/1			
Default gateway	192.168.19.1	192.168.19.1			
Redundant management IP address (AP SSO)	192.168.19.154	192.168.19.155			
Redundancy port connectivity (AP SSO)	Dedicated Ethernet cable	Dedicated Ethernet cable			
Hostname	DMZ-WLC-Guest-1	DMZ-WLC-Guest-2 ²			
Local administra- tor username and password	admin/C1sco123	admin/C1sco123			
Mobility group name	GUEST	GUEST			
RADIUS server IP address	10.4.48.15	10.4.48.15			
RADIUS shared key	SecretKey	SecretKey			
Management network (optional)	10.4.48.0/24	10.4.48.0/24			
TACACS server IP address (optional)	10.4.48.15	10.4.48.15			
TACACS shared key (optional)	SecretKey	SecretKey			
Wireless data network parameters					
SSID	Wireless-Guest	Wireless-Guest			
VLAN number	1128	1128			
Default gateway	192.168.28.1	192.168.28.1			
Controller interface IP address	192.168.28.5	192.168.28.6 ¹			

Table 9 - Cisco DMZ wireless	controller parameters	checklist
------------------------------	-----------------------	-----------

Notes:

- If you're using AP SSO high availability, the IP address of the resilient WLC not required, as the secondary controller's management interface is offline until the primary fails. During this time, the IP address of the RP (Example: 192.168.19.155) is used for outbound communication to the NTP server and to monitor the status of its default gateway.
- 2. If using AP SSO, the resilient standby controller does not have a unique hostname, as it inherits the continuation of its paired primary WLC.

August 2013

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

Step 1: Terminate the autoinstall process.

Would you like to terminate autoinstall? [yes]: YES

Step 2: Enter a system name. (Example: GUEST-1)

System Name [Cisco 7e:8e:43] (31 characters max): DMZ-WLC-Guest

Step 3: 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 4: Use DHCP for the service port interface address.

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

Step 5: Enable the management interface. If you are deploying a Cisco 5500 or 2500 Series Wireless LAN Controller, configure at least two interfaces as an EtherChannel trunk.

```
Enable Link Aggregation (LAG) [yes][NO]: YES
Management Interface IP Address: 192.168.19.54
Management Interface Netmask: 255.255.0
Management interface Default Router: 192.168.19.1
Management Interface VLAN Identifier (0 = untagged): 1119
```

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 and you want to enable AP SSO, enable high availability.

Enable HA [yes][NO]: YES
Configure HA Unit [Primary][secondary]: < Primary or Secondary>
Redundancy Management IP Address: 192.168.19.154
Peer Redundancy Management IP Address: 192.168.19.155

Step 8: The virtual interface is used by the WLC for mobility DHCP relay and intercontroller communication. Enter an IP address that is not used in your organization's network. (Example: 192.0.2.1)

Virtual Gateway IP Address: 192.0.2.1



Step 9: If configuring a Cisco 2500 Series WLC, enter the multicast IP address for communication of multicast traffic by using the multicast-multicast method. This WLC does not support multicast using the multicast-unicast method.

Multicast IP Address: 239.40.40.40

Step 10: Enter a name for the default mobility and RF group. (Example: GUEST)

Mobility/RF Group Name: GUEST

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

Network Name (SSID): Guest Configure DHCP Bridging Mode [yes][NO]: NO

Step 12: Enable DHCP snooping.

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

- Step 13: Do not configure the RADIUS server now. You will configure the RADIUS server later by 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 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 enter **NO**, the system restarts without saving the configuration, and you 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 by using the credentials defined in Step 3. (Example: https://dmz-wlc-guest.cisco.local/)

Procedure 8 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.

ahaha									i <u>P</u> ing Logout <u>R</u> efresh
cisco	MONITOR	<u>W</u> LANs		WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK
Commands	Set Time						Set	Date and	Time Set Timezone
Download File Upload File	Current T	ime	Tue May 31 11:07	:38 2011					
Config Boot	Date							_	
Scheduled Reboot			Month		May	•			
Reset to Factory Default			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 Cana	ada) 🔹	·	
	Foot Note	5							
	1. Automatic	ally sets d	aylight savings tim	e where used.					

Procedure 9 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.

ahaha							Sa <u>v</u> e Co	nfiguratio	n <u>P</u> ing Lo	gout <u>R</u> efresh
cisco	MONITOR	<u>W</u> LANs		WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK	
Management	SNMP v1	/ v2c Co	ommunity > N	ew					< Back	Apply
Summary SNMP General SNMP V3 Users Communities Trap Receivers Trap Controls Trap Logs	Communi IP Addres IP Mask Access Mo Status	ty Name is ode	cisco 10.4.48.0 255.255.255.0 Read Only v Enable v							
Telnet-SSH Serial Port Local Management Users										
User Sessions Logs Mgmt Via Wireless Software Activation Tech Support										

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	nfiguratio	n <u>P</u> ing L	.ogout <u>R</u> efresh
cisco	MONITOR	<u>W</u> LANs		WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK	
CISCO Management Summary SNMP General SNMP V3 Users Computities	SNMP v1 Communi IP Addres IP Mask	<u>WLANS</u> / v2c Cc ty Name is	cisco123 10.4.48.0 255.255.255.0	ew		MANAGEMENT	COMMANDS		Seck	Apply
Trap Receivers Trap Controls Trap Logs	Access Mo Status	ode	Read/Write 👻							
HTTP-HTTPS										
Telnet-SSH										
Serial Port										
Local Management Users										
User Sessions										
Logs										
Mgmt Via Wireless										
Software Activation										
Tech Support										

Step 12: Navigate to Management > SNMP > Communities.

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

Step 13: On the "Are you sure you want to delete?" message, click OK.

Step 14: Repeat Step 12 and Step 13 for the private community.

								Sa <u>v</u> e Cor	nfiguration	n <u>P</u> ing	Logout <u>R</u> efresh
cisco	MONITOR	<u>W</u> LANs		WIRELESS	SECURITY	MANAG	EMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBA	ск
Management	SNMP v1 /	v2c Co	ommunity								New
Summary											
▼ SNMP	Community	Name		IP Address	IP Mask	/	Access M	ode Status			
General	cisco			10.4.48.0	255.255.2	55.0 F	Read-Only	Enable			
SNMP V3 Users	cisco123			10.4.48.0	255.255.2	55.0 F	Read-Writ	e Enable			
Trap Receivers											
Trap Controls											
ITAP LOGS											
HTTP-HTTPS											
Teinet-SSH											
Serial Port											
Local Management Users											
User Sessions											
Logs											
Mgmt Via Wireless											
Software Activation											
Tech Support											

Procedure 10 Limit which networks can manage the WLC

(Optional)

In networks where network operational support is centralized, you can increase network security by using an access control list in order to limit the networks that can access your controller. In this example, only devices on the 10.4.48.0/24 network are able to access the device via SSH or SNMP.

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

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

Step 3: In the list, choose the name of the access control 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 L	ogout <u>R</u> efresh
cisco	MONITOR	<u>W</u> LANs		WIRELESS	SECURITY	MANAGEMEN	COMMANDS	HELP	<u>F</u> EEDBACK	
Security	Access C	ontrol L	ists > Rules >	New					< Back	Apply
 AAA Local EAP 	Sequence		1 IP Address]	IP Addr 10.4.4	ess 8.0	Netmask 255.255.255.0	_		
 Priority Order Certificate 	Destination		Any	•						
 Access Control Lists Access Control Lists CPU Access Control Lists 	Protocol		ТСР	•						
FlexConnect ACLs Wireless Protection Policies	Destination P	Port	HTTPS	•						
▶ Web Auth	DSCP		Any	•						
TrustSec SXP Advanced	Direction		Any	·						
	Action		Permit	·						

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

Table 10 - 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	TCP	HTTPS	Deny
4	Any	Any	ТСР	Other/22	Deny
5	Any	Any	Any	Any	Permit

DMZ-WLC-Guest -	8 10 54 /r	croops (fran	agent html										-	Cartificate Em	
Favorites CMZ-WLC-	Guest													. Conneste Ent	a [4] A]
uluili. cisco	MONI	tor <u>w</u>	LANS <u>C</u> ONT	ROLLER	WIRELESS	SECU	IRITY MANA	GEMENT	C <u>O</u> MMANDS	HELP	EEEDB	Sa <u>v</u> e Conf ACK	iguration	Ping Logout	<u>R</u> efresh
Security	Acce	ess Con	trol Lists > I	Edit								< Back	<	Add New Rule	
AAA General RADIUS Authentication Accounting Fallback TACACS+ IDAP	Gene Acces Deny	e ral s List Nam Counters	e SBA 0	-DMZ-AC	_										
Local Net Users MAC Filtering	Seq	Action	Source IP/N	lask	Destination IP/Mask		Protocol	Source Port	Dest Port		DSCP	Direction	Number of Hits		
Disabled Clients User Login Policies	1	Permit	10.4.48.0 255.255.255.	, /	0.0.0.0	/	TCP	Any	HTTP	\$	Any	Any	0		
AP Policies Password Policies	_2	Permit	10.4.48.0 255.255.255.	, /	0.0.0.0	/	тср	Any	22		Any	Any	0		
 Local EAP Priority Order 	_3	Deny	0.0.0.0	/	0.0.0.0	/	тср	Any	HTTP	5	Any	Any	0		
Certificate Access Control Lists	4	Deny	0.0.0.0	/	0.0.0.0	/	тср	Any	22		Any	Any	0		
Wireless Protection Policies	_5	Permit	0.0.0.0	/	0.0.0.0	/	Any	Any	Any		Any	Any	0	۵	
 Web Auth TrustSec SXP Advanced 															

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 just created, and then click Apply.

Procedure 11 Configure management authentication

(Optional)

You can use this procedure to deploy centralized management authentication by configuring an authentication, authorization and accounting (AAA) service. If you prefer to use local management authentication, skip to Procedure 12.

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, it controls all management access to the network infrastructure devices (SSH and HTTPS).

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)

սիսիս						Sa <u>v</u> e Co	nfiguration	n <u>P</u> ing	Logout <u>R</u> efresh
CISCO	MONITOR WLAN	s <u>C</u> ONTROLLER	WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	FEEDBAC	к
Security	TACACS+ Auth	entication Serv	ers > New					< Back	Apply
 AAA General ADUS Characs+ Authentication Accounting Authentication LDAP Local Net Users MAC Filtering Disabled Clients User Login Policies Password Policies Local EAP Priority Order Certificate Access Control Lists Wireless Protection Policies Web Auth TrustSec SXP Advanced 	Server Index (Pric Server IP Address Shared Secret For Shared Secret Confirm Shared S Port Number Server Status Server Timeout	vrity) mat ecret	1 • 10.4.48.15 ASCII • 49 Enabled • 5 second	ds					

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										.ogout <u>R</u> efresh
cisco	MONITOR	WLANs		WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	FEEDBACK	
Security AAA General RADIUS TACACS+ Authentication Accounting Authorization LDAP	Server In Server In Server IP Shared Se Shared Se Confirm S	Accourt dex (Priorit: Address ecret Forma ecret shared Secr	y) 1 • 10.4 ht ASC et ••••	S > New .48.15 II ▼]		4	: Back	Apply
Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies Password Policies	Port Numl Server Sta Server Tir	ber atus meout	49 Enat	seconds						
Local EAP										
Priority Order										
Certificate										
Access Control Lists										
 Wireless Protection Policies 										
Web Auth										
TrustSec SXP										
Advanced										

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)

սիսիս						Sa <u>v</u> e Cor	nfiguration <u>P</u> ing	Logout <u>R</u> efresh
cisco	MONITOR WLAN	Is <u>C</u> ONTROLLER	WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP FEEDB	ACK
Security	TACACS+ Aut	orization Serve	rs > New				< Back	Apply
 AAA General RADIUS TACACS+ Authentication Accounting Authentication Accounting Authentication IDAP Local Ket Users NAC Filtering Disabled Clients User Login Policies Priority Order Certificate Access Control Lists Wireless Protection Policies Web Auth TrustSec SXP Advanced 	Server Index (Pri Server IP Addres Shared Secret Fo Shared Secret Confirm Shared S Port Number Server Status Server Timeout	ority) ; mmat eoret	1 • 10.4.48.15 ASCII • 49 5 second	da				

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: Use the arrow buttons to move RADIUS to the Not Used list, and then click Apply.

cisco	MONITOR	WLANs		WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	EEEDBACK	
Security	Priority C	Order > N	lanagement L	Jser					l	Apply
AAALocal EAP	Authentic	ation								
 Priority Order Management User 	Not	Used		Order U	sed for Authe	ntication				
Certificate	RADIU	JS ^	>		TACACS+	Up				
Access Control Lists Wireless Protection Policies		v				Down				
Web Auth	If LOCAL is	elected as	second priority the	en user will be	authenticated a	gainst				
TrustSec SXP Advanced	LUCAL ONLY	it first prior	ity is unreachable.							

Tech Tip If using Cisco Secure ACS in order to authenticate TACACS management access to the WLC, you must add the WLC as an authorized network access device. Failure to do so will prevent administrative access to the WLC by using the Secure ACS server.

Procedure 12 Create the guest wireless LAN interface

The guest wireless interface is connected to the DMZ of the Cisco ASA 5540 security appliance. This allows guest wireless traffic only to and from the Internet. All guest traffic, regardless of the controller to which the guest initially connects, is tunneled to the guest WLC and leaves the controller on this interface.

To easily identify the guest wireless devices on the network, use an IP address range for these clients that is not part of your organization's regular network. This procedure adds an interface that allows devices on the guest wireless network to communicate with the Internet.

Step 1: In Controller>Interfaces, click New.

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

Step 3: Enter the VLAN Id, and then click Apply. (Example: 1128)

										ogout <u>R</u> efresh
CISCO	MONITOR	<u>W</u> LANs	<u>C</u> ONTROLLER	WIRELESS	<u>S</u> ECURITY	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HELP	EEEDBACK	:
Controller	Interfaces	s > New						<	Back	Apply
General	Interface	Name	Wireless-Guest							
Interfaces	VLAN Id		1128							
Interface Groups										
Multicast Network Routes										
Redundancy										
Internal DHCP Server										
Mobility Management Ports										
▶ NTP										
▶ CDP										
PMIPv6										
▶ mDNS										
Advanced										

Step 4: In the IP Address box, enter the IP address to assign to the WLC interface. (Example: 192.168.28.5)

Step 5: Enter the Netmask. (Example: 255.255.252.0)

Step 6: In the **Gateway** box, enter the IP address of the firewall's DMZ interface defined in Procedure 2. (Example: 192.168.28.1)

Step 7: In the Primary DHCP Server, enter the IP address of your organization's DHCP server, and then click Apply. (Example: 10.4.48.10)

սիսիս								Logout <u>R</u> efresh
cisco	MONITOR WLANS CO	ONTROLLER WIRELE	SS <u>S</u> ECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	EEEDBACK	
Controller	Interfaces > Edit						< Back	Apply
Controller General Inventory Interfaces Interface Groups Multicast Network Routes Redundancy Internal DHCP Server Molility Management Ports	Interfaces > Edit General Information Interface Name MAC Address Configuration Guest Lan Quarantine Quarantine Vian Id NAS-ID	wireless-guest 88:43:e1:7e:0a:6 0 DM2-WLC-Guest					< Back	Apply ^
Ports NTP CDP PMIPv6 IPv6 mDNS Advanced	Enable DHCP Option 82 Physical Information The interface is attached Enable Dynamic AP Management Interface Address VLAN Identifier IP Address Netmask Gateway DHCP Information Primary DHCP Server Secondary DHCP Server	to a LAG.						



Procedure 13 Configure the guest wireless LAN

Step 1: Navigate to WLANs.

Step 2: Hover over the blue list next to your guest WLAN, and then click Mobility Anchors.

Step 3: In the Switch IP Address (Anchor) list, choose (local).

Step 4: Click Mobility Anchor Create, and then click OK.

11 111 11			Save Configuration Ping Logout	Refresh
cisco	MONITOR WLANS CONTROLLER WIREL	ESS SECURITY MANAGEMENT	COMMANDS HELP FEEDBACK	
WLANs	Mobility Anchors		< Bac	:k
WLANS	WLAN SSID Guest			
Advanced	Switch IP Address (Anchor)	Data Path	Control Path	
	Mobility Anchor Create			
	Switch IP Address (Anchor)	local) 👻		

Step 5: Click Back.

Step 6: Click the WLAN ID of the SSID created in Procedure 7. (Example: Guest)

Step 7: On the General tab, in the **Interface/Interface Group(G)** list, choose the interface created in Procedure 12. (Example: wireless-guest)

սիսիս	Sa <u>v</u> e Configuration <u>P</u> ing Logout <u>R</u> efrest
CISCO	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
WLANs	WLANs > Edit 'Guest' < Back Apply
▼ WLANs	
WLANs	General Security Qos Advanced
Advanced	Profile Name Guest
	Type WLAN
	SSID Guest
	Status 🗹 Enabled
	Security Policies [WPA2][Auth(802.1X)]
	(Modifications done under security tab will appear after applying the changes.)
	Radio Policy
	Interface
	Group(G) wireless-guest
	Multicast Vlan Feature
	Broadcast SSID 😢 Enabled
	Foot Notes
	2 Web Policy cannot be used in combination with 1Psec 2 H-REAP Local Switching is not supported with IPsec, CRANITE authentication
	3 When client exclusion is enabled, a Timeout Value of zero means infinity (will require administrative override to reset excluded clients) 4 Client MFP is not active unless WPA2 is configured
	5 Learn Client IP is configurable only when HREAP Local Switching is enabled 6 WMM and open or AES security should be enabled to support higher 11n rates
	7 Multicast Should Be Enabled For IPV6. 8 Band Select is configurable only when Radio Policy is set to 'All'.
	9 Value zero implies there is no restriction on maximum clients allowed. 10 MCC Filtering is not supported with HERAE local authentication.
	11 MAC Filtering should be enabled.
	12 Guest tunneing, Local switching, Unit'r Requirea snouia be aisaoled. 13 Max-associated-clients feature is not supported with HREAP Local Authentication.

Step 8: Click the Security tab, and then on the Layer 2 tab, in the Layer 2 Security list, choose None.

				Sa <u>v</u> e Configuration	<u>P</u> ing Logout <u>R</u> efresh
CISCO	MONITOR WLANS COM	ITROLLER WIRELESS	SECURITY MANAGEMENT	COMMANDS HELP	<u>F</u> EEDBACK
WLANS	WLANs > Edit 'Gues	r.		<	Back Apply
WLANs	General Security	QoS Advanced			
Advanced	Layer 2 Layer 3	AAA Servers			
	Layer 2 Security 🦉 T	ione ΦΑΑC Filtering			
	Foot Notes 1 Web Policy cannot be us 2 H-REAP local Switching 3 When client exclusion is 4 Client MPIs not active 5 Learn Client IP is conflug 6 WMM and open or AES 7 Multicast Should Be Enal 8 Band Select is configured 9 Value zero implies there 10 MAC Filtering is not sup 11 MAC Filtering is not sup 12 Guest tumening, Local 13 Max-associated-clients	ad in combination with IPsec, s not supported with IPsec, enabled, a Timeout Value of rable only when HREAP Loca lead For IPv6. le only when Radio Policy is is no restriction on maximu- enabled. withing, DHCP Required sh feature is not supported with restructs in the supported with	CRANITE authentication zero means infinity (will require il Switching is enabled support higher 11n rates set to 'Mi'. n clients allowed, thentication uid be disabled. HREAP Local Authentication.	administrative override to i	reset excluded clients)



- • • 6 DMZ-WLC-Guest -C v Attps://192.168.19.54/s 🝷 😵 Certificate Error 🍫 👂 🚖 Favorites 🛛 🌈 DMZ-WLC-Guest ululu cisco MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP EEEDBACK WLANs WLANs > Edit 'Guest' < Back Apply WLANS General Security QoS Advanced Advanced Layer 2 Layer 3 AAA Servers Layer 3 Security None 👻 👿 Web Policy 🛓 Authentication Passthrough Conditional Web Redirect Splash Page Web Redirect On MAC Filter failure¹⁰ IPv4 None ▼ IPv6 None ▼ WebAuth FlexAcl None ▼ Preauthentication ACL Over-ride Global Config 🛛 Enable
 Foot Notes

 1 Web Policy cannot be used in combination with IPsec.
 CRANTE asthemicisticn, Override Interface ACLS

 2 Miniconnect Local Switching is not supported with IPsec.
 CRANTE asthemicisticn, Override Interface ACLS

 2 Clent MPF is not active unless WAB2 is configured
 Is in an addition with IPsec.

 3 Clent MPF is not active unless WAB2 is configured
 Is in an addition with IPsec.

 4 Clent MPF is not active unless WAB2 is configured
 Is inabled

 5 WMM and open or AES security should be enabled to support higher LII rates

 9 MAC Pilening is not supported functional submentation

 10 MAC Filening is not supported functional submentation

 10 MAC Filening Local submentation

 11 Guest Summaling, Jobe P Required should be disabled.

 12 Guest Summaling, Jobe P Required should be disabled.

 13 WLAH based central withing is not supported with ResConnect Local Authentication.

 13 WLAH based central withing with rest supported with ResConnect Local Authentication.

 14 Enabling Br-andomize will prevent clents from decrypting breadcast and multicast packets.
 Foot Notes

Step 9: On the Layer 3 tab, select Web Policy, and then click OK.

Step 10: On the QoS tab, in the Quality of Service (QoS) list, choose Bronze (background), click Apply, and then click OK.

🏉 DMZ-WLC-Guest -								
🚱 🕞 🗢 🙋 https://192.168	19.54/screens/frameset.html						.	😵 Certificate Error 🏼 😽 🗙
🚖 Favorites 🛛 🏉 DMZ-WLC-0	Guest							
بالبيالي							Sa <u>v</u> e Configuration	<u>Ping</u> Logout <u>R</u> efresh
CISCO	MONITOR WLANS CONT	ROLLER WIRE	LESS <u>S</u> ECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP FEED	васк	
WLANs	WLANs > Edit 'Guest'						< Bac	k Apply
VLANS WLANS	General Security	QoS Advan	iced					
Advanced	Quality of Service (QoS)	Bronze (bac	karound) 🔻					Â
	Application Visibility	🔲 Enabled						
	AVC Profile	none 🔻						
	Netflow Monitor	none 🔻						
	Override Per-User Band	dwidth Contrac	cts (kbps) 🌆					-
		DownStream	UpStream					
	Average Data Rate	0	0					
	Burst Data Rate	0	0					
	Average Real-Time Rate	0	0					
	Burst Real-Time Rate	0	0					E
	Clear							
	Override Per-SSID Ban	dwidth Contra	cts (kbps) 😃					
		DownStream	UpStream					
	Average Data Rate	0	0					
	Burst Data Rate	0	0					
	Foot Notes							
	1 Web Policy cannot be used 2 FlexConnect Local Switchin	l in combination w a is not supported	ith IPsec I with IPsec, CRANITI	authentication. Ov	erride Interface /	ICL5		
	3 When client exclusion is er 4 Client MFP is not active uni	abled, a Timeout less WPA2 is confi	Value of zero means gured	infinity (will require	administrative c	verride to rese	t excluded clients)	
	5 Learn Client IP is configure 6 WMM and open or AES sec	ible only when Fle urity should be en	xConnect Local Switc abled to support hig!	hing is enabled er 11n rates				
	8 Value zero implies there is 9 MAC Filtering is not suppor	no restriction on ted with FlexConn	maximum clients allo ect Local authenticati	wed. on				
	10 MAC Filtering should be e 11 Guest tunneling, Local sw	nabled. itching, DHCP Req	uired should be disal	ved.				
	12 Max-associated-clients fe 13 VLAN based central switc	ature is not suppo hing is not suppor	rtea with FlexConnec ted with FlexConnect	t Local Authentication	on. 7.			_
	Average Real-Time Rate Burst Real-Time Rate Clear Override Per-SSID Banu Average Data Rate Burst Data Rate Burst Data Rate I Wer Check Coll S within 3 Men cleart exclusion for 2 MarcConet Coll S within 3 Men cleart exclusion for 3 Men cleart exclusion for 4 Men cleart exclusion for 5 Marc Rate Men cleart exclusion 6 Men cleart exclusion for 1 Guest funding, Local s in 1 Guest funding and the second seco	0 0 0 0 0 0 0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0 0 0 0 0 0 0	" authentication, Ou finithr (unit require bing is anabled or 11, rates on viet Local Authenticatio Local Authenticatio Cost authentication dicast and multicas	erride Interface ; administrative c 20. 2. pokets.	NCLs verride to rese	excluded clients)	

Procedure 14 Configure mobility groups

If you are not using AP-SSO, then you need to add each of the WLCs to the mobility group.

Step 1: On the guest controller, navigate to Controller > Mobility Management > Mobility Groups.

Step 2: On the Static Mobility Group Member page, note the MAC address, IP address, and mobility group name for the local controller. You need this information for the following steps.

COMZ-WLC-Guest -								
C 🔾 🗢 🖉 https://192.16	8.19.54/screens/frameset.htr	nl					👻 🗟 Certificate E	rror 🍫 🗙
👷 Favorites 🛛 🌈 DMZ-WLC-	Guest							
սիսիս							Sage Configuration Bing Logo	ut <u>B</u> efresh
cisco	MONITOR WLANS		WIRELESS SECURITY	MANAGEMENT	COMMANDS HEL	P <u>F</u> EEDBACK		
Controller	Static Mobility Gro	up Members					New	EditAll
General Inventory	Local Mobility Gro	up GUEST						
Interfaces	MAC Address	IP Address	Group Name	Multicast IP	Hash Key		Status	
Interface Groups	88:43:e1:7e:0a:60	192.168.19.54	GUEST	0.0.0.0	none		Up	
Multicast								
Network Routes								
Redundancy Automode DUCD Common								
Internal DHCP Server Makility Management								
Mobility Groups Mobility Anchor Config Multicast Messaging								
Ports								
▶ NTP								
► CDP								
▶ PMIPv6								
▶ IPv6								
mDNS								
Advanced								
	•				m			•

Step 3: On every controller in your organization that is not a resilient WLC and is providing DMZ guest access services, navigate to **Controller > Mobility Management > Mobility Groups**, and then click **New**.

Step 4: In the **Member IP Address** box, enter the IP address of the guest controller. (Example: 192.168.19.54 and/or 192.168.19.55 if not using AP-SSO)

Step 5: In the Member MAC Address box, enter the MAC address of the guest controller.

Step 6: In the Group Name box, enter the mobility group name configured on the guest controller, and then click Apply. (Example: GUEST)

DMZ-WLC-Guest - O Image: Contract of the state of t	3.19.54/screens/frameset.html						▼ 🖉 Cer	rtificate Error 🦂 🗙
🚖 Favorites 🏾 🏉 DMZ-WLC-	Guest							
սիսիս						Sa <u>v</u> e	Configuration <u>P</u> ing	Lo <u>q</u> out <u>R</u> efresh
CISCO	<u>M</u> ONITOR <u>W</u> LANS <u>C</u> C	NTROLLER WIRELESS	<u>S</u> ECURITY	MANAGEMENT	C <u>O</u> MMANDS	HE <u>L</u> P	EEEDBACK	
Controller	Mobility Group Memb	er>New					< Back	Apply
General Inventory Interfaces Multicast Network Routes Redundancy Internal DHCP Server Mobility Anchor Config Multicast Messaging	Member IP Address Member MAC Address Group Name Hash	192.168.19.55						
Ports NTP								
CDP PMIPv6								
mDNS Advanced								

Step 7: On the guest controller, navigate to Controller > Mobility Management > Mobility Groups, and then click New.

Step 8: In the **Member IP Address** box, enter the IP address of a campus or remote-site controller. (Example: 10.4.46.64)

Step 9: In the Member MAC Address box, enter the MAC address of the campus or remote-site controller.

Step 10: In the **Group Name** box, enter the mobility group name configured on the campus or remote-site controller, and then click **Apply**. (Example: CAMPUS)

😋 🕒 🔹 https://192168.19.54/screens/frameset.html 🔹 🗴 Certificate Error	↔ ×
البالية، Save Configuration Bing Logove CISCO Monitor WLANS Controller Wireless Security Management Commands Help Feedback	<u>R</u> efresh
Controller Mobility Group Member > New < Back Appl	,
General Member IP Address 10.4.46.64 Invertary Member IP Address 81-43-61 Interface Croups Group Name CAMPUS Multicast Hash none Network Routes Hash none > Redundancy Mobility Groups Mobility Groups > Mobility Groups Perts F > NTP Perts Perts > NTP > > NTP > > NTP > > NDNS > > MoNis Advanced	

Step 11: On each controller, click Save Configuration, and then click OK.

Step 12: Repeat Step 7 through Step 11 on every controller in your organization.

Step 13: Navigate to Controller > Mobility Management > Mobility Groups, and then verify that connectivity is up between all the controllers by examining the mobility group information. In the Status column, all controllers should be listed as Up.

ahaha									Sa <u>v</u> e Configur	ation <u>P</u> ing I	.ogout <u>R</u> efresh
cisco	MONITOR WLANS		WIRELESS	<u>S</u> ECURITY	MANAGEMENT	C <u>O</u> MMANDS	HE <u>L</u> P	EEEDBACK			
Controller	Static Mobility Gro	up Members								New	EditAll
General Inventory	Local Mobility Gro	up CAMPUS									
Interfaces	MAC Address	IP Address	Group	Name	Multicast IP	Hash Key			Status		
Interface Groups	88:43:e1:7e:08:a0	10.4.46.64	CAMPU	s	0.0.0.0	none			Up		
Multicast											_
Network Routes	88:43:e1:7e:0a:60	192.168.19.54	GUEST		0.0.0.0	none			Up		
Redundancy											
▶ Internal DHCP Server											
 Mobility Management Mobility Groups Mobility Anchor Config Multicast Messaging 											

Procedure 15 Create the lobby admin user account

Typically, the lobby administrator is the first person to interact with your corporate guests. The lobby administrator can create individual guest user accounts and passwords that last from one to several days, depending upon the length of stay for each guest.

You have two options to configure the lobby admin user account.

If you have not deployed Cisco Secure ACS and TACACS+ for management access control to the controller, perform the steps in Option 1.

If you have deployed Cisco Secure ACS and TACACS+ for management access control to the controller, perform the steps in Option 2.

Option 1: Local lobby admin user account

Step 1: In Management > Local Management Users, click New.

Step 2: Enter the username. (Example: Guest-Admin)

Step 3: Enter and confirm the password. (Example: C1sco123)

Step 4: In the User Access Mode list, choose LobbyAdmin, and then click Apply.

C C C T Attps://192.168.19.54/screens/frameset.html	🝷 😵 Certificate Error 😽 🗙
A Favorites C DMZ-WLC-Guest	
المالية المالية مالية المالية ال	Saxe Configuration Ping Logout Befresh T
Management Local Management Users > New Summary User Name S SMMP Password HTTP-HTTPS Confirm Password Serial Port User Access Mode Local Management Users User Access Mode User Sessions Local Management User Sessions > Logs Monnt Via Vireless > Software Activation > Tech Support	< Back Apply

Option 2: Centralized lobby admin user account

Create groups in the Cisco Secure ACS internal identity store for network device administrators and helpdesk users. Users in the network device administrator group have enable-level EXEC access to the network devices when they log in, while helpdesk users must type in the enable password on the device in order to get enable-level access.

Step 1: Within Microsoft Active Directory, it is assumed that a lobby ambassador group (Example: Lobby Admins) has been created. Within this group is each of the lobby ambassadors employees within the organization. (Example: Linda Lobby)

Linda Lobby Properties ? 🗙
Dial-in Environment Sessions Remote control Remote Desktop Services Profile Personal Virtual Desktop COM+ General Address Account Profile Telephones Organization Member Of
Member of: Name Active Directory Domain Services Folder Domain Users cisco.local/Users Lobby Admins cisco.local/Users
Add Remove Primary group: Domain Users Set Primary Group There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.
OK Cancel Apply Help

Step 2: In Cisco Secure ACS, navigate to Users and Identity Stores > External Identity Stores > Active Directory.

Step 3: Click the **Directory Groups** tab, and in the **Group Name** box, enter the lobby admin group (Example: cisco.local/Users/Lobby Admins), and then click **Add**.

Cisco Secure A	ACS
My Workspace My Workspace My Workspace More and Identity Stores Identity Groups Internal Identity Stores Users Hosts External Identity Stores LDAP Active Directory RSA SecurID Token Servers RADIUS Identity Gevers Certificate Authonities Certificate Authonities	Users and Identity Stores > External Identity Stores > Active Directory General Directory Groups Directory Attributes Directory groups must be selected on this page to be available as options in group mapping conditions in policy rules. Click Select to launch a dialog to select groups from the directory. Selected Directory Groups: Group Name clisco local/Users/wpn-administrator clisco local/Users/wpn-administrator clisco.local/Users/wpn-partner E
System Administration System Administration	Add A Edit V Replace A Deselect Select GroupName Elscolocal/Users/Lobby Admins Example for group format : cisco com/Users/Domain Users

The lobby admin group appears in the Selected Directory Groups list.

Next, the Active Directory group that was just added to Cisco Secure ACS needs to be mapped to a Secure ACS policy.

Step 4: In Cisco Secure ACS, navigate to Access Policies > Access Services > Default Device Admin > Group Mapping, and then at the bottom of the screen, click Create.

CISCO EVAL(Days left: 323)										
▶ 😚 MyWorkspace	Acc	ess Pol	icies > .	Acces:	s Services	> Default Device Admin > Group Mapping				
In the second	atwork Resources									
B Users and Identity Stores	Group Mapping Policy									
Policy Elements		Filter:	Status			💌 Match if: Equals 💌 🔍 Clear Filter 🛛 🚱 🤝				
Access Policies Access Services	ŀ	E	St	atus	Name	Conditions Results Compound Condition Identity Group	Hit Count			
Service Selection Rules O Default Device Admin		1 🔳		0	Rule-1	AD-AD1:ExternalGroups contains any cisco.local/Builtin/Network Device Admins All Groups:Network Admins	13100			
Identify Count Arepton Authorization • O Default Network Access • G Remote Access VPN • Write Network Authorization • Max User Session Policy Max Session Policy Max Session Folicy Max Bession Folicy • Count Authorization • Count Area Count Area • Count Area • System Administration					I					
	1	• E	De	efault		If no rules defined or no enabled rule matches. All Groups	18			
		Creat	e •	Di	uplicate	Edit Delete Move to V				

Step 5: Under Conditions, select Compound Condition, in the Dictionary list, choose AD-AD1, and then in the Attribute box, click Select. This selects External Groups.

Step 6: Under the Value box, click Select.

Step 7: In the String Enum Definition dialog box, select the lobby admin Active Directory group (Example: cisco. local/Users/Lobby Admins), and then click **OK**.

String	Enum Definition	Showing 1-5 of 5 50	🔻 per page 😡
Filter	▼ Match if: ▼ Go ▼		
	Enum Name		•
	cisco.local/Builtin/Network Device Admins		
	cisco.local/Users/vpn-administrator		
	cisco.local/Users/vpn-employee		
	cisco.local/Users/vpn-partner		
V	cisco.local/Users/Lobby Admins		
		阔 🖪 Page	1 of 1 🕨 🕨
OK	ancel		

Step 8: Under Current Condition Set, click Add. The new condition appears in the Current Condition Set box.

Condition:		
Dictionary:	Attribute:	
AD-AD1	▼ ExternalGroups Select	
Operator:	Value:	
contains any 🔹	Select Deselect Clear	
Current Condition	Set:	
	Add V Edit A Replace V	
And > • Or > •	AD-AD1:ExternalGroups contains any cisco.local/Users/Lobby Ad C	
Results	Delete Preview	
Jentity Group:	Select	

Step 9: Under Results, click **Select**, select the Cisco Secure ACS identity group that will mapped to the Active Directory group specified in the Current Condition Set, and then click **OK**.

Conditions		
🔽 Compound C	Condition:	
Condition:		
Dictionary:	Attribute:	
AD-AD1	✓ ExternalGroups	
Operator:	Value:	
contains any 🔻		
Current Conditi	Select Deselect Clear	
Current Conditi		
And > • Or > •	Add V Edit A Replace V AD-AD1:ExternalGroups contains any cisco.local/Users/Lobby Ad E Delete Preview	E
D#-		
Results		
Identity Group: Al	Il Groups:Lobby Admin Select	
2		
OK Cancel		Help

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

Step 10: In Policy Elements > Authorization and Permissions > Device Administration > Shell Profiles, click Create.

Step 11: Under the General tab, in the **Name** box, enter a name for the wireless shell profile. (Example: Lobby Admins)

Step 12: On the Custom Attributes tab, in the Attribute box, enter role1.

Step 13: In the Requirement list, choose Mandatory.

Cisco Secure ACS -		- • ×
C V V / 10.4.48.15/acsadmin		🝷 😵 Certificate Error 🏼 🎸 🗙
🖕 Favorites 🏾 🏉 Cisco Secure ACS		
Cisco Secure AC	S acsadmin acs-1 (P	imary) LogOut About Help
▶ 😚 My Workspace	Policy Elements > Authorization and Permissions > Device Administration > Shell Profiles > Create	
Network Resources	General Common Tasks Custom Attributes	
With the second seco	Common Taske Attributes	
🔹 🦻 Policy Elements	Attribute Requirement Value	
Session Conditions Date and Time Custom Network Conditions Authorization and Permissions Network Access Device Administration Shell Pontles		E
Command Sets	Manually Entered	
Named Permission Objects	Attribute Requirement Value	
Access Policies	Tote1 Histoatory Loost	
Contoring and reports System Administration		E
	Add A Edit V Replace A Delete	
	Attribute: role1 Attribute: role1 Attribute: Static • Attribute: Static • LOBBY	

Step 14: In the Value box, enter LOBBY, and then click Add.

Step 15: Click Submit.

Next, you create a WLC authorization rule.

Step 16: In Access Policies > Default Device Admin > Authorization, click Create.

- Step 17: In the Name box, enter a name for the WLC authorization rule. (Example: Lobby Admin)
- Step 18: Under Conditions, select Identity Group, and then in the box, enter All Groups:Lobby Admins.

Step 19: Select NDG:Device Type, and then in the box, enter All Device Types:WLC.

Step 20: In the Shell Profile box, enter Lobby Admins, and then click OK.

General Name: Lobby Admin	Status:	Enabled e lower rig	▼ ● ht area of the policy rules	s screen controls	which
Conditions	ditions and resul	is are avai	able here for use in polic	y rules.	
Identity Group:	in	→ A	II Groups:Lobby Admins	Select	
NDG:Location:	-ANY-				
NDG:Device Type:	in	→ A	II Device Types:WLC	Select	
Time And Date:	-ANY-				
Protocol:	-ANY-				
Results					
Shell Profile: Lobby Ad	Imins	S	elect		

Step 21: Click Save Changes.

Procedure 16 Configure the internal WLCs for a guest

When a client connects to the guest SSID, the client must be anchored to the controller in the DMZ. The guest clients' traffic is tunneled from the controller to which the access point is connected to the guest controller, where the access point is given an IP address for the DMZ. The clients' traffic is then redirected to the web authentication page located on the guest controller. The client will not be authorized to connect with any IP protocol until it presents credentials to this authentication page.

սիսիս			S	Sa <u>v</u> e Configur	ation <u>P</u> ing Logout <u>R</u> efresh
cisco	MONITOR WLANS C	ontroller Wireless <u>s</u> ecu	IRITY M <u>a</u> nagement C <u>o</u> mm	ANDS HE	LP <u>F</u> EEDBACK
WLANs	WLANs				Entries 1 - 2 of 2
WLANS	Current Filter: None	[Change Filter] [Clear Filter]	Create New	v v	Go
Advanced	WLAN ID Type	Profile Name	WLAN SSID	Admin Status	Security Policies
	1 WLAN	WLAN-Data	WLAN-Data	Enabled	[WPA2][Auth(802.1X)]
	2 WLAN	Voice	WLAN-Voice	Enabled	[WPA2][Auth(802.1X)]

Step 1: On the WLANs page, in the list, choose Create New, and then click Go.



Step 2: Enter the Profile Name. (Example: Guest)

Step 3: In the SSID box, enter the guest WLAN name, and then click Apply. (Example: Guest)

սիսիս				Sa <u>v</u> e Cor	nfiguration <u>P</u> ing Logout <u>R</u> efresh
cisco	MONITOR WLANS	CONTROLLER WIRELESS	SECURITY MA	NAGEMENT C <u>O</u> MMANDS	HELP FEEDBACK
WLANs	WLANs > New				< Back Apply
WLANS WLANS Advanced	Type Profile Name SSID ID	WLAN Guest Guest 3			

Step 4: Click the Security tab, and then on the Layer 2 tab, in the Layer 2 Security list, choose None.

CISCO	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK	e (<u>R</u> eine
WLANs	WLANs > Edit 'Guest'	Apply
WLANs	General Security QoS Advanced	
Advanced	Layer 2 Layer 3 AAA Servers	_
	Layer 2 Security P None	
	MAC Filtering	
	Foot Notes	
	1 Web Policy cannot be used in combination with IPsec	
	2 H-REAP Local Switching is not supported with IPsec, CRANITE authentication	unic)
	4 Client MFP is not active unless WPA2 is configured	ints)
	5 Learn Client IP is configurable only when HREAP Local Switching is enabled 5 MMM and ones or AES casurity should be enabled to support bisher: 1 to rates	
	7 Multicast Should Be Enabled For IPV6.	
	8 Band Select is configurable only when Radio Policy is set to 'All'. 9 Value zero implier there is no restriction on environm cliente allowed.	
	10 MAC Filtering is not supported with HREAP Local authentication	
	9 Fallo Edit on the supported with NEAP Local automatication 10 MAC Filtering is not supported with NEAP Local automatication 11 MAC Filtering should be enabled. 12 Guest Humalina Local switchina, DHCP Renuired should be disabled.	

սիսիս	Sa <u>v</u> e Configuration <u>P</u> ing Logout <u>R</u> efres
cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP EEEDBACK
WLANs	WLANs > Edit 'Guest' < Back Apply
WLANS WLANS Advanced	General Security QoS Advanced Layer 3 AAA Servers Layer 3 Security None • Image: Security Security Image: Security Security Image: Security None • Image: Security Security Image: Security Security

Step 5: On the Layer 3 tab, select Web Policy.

Step 6: On the QoS tab, in the Quality of Service (QoS) list, choose Bronze (background), and then click Apply.

								Logout <u>R</u> efresh
CISCO	MONITOR <u>W</u> LANS <u>C</u> ON	TROLLER W <u>I</u> RE	LESS <u>S</u> ECURITY	MANAGEMENT	C <u>O</u> MMANDS	HE <u>L</u> P	EEEDBACK	
WLANs	WLANs > Edit 'Guest'						< Back	Apply
WLANS	General Security	QoS Advan	ced					<u>^</u>
Advanced	Quality of Service (QoS)	Bronze (back	(ground) 👻					
	Application Visibility	Enabled						
	AVC Profile	none 👻						
	Netflow Monitor	none 👻						
	Override Per-User Ban	dwidth Contrac	ts (kbps) <u>16</u>					E
		DownStream	UpStream					
	Average Data Rate	0	0					
	Burst Data Rate	0	0					
	Average Real-Time Rate	0	0					
	Burst Real-Time Rate	0	0					
	Clear							
	Override Per-SSID Bar	dwidth Contrac	ts (kbps) <u>16</u>					
		DownStream	UpStream					
	Average Data Rate	0	0					-
	<pre>(</pre>							•

Sa<u>v</u>e Configuration | <u>P</u>ing | Logout <u>R</u>efres uluilu cisco MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK WLANs WLANs > Edit 'Guest' < Back Apply WLANS WLANs General Security QoS Advanced ъ Advanced Profile Name Guest Туре WIAN Guest SSID Status Enabled Security Policies [WPA2][Auth(802.1X)] (Modifications done under security tab will appear after applying the changes.) Radio Policy All -Interface/Interface Group(G) Multicast Vlan Feature 🔲 Enabled Broadcast SSID Enabled Foot Notes
2 H-REAP Local Switching is not supported with IPsec, CRANITE authentication
3 H-REAP Local Switching is not supported with IPsec, CRANITE authentication
4 Claim MP is not exclusion is enabled, a Timeout Value of zero means infinity (will requ
4 Claim MP is not exclusion with the configured of Switching is enabled
6 With and open a AES security should be enabled to support higher 1 in rates
7 Multicast Should Be Enabled For IPV6.
8 Bend Select is configurable only when Radio Policy is set to 'AIT'.
9 Value zero implies there is no restriction on maximum cleints allowed.
11 MAC Filtering should be enabled.
12 Guest tumeling. Local Switching, DHCP Required should be disabled.
13 Max-associated-cleints feature is not supported with HREAP Local Authentication. Foot Notes administrative override to reset excluded clients;

Step 7: On the General tab, to the right of Status, select Enabled, and then click Apply.

Step 8: Click Back.

Step 9: Hover over the blue list next to your guest WLAN, and then click Mobility Anchors.

Step 10: In the **Switch IP Address (Anchor)** list, choose the IP address of the guest controller. (Example: 192.168.19.54)

Step 11: Click Mobility Anchor Create, and then click OK.

սիսիս										Logout <u>R</u> efresh
CISCO	<u>M</u> ONITOR	<u>W</u> LANs	<u>C</u> ONTROLLER	WIRELESS	<u>S</u> ECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	EEEDBACK	
WLANS WLANS WLANS Advanced	Mobility Ai WLAN SSID Switch IP A 192.168.19.1 Mobili Switch IP A	nchors Gu Address (54 ity Ancho Address	est-10k Anchor) r Create (Anchor)	(local) v	Data Path up	C	ontrol Pa	ath	< Back

Step 12: Repeat Step 1through Step 10 for every internal controller in your organization.



Procedure 17 Create guest accounts

Now you can use the lobby administrator account to create usernames and passwords for partners, customers, and anyone else who is not normally granted access to your network.

Step 1: Using a web browser, open the DMZ wireless LAN controller's web interface (for example, https://guest-1.cisco.local/), and then log in using your LobbyAdmin account with the username and password created in Active Directory. (Example: LindaLobby/c1sco123)

Step 2: From the Lobby Ambassador Guest Management page, click New.

 cısco	Lobby Ambassador Guest Management	Logout Refresh Help
Guest Management	Guest Users List	yew
	Items 0	to 0 of 0
	User name WLAN SSLU Account Remaining Time Description	

Step 3: Create a new username and password, or allow the system to create a password automatically by selecting **Generate Password**.

uluili. cisco	Lobby Ambassador Gues	Management Logout Refresh Help
Guest Management	Guest Users List > N	W < Back Apply
	User Name Generate Password Password	partner
	Confirm Password	
	Lifetime	1 day Message from webpage
	Guest User Role	The generated password for this user is BINK54yY
	WLAN SSID	
	Description	

Step 4: Click Apply. The new user name and password are created.

With a wireless client, you can now test connectivity to the guest WLAN. Without any security enabled, you should receive an IP address, and after opening a web browser, you should be redirected to a web page to enter a username and password for Internet access, which will be available to a guest user for 24 hours.

Appendix A: Product List

Wireless LAN Controllers

Functional Area	Product Description	Part Numbers	Software	
Remote Site Controller	Cisco 7500 Series Wireless Controller for up to 6000 Cisco access points	AIR-CT7510-6K-K9	7.4.100.0	
	Cisco 7500 Series Wireless Controller for up to 3000 Cisco access points	AIR-CT7510-3K-K9	-	
	Cisco 7500 Series Wireless Controller for up to 2000 Cisco access points	AIR-CT7510-2K-K9		
	Cisco Flex 7500 Series Wireless Controller for up to 1000 access points	AIR-CT7510-1K-K9		
	Cisco 7500 Series Wireless Controller for up to 500 Cisco access points	AIR-CT7510-500-K9	-	
	Cisco 7500 Series Wireless Controller for up to 300 Cisco access points	AIR-CT7510-300-K9		
	Cisco 7500 Series High Availability Wireless Controller	AIR-CT7510-HA-K9		
	Cisco Virtual Wireless Controller for up to 5 Cisco access points	L-AIR-CTVM-5-K9		
	Cisco Virutal Wireless Controller 25 Access Point Adder License	L-LIC-CTVM-25A		
	Cisco Virtual Wireless Controller 5 Access Point Adder License	L-LIC-CTVM-5A		
	Cisco Virtual Wireless Controller 1 Access Point Adder License	L-LIC-CTVM-1A		
On Site, Remote Site, or Guest 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 5500 Series Wireless Controller for High Availability	AIR-CT5508-HA-K9		
On Site Controller, Guest Controller	Cisco 2500 Series Wireless Controller for up to 50 Cisco access points	AIR-CT2504-50-K9	7.4.100.0	
	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		

Wireless LAN Access Points

Functional Area	Product Description	Part Numbers	Software
Wireless Access Points	Cisco 3600 Series Access Point Dual Band 802.11a/g/n and CleanAir with Internal Antennas	AIR-CAP3602I-x-K9	7.4.100.0
	Cisco 3600 Series Access Point Dual Band 802.11a/g/n and CleanAir with External Antennas	AIR-CAP3602E-x-K9	
	Cisco 2600 Series Access Point Dual Band 802.11a/g/n and CleanAir with Internal Antennas	AIR-CAP2602I-x-K9	
	Cisco 2600 Series Access Point Dual Band 802.11a/g/n and CleanAir with External Antennas	AIR-CAP2602E-x-K9	
	Cisco 1600 Series Access Point Dual-band controller-based 802.11a/g/n with Internal Antennas	AIR-CAP1602I-x-K9	
	Cisco 1600 Series Access Point Dual-band controller-based 802.11a/g/n with External Antennas	AIR-CAP1602E-x-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

Data Center Core

Functional Area	Product Description	Part Numbers	Software	
Core Switch	Cisco Nexus 5596 up to 96-port 10GbE, FCoE, and Fibre Channel N5K-C5596UP-FA SFP+		NX-OS 5.2(1)N1(3) Layer 3 License	
	Cisco Nexus 5596 Layer 3 Switching Module	N55-M160L30V2		
	Cisco Nexus 5548 up to 48-port 10GbE, FCoE, and Fibre Channel SFP+	N5K-C5548UP-FA		
	Cisco Nexus 5548 Layer 3 Switching Module	N55-D160L3		
	Cisco Nexus 5500 Layer 3 Enterprise Software License	N55-LAN1K9		
	Cisco Nexus 5500 Storage Protocols Services License, 8 ports	N55-8P-SSK9		
Ethernet Extension	Cisco Nexus 2000 Series 48 Ethernet 100/1000BASE-T (enhanced) Fabric Extender	N2K-C2248TP-E	_	
	Cisco Nexus 2000 Series 48 Ethernet 100/1000BASE-T Fabric Extender	N2K-C2248TP-1GE		
	Cisco Nexus 2000 Series 32 1/10 GbE SFP+, FCoE capable Fabric Extender	N2K-C2232PP-10GE		


LAN Access Layer

Functional Area	Product Description	Part Numbers	Software
Modular Access Layer Switch	Cisco Catalyst 4507R+E 7-slot Chassis with 48Gbps per slot	WS-C4507R+E	3.4.0.SG(15.1-2SG) IP Base license
	Cisco Catalyst 4500 E-Series Supervisor Engine 7L-E	WS-X45-SUP7L-E	
	Cisco Catalyst 4500 E-Series 48 Ethernet 10/100/1000 (RJ45) PoE+ ports	WS-X4648-RJ45V+E	
	Cisco Catalyst 4500 E-Series 48 Ethernet 10/100/1000 (RJ45) PoE+,UPoE ports	WS-X4748-UPOE+E	
Stackable Access Layer Switch	Cisco Catalyst 3850 Series Stackable 48 Ethernet 10/100/1000 PoE+ ports	WS-C3850-48F	3.2.1SE(15.0-1EX1) IP Base license
	Cisco Catalyst 3850 Series Stackable 24 Ethernet 10/100/1000 PoE+ Ports	WS-C3850-24P	
	Cisco Catalyst 3850 Series 2 x 10GE Network Module	C3850-NM-2-10G	
	Cisco Catalyst 3850 Series 4 x 1GE Network Module	C3850-NM-4-1G	
	Cisco Catalyst 3750-X Series Stackable 48 Ethernet 10/100/1000 PoE+ ports	WS-C3750X-48PF-S	15.0(2)SE2 IP Base license
	Cisco Catalyst 3750-X Series Stackable 24 Ethernet 10/100/1000 PoE+ ports	WS-C3750X-24P-S	
	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	-
Standalone Access Layer Switch	Cisco Catalyst 3560-X Series Standalone 48 Ethernet 10/100/1000 PoE+ ports	WS-C3560X-48PF-S	15.0(2)SE2 IP Base license
	Cisco Catalyst 3560-X Series Standalone 24 Ethernet 10/100/1000 PoE+ ports	WS-C3560X-24P-S	
	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	
Stackable Access Layer Switch	Cisco Catalyst 2960-S Series 48 Ethernet 10/100/1000 PoE+ ports and Two 10GbE SFP+ Uplink ports	WS-C2960S-48FPD-L	15.0(2)SE2 LAN Base license
	Cisco Catalyst 2960-S Series 48 Ethernet 10/100/1000 PoE+ ports and Four GbE SFP Uplink ports	WS-C2960S-48FPS-L	
	Cisco Catalyst 2960–S Series 24 Ethernet 10/100/1000 PoE+ ports and Two 10GbE SFP+ Uplink ports	WS-C2960S-24PD-L	
	Cisco Catalyst 2960-S Series 24 Ethernet 10/100/1000 PoE+ ports and Four GbE SFP Uplink ports	WS-C2960S-24PS-L	
	Cisco Catalyst 2960-S Series Flexstack Stack Module	C2960S-STACK	

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	

LAN Core Layer

Functional Area	Product Description	Part Numbers	Software
Modular Core Layer Switch	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	

WAN Remote Site

Functional Area	Product Description	Part Numbers	Software
Modular WAN Remote- site Router	Cisco 3945 Voice Sec. Bundle, PVDM3-64, UC and SEC License PAK	C3945-VSEC/K9	15.2(4)M3 securityk9 license datak9 license
	Cisco 3925 Voice Sec. Bundle, PVDM3-64, UC and SEC License PAK	C3925-VSEC/K9	
	Data Paper PAK for Cisco 3900 series	SL-39-DATA-K9	
	Cisco 2951 Voice Sec. Bundle, PVDM3-32, UC and SEC License PAK	C2951-VSEC/K9	
	Cisco 2921 Voice Sec. Bundle, PVDM3-32, UC and SEC License PAK	C2921-VSEC/K9	
	Cisco 2911 Voice Sec. Bundle, PVDM3-32, UC and SEC License PAK	C2911-VSEC/K9	
	Data Paper PAK for Cisco 2900 series	SL-29-DATA-K9	
	1941 WAAS Express only Bundle	C1941-WAASX-SEC/ K9	
	Data Paper PAK for Cisco 1900 series	SL-19-DATA-K9	
Fixed WAN Remote-site Router	Cisco 881 SRST Ethernet Security Router with FXS FXO 802.11n FCC Compliant	C881SRST-K9	15.2(4)M3 securityk9 license datak9 license

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)
	Cisco ASA 5525-X IPS Edition - security appliance	ASA5525-IPS-K9	IPS 7.1(7) E4
	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

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-0000355-1 08/13