



Cisco Unified Wireless Guest Access Services

The introduction of Wireless LAN (WLAN) technologies in the enterprise has changed the way corporations and small-to-medium businesses function by freeing staff and network resources from the constraints of fixed network connectivity.

WLAN has also changed how individuals access the Internet and their corporate networks from public locations. The advent of public WLAN (hotspots) has caused mobile workers to become accustomed to being able to access their corporate network from practically anywhere.

Introduction

The paradigm of public access has extended to the enterprise itself. Long gone is the scenario where it was sufficient for a company to provide its partners, visitors, and guests with a place to sit along with an outside line with which to make phone calls. Our highly mobile, information-on-demand culture requires on-demand network connectivity. A half-day spent at a partner or customer venue without access to one's own network resources can impact the productivity of a meeting, service or sales call, and reduce the overall personal productivity of an individual who is away from their office. For this reason, enterprise guest access services are becoming increasingly important and a necessity in the corporate environment.

While there is broad recognition that guest networking is becoming increasingly important, there is also well-founded apprehension over how one safeguards their internal company information and infrastructure assets. Ironically, unbeknownst to many enterprises, their network might already play host to guests who, in an uncontrolled manner, find ways to access the Internet via improperly implemented wired or wireless networks. These guests are not hackers in the true sense, but otherwise well-intentioned individuals trying to get their jobs done. So, on the surface, while it might sound risky

to implement a guest access solution, when implemented correctly, an enterprise that implements a guest access solution will most likely improve their overall security posture as a result of the network audits associated with the implementation process.

In addition to overall improved security, implementing a guest access network offers these additional general benefits:

- Authentication and authorization control of guests based on variables including date, duration, and bandwidth
- An audit mechanism to track who is currently using, or has used, the network

Additional benefits of a wireless-based guest access include the following:

- It provides wider coverage by including areas such as lobbies and other common areas that otherwise might not have been wired for network connectivity.
- It removes the need for designated guest access areas or rooms.

Scope

Several architectures can be implemented to offer guest access in the enterprise. It is not the goal of this chapter to cover all possible solutions. Instead, this chapter focuses on the implementation of wireless guest networking using the Cisco Unified Wireless solution. For more information on deploying wired and wireless Guest Access services in other topology scenarios, see the following URL: http://www.cisco.com/en/US/docs/solutions/Enterprise/Network_Virtualization/GuestAcc.html.

Wireless Guest Access Overview

Ideally, the implementation of a wireless guest network uses as much of an enterprise's existing wireless and wired infrastructure as possible to avoid the cost and complexity of building a physical overlay network. Assuming this is the case, the following additional elements and functions are needed:

- A dedicated guest WLAN/SSID—Implemented throughout the campus wireless network wherever guest access is required.
- Guest traffic segregation—Requires implementing Layer 2 or Layer 3 techniques across the campus
 network to restrict where guests are allowed to go.
- Access control—Involves using imbedded access control functionality within the campus network or implementing an external platform to control guest access to the Internet from the enterprise network.
- Guest user credential management—A process by which a sponsor or lobby administrator can create temporary credentials in behalf of a guest. This function might be resident within an access control platform or it might be a component of AAA or some other management system.

Guest Access using the Cisco Unified Wireless Solution

The Cisco Unified WLAN solution offers a flexible, easy-to-implement method for deploying wireless guest access by using Ethernet in IP (RFC3378) within the centralized architecture. Ethernet in IP is used to create a tunnel across a Layer 3 topology between two WLC endpoints. The benefit of this approach is that there are no additional protocols or segmentation techniques that must be implemented to isolate guest traffic from the enterprise. See Figure 10-1 for an example of guest access topology using a centralized WLAN architecture.



Figure 10-1 Centralized Controller Guest Access

As shown in Figure 10-1, a WLC is located in the enterprise DMZ where it performs an "anchor" function. This anchor controller is responsible for terminating EoIP tunnels that originate from other campus WLCs throughout the network. These "foreign" controllers are responsible for termination, management, and standard operation of the various WLANs provisioned throughout the enterprise, including one or more guest WLANs. Guest WLANs, instead of being switched locally to a corresponding VLAN, are instead transported via an EoIP tunnel to the anchor controller. Specifically, guest WLAN data frames are encapsulated using LWAPP from the AP to the foreign controller and then encapsulated in EoIP from the foreign WLC to a guest VLAN defined on the anchor WLC. In this way, guest user traffic is forwarded to the Internet transparently, with no visibility by, or interaction with, other traffic in the enterprise.

WLAN Controller Guest Access

The WLC Guest Access solution is self-contained and does not require any external platforms to perform access control, web portal, or AAA services. All these functions are configured and run within the anchor controller. However, the option exists to implement one or all of these functions externally and will be discussed later in the chapter.

Supported Platforms

The anchor function, which includes tunnel termination, web authentication, and access control is supported on the following WLC platforms (using version 4.0 and later software images):

- Cisco 4400 Series
- Cisco 6500 Series (WISM)
- Cisco 3750 with integrated WLC

The following WLC platforms cannot be used for anchor functions, but can be used for standard controller deployments and guest mobility tunnel origination (foreign WLC) to a designated anchor controller(s):

- Cisco WLAN Controller Module for Integrated Service Routers (ISR)
- Cisco 2100 Series

Auto Anchor Mobility to Support Wireless Guest Access

Auto anchor mobility, or guest WLAN mobility, is a key feature of the Cisco Unified Wireless solution. It offers the ability to map a provisioned guest WLAN to one or more (anchor) WLCs by using an EoIP tunnel. Auto anchor mobility allows a guest WLAN and all associated guest traffic to be transported transparently across an enterprise network to an anchor controller that resides in the Internet DMZ (see Figure 10-2).



Figure 10-3 shows a sniffer trace of an Ethernet in IP tunnel (highlighted) between a foreign controller with a guest WLAN provisioned and an anchor controller that is performing local web authentication. The first IP detail shown represents the Ethernet in IP tunnel between the foreign and anchor controllers. The second IP detail is that of guest traffic (in this case, a DNS query).



Figure 10-3 Sample Ethernet in IP Sniffer Trace

Anchor Controller Deployment Guidelines

This section provides guidelines for deploying an anchor controller to support wireless guest access.

Anchor Controller Positioning

Because the anchor controller is responsible for termination of guest WLAN traffic and subsequent access to the Internet, it is typically positioned in the enterprise Internet DMZ. In doing so, rules can be established within the firewall to precisely manage communications between authorized controllers throughout the enterprise and the anchor controller. Such rules might including filtering on source or destination controller addresses, UDP port 16666 for inter-WLC communication, and IP protocol ID 97 Ethernet in IP for client traffic. Other rules that might be needed include the following:

- TCP 161 and 162 for SNMP
- UDP 69 for TFTP
- TCP 80 or 443 for HTTP, or HTTPS for GUI access
- TCP 23 or 22 for Telnet, or SSH for CLI access

Depending on the topology, the firewall can be used to protect the anchor controller from outside threats.

For the best possible performance and because of its suggested positioning in the network, it is strongly recommended that the guest anchor controller be dedicated to supporting guest access functions only. In other words, the anchor controller should not be used to support guest access in addition to controlling and managing other LWAPP APs (LAPs) in the enterprise.

DHCP Services

As previously described, guest traffic is transported at Layer 2 via EoIP. Therefore, the first point at which DHCP services can be implemented is either locally on the anchor controller or the controller can relay client DHCP requests to an external server. See Guest Access Configuration, page 10-14 for configuration examples.

Routing

Guest traffic egress occurs at the anchor controller. Guest WLANs are mapped to a dynamic interface/VLAN on the anchor. Depending on the topology, this interface might connect to an interface on a firewall, or directly to an Internet border router. Therefore, a client's default gateway IP is either that of the firewall or the address of a VLAN/interface on the first hop router. For ingress routing, it is assumed the guest VLAN is directly connected to a DMZ interface on a firewall or to an interface on a border router. In either case, the guest (VLAN) subnet is known as a directly connected network and advertised accordingly.

Anchor Controller Sizing and Scaling

The most cost-effective platform to support guest networking in most enterprise deployments is the Cisco 4400 Series controller. Assuming the controller is being deployed to support guest access with EoIP tunnel termination only, the 4402 with support for 12 APs is sufficient because it is assumed the controller is not going to be used to manage LAPs in the network.

A single 4400 Series controller can support EoIP tunnels from up to 40 foreign controllers within the enterprise. Additionally, the 4400 supports up to 2500 simultaneous users and has a forwarding capacity of 2 Gbps.

Anchor Controller Redundancy

Beginning with Release 4.1 of Unified Wireless solution software, a "guest N+1" redundancy capability was added to the auto anchor/mobility functionality. This new feature introduces an automatic ping function that enables a foreign controller to proactively ping anchor controllers to verity control and data path connectivity. In the event of failure or an active anchor becomes unreachable, the foreign controller does the following:

- Automatically detects that the anchor has become unreachable
- Automatically disassociates any wireless clients that were previously associated with the unreachable anchor
- Automatically re-associates wireless client(s) to an alternate anchor WLC

With guest N+1 redundancy, two or more anchor WLCs can be defined for a given guest WLAN. Figure 10-4 shows a generic guest access topology with anchor controller redundancy.



Figure 10-4 Guest Access Topology with Guest Anchor N+1 Redundancy

Keep in mind the following with regard to guest N+1 redundancy:

- A given foreign controller load balances wireless client connections across the list of anchor controllers configured for the guest WLAN. There is currently no method to designate one anchor as primary with one or more secondary anchors.
- Wireless clients that are associated with an anchor WLC that becomes unreachable are re-associated with another anchor defined for the WLAN. When this happens, assuming web authentication is being used, the client is redirected to the web portal authentication page and required to re-submit their credentials.



Multicast traffic is not supported over guest tunnels, even if multicast is enabled on the Cisco Unified Wireless Network.

Web Portal Authentication

The Cisco Centralized Guest Access solution offers a built-in web portal that is used to solicit guest credentials for authentication and offers simple branding capabilities, along with the ability to display disclaimer or acceptable use policy information (see Figure 10-5).

Web Authentication	Preview - Microsoft Internet Explorer provided by Cisco Systems, Inc.	
	rites Iools Help Links 🛅 TSE-LAB 🕘 My Yahoo! 🙆 Customize Links 🙆 VPN 3002 Hardware Client 🙆 Windows	••••••••••••••••••••••••••••••••••••••
🕒 🕞 Back 👻 🌍 👻 🖹	👔 🏠 🔎 Search 👷 Favorites 🛷 😥 - 💺 📴 🖵 🚉 💈	
Address 🙆 https://10.20.1	110.254/screens/base/login_preview.html	💌 🄁 Go
Login		ululu ▲ cisco
Cisco is pleased to	Cisco wireless network provide the Wireless LAN infrastructure lase login and put your air space to work.	
User Name		
Password		
	Submit	
		Internet
🕘 Done		Internet 🔬 🚰

Figure 10-5 Controller Web Authentication Page

The web portal page is available on all Cisco WLAN controller platforms and is invoked by default when a WLAN is configured for Layer 3 web policy-based authentication.

If a more customized page is required, administrators have the option of importing and locally storing a customized page. Additionally, if an enterprise wants to use an external web server, the controller can be configured to redirect to it in place of using the internal server. See Guest Access Configuration, page 10-14 for web page configuration guidelines.

User Redirection

As is typical for most web-based authentication systems, in order for guest clients to be redirected to the WLC web authentication page, they must launch a web browser session and attempt to open a destination URL. For redirection to work correctly, the following conditions must be met:

• DNS resolution—The guest access topology must ensure that valid DNS servers are assigned via DHCP and those DNS servers are reachable to users prior to authentication. When a client associates to a web policy WLAN for authentication, all traffic is blocked except DHCP and DNS. Therefore, the DNS servers must be reachable from the anchor controller. Depending on the topology, this might require opening up conduits through a firewall to permit DNS or modifying ACLs on an Internet border router.



Clients with static DNS configurations might not work depending on whether their configured DNS servers are reachable from the guest network.

- Resolvable Home Page URL—The home page URL of a guest user must be globally resolvable by DNS. If a user home page is, for example, an internal company home page that cannot be resolved outside of their company intranet, that user is not redirected. In this case, the user must open a URL to a public site such as www.yahoo.com or www.google.com.
- HTTP Port 80—If the home page of a user is resolvable, but connects to a web server on a port other than port 80, they are not redirected. Again, the user is required to open a URL that uses port 80 to be redirected to the WLC web authentication page.

Note

In addition to port 80, there is an option to configure one additional port number that the controller can monitor for redirection. The setting is available only through the CLI of the controller: <*controller_name>* config> network web-auth-port *port>*.

Guest Credentials Management

Guest credentials can be created and managed centrally using WCS beginning with release 4.0 and later. A network administrator can create a limited privilege account within WCS that permits lobby ambassador access for the purpose of creating guest credentials. With such an account, the only function a lobby ambassador is permitted to do is create and assign guest credentials to controllers that have web-policy configured WLANs. For configuration guidelines, see Guest Access Configuration, page 10-14.

As with many configuration tasks within WCS, guest credentials are created using templates. Beginning with release 4.1, the following new guest user template options and capabilities were introduced:

- There are two types of guest templates: one for scheduling immediate guest access with limited or unlimited lifetime, and the other permits administrators to schedule "future" guest access and offers time of day as well as day of week access restrictions.
- The solution now offers administrators the ability to e-mail credentials to guest users. Additionally, when the "schedule" guest template is used, the system automatically e-mails credentials for each new day (interval) that access is offered.
- Guest credentials can be applied to the WLC(s) based on a (guest) WLAN SSID and WCS mapping information; campus/building/floor location or based on a WLAN SSID and a specific controller or list of controllers. The latter method is used when deploying guest access using the guest mobility anchor method as discussed in this chapter.

For further information, see Guest Management Using WCS, page 10-30.

After a lobby ambassador has created a guest template, it is applied to one or more controllers depending on the guest access topology. Only controllers with a "*web*" *policy-configured WLAN* are listed as a candidate controller to which the template can be applied. This is also true when applying guest templates to controllers based on WCS map location criteria.

Guest credentials, once applied, are stored locally on the (anchor) WLC (under Security > Local Net Users) and remain there until expiration of the "Lifetime" variable as defined in the guest template. If a wireless guest is associated and active when their credentials expire, the WLC stops forwarding traffic and returns to the WEBAUTH_REQD policy state for that user. Unless the guest credentials are re-applied (to the controller), the user is no longer able to access the network.



The Lifetime variable associated with guest credentials is independent of the WLAN session timeout variable. If a user remains connected beyond the WLAN session timeout interval, they are de-authenticated. The user is then redirected to the web portal and, assuming their credentials have not expired, must log back in to regain access. To avoid annoying redirects for authentication, the guest WLAN session timeout variable should be set appropriately.

Local Controller Lobby Admin Access

In the event that a centralized WCS management system is not deployed or unavailable, a network administrator can establish a local admin account on the anchor controller, which has only lobby admin privileges. A person who logs in to the controller using the lobby admin account has access to guest user management functions. Configuration options available for local guest management are limited in contrast to the capabilities available through WCS, and include the following:

- User name
- Generate password (check box)
- Administrator-assigned password
- Confirm the password
- Lifetime-days:hours:minutes:seconds
- SSID (check box)
- Only WLANs configured for Layer 3 web policy authentication are displayed
- Description

Any credentials that may have been applied to the controller by WCS are shown when an admin logs into the controller. A local lobby admin account has privileges to modify or delete any guest credentials that were previously created by WCS. Guest credentials that are created locally on the WLC do not automatically appear in WCS unless the controller's configuration is updated/refreshed in WCS. Locally created guest credentials that are imported into WCS as a result of a WLC configuration refresh appear as a new guest template that can be edited and re-applied to the WLC.

Guest User Authentication

As previously discussed in Guest Credentials Management, page 10-10, when an administrator uses WCS or a local account on a controller to create guest user credentials, those credentials are stored locally on the controller, which in the case of a centralized guest access topology, would be the anchor controller.

When a wireless guest logs in through the web portal, the controller handles the authentication in the following order:

1. The controller checks its local database for username and password and, if present, grants access.

If no user credentials are found, then:

2. The controller checks to see if an external RADIUS server has been configured for the guest WLAN (under WLAN configuration settings). See External Radius Authentication, page 12-38 for a configuration example. If so, then the controller creates a RADIUS access-request packet with the user name and password and forwards it to the selected RADIUS server for authentication.

If no specific RADIUS servers have been configured for the guest WLAN:

3. The controller checks its global RADIUS server configuration settings. Any external RADIUS servers configured with the option to authenticate "network" users are queried with the guest user credentials. See External Radius Authentication, page 12-38 for a configuration example. Otherwise, if no RADIUS servers have "network user" checked, and the user has not authenticated as a result of 1 or 2 above, authentication fails.

Note

A RADIUS server can still be used to support network user authentication even if the network user check box is cleared under the WLC Security > AAA > RADIUS settings. However, to do so, a server must then be explicitly selected under the Security > AAA Servers settings of a given WLAN. See External Radius Authentication, page 12-38 for a configuration example.

External Authentication

WLC and WCS guest account management (lobby ambassador) capabilities can be used only to create and apply guest user credentials for local authentication on the WLC. However, there may be cases where an enterprise already has an existing guest management /authentication solution deployed as part of a wired guest access or NAC solution. If this is the case, the anchor controller/guest WLAN can be configured to forward web portal authentication to an external RADIUS server, as described in Guest User Authentication, page 10-11.

The default protocol used by the controller to authenticate web users is Password Authentication Protocol (PAP). In the event you are authenticating web users to an external AAA server, be sure to verify the protocols supported by that server. The anchor controller can also be configured to use CHAP or MD5-CHAP for web authentication. The web auth protocol type is configured under the Controller configuration settings of the WLC.

External Authentication using Cisco Secure ACS and Microsoft User Databases

If a guest access deployment is planning to use a Microsoft user database in conjunction with Cisco ACS to authenticate guest users, see the following additional Cisco ACS configuration caveats: http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.0/in stallation/guide/windows/postin.html.

See specifically the following URL: http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.0/in stallation/guide/windows/postin.html#wp1041223

Guest Pass-through

Another variation of wireless guest access is to bypass user authentication altogether and allow open access. However, an enterprise may still need to present an acceptable use policy or disclaimer page to users before granting access. If this is the case, then a guest WLAN can be configured for web policy pass through. In this scenario, a guest user is redirected to a portal page containing disclaimer information. Pass through mode also has an option for a user to enter an e-mail address before connecting (see Figure 10-6 and Figure 10-7 for sample pages). See Guest Access Configuration, page 10-14 for configuration examples.

💪 Web Authentication - Windows Internet Explorer	
CO Co + C https://1.1.1.1/login.html?redirect=www.yahoo.com/	Google
😪 🏟 🍘 Web Authentication	🟠 🔹 🗟 👻 🖨 Page 👻 🎯 T <u>o</u> ols 👻
Connect	
Welcome to the Cisco wireless network	
Cisco is pleased to provide the Wireless LAN infrastructure for your network. Please login and put your air space to work.	
Accept	
6	
	a
	v d v d v d v d v d v d v d v d v d v d
Done	🚺 🚺 🕞 Internet 🕅 🕄 100% 👻 🤶

Figure 10-6 Pass-through Welcome AUP Page

/eb Authentication - Windows Internet Explorer		_ 🗗 🗙
+ Attps://1.1.1.1/login.html?redirect=www.yahoo.com/	Google 🗲 🖌	₽ •
2 Contraction	🟠 🔹 🗟 👻 🖶 🔁 Pag	ge 🔹 🍥 Tools 🔹 🎽
Connect		
Connect		
Welcome to the Cisco wireless network		
Cisco is pleased to provide the Wireless LAN infrastructure for your network. Please login and put your air space to work.		
Email Address		
Accept		
		•
	🐻 🚱 Internet	€ 100% -

Figure 10-7 Pass-through Page with E-mail

Guest Access Configuration

This section describes how to enable a wireless guest access service within the Cisco Unified Wireless solution. The configuration tasks require the use of a web browser, Windows IE6 (only). A web session is established with the controller by opening an HTTPS session to the controller management IP address: https://management_IP or optionally to a controller service port IP address.

The following procedures assume there is already a deployed infrastructure of controllers and LAPs with the possible exception of the anchor WLC(s). See Anchor Controller Deployment Guidelines, page 10-6 for more information.



Cisco recommends that the configuration steps outlined in this section be followed in the order in which they are presented.

The following references are used throughout the configuration sections:

- Foreign WLC—Refers to the one or more WLCs deployed throughout an enterprise campus or at branch location that are used for managing and controlling a group of LAPs. Foreign controllers map a guest WLAN into a guest mobility EoIP tunnel.
- Anchor WLC—Refers to one or more WLCs deployed in the enterprise DMZ that are used to perform guest mobility EoIP tunnel termination, web redirection, and user authentication.



Only the relevant portion of a given configuration screen capture is shown in this section.

The implementation of the Cisco Unified Wireless Guest Access solution can be broken into the following configuration categories:

- Anchor WLC Installation and Interface configuration—This section briefly discusses installation
 requirements, steps and caveats associated with implementing one or more anchor WLCs. When
 implementing guest access for the first time in an existing Unified Wireless deployment, the anchor
 WLC is usually a new platform that is installed at the Internet edge of an Enterprise network.
- 2. Mobility Group Configuration—This section outlines the parameters that must be configured in order for the foreign WLCs to be able to initiate EoIP tunnels to one or more guest anchor WLCs. The mobility group configuration does not itself create the EoIP tunnels, but rather establishes peer relationships between the foreign and anchor WLCs in order to support a guest access WLAN service.
- **3.** Guest WLAN Configuration—Highlights WLAN specific configuration parameters that are required to map the guest WLAN (originating from a foreign WLC) to the anchor WLC. It is during this portion of the guest access solution configuration that EoIP tunnels are created between the foreign and anchor WLCs. This section also covers the settings required to invoke Layer 3 redirection for web-based authentication.
- 4. Guest Account Management—This section outlines how to configure and apply guest user credentials locally on the anchor WLC using WCS' or the anchor WLC's lobby admin interface.
- **5.** Other Features and Solution Options—Discusses other features that may be configured including, but not limited to:
 - a. Web-portal page configuration and management
 - **b.** Support for external web redirection
 - c. Pre-authentication ACLs
 - d. Anchor WLC DHCP configuration
 - e. External radius authentication
 - f. External access control

Anchor WLC Installation and Interface Configuration

As described in Anchor Controller Positioning, page 10-6, Cisco recommends that the anchor WLC be dedicated solely to guest access functions and not be used to control and manage LAPs in the enterprise.

This section does not address all aspects of interface configuration on the anchor WLC. It is assumed the reader is familiar with the WLC initialization and configuration process required upon initial bootup using the serial console interface. If not, see the following URL: http://www.cisco.com/en/US/docs/wireless/controller/4400/quick/guide/ctrlv32.html.

This section offers specific information and caveats as they pertain to configuring interfaces on a WLC being deployed as an anchor in a guest access topology.

As part of the initial configuration (using the serial console interface), you are required to define the following three static interfaces:

• Controller management—This interface/IP is used for communications with other controllers in the network. It is also the interface used to terminate EoIP tunnels that originate from the foreign controllers.

- AP manager interface—Even though the controller is not used to manage APs, you are still required to configure this interface. Cisco recommends the AP manager interface be configured on the same VLAN and subnet as the management interface.
- Virtual interface—The controller quickstart installation documentation recommends defining the virtual IP with an address, such as 1.1.1.1. This address needs to be the same for all controllers that are members of the same mobility group name. The virtual interface is also used as the source IP address when the controller redirects clients for web authentication.

Guest VLAN Interface Configuration

The interfaces previously described are for operations and administrative functions associated with the controller. To implement a guest access service, another interface must be defined. This is the interface through which guest traffic is forwarded for routing to the Internet. As previously described in Anchor Controller Positioning, page 10-6, the guest interface will likely connect to a port on a firewall or be switched to an interface on an Internet border router.

Defining a New Interface

Perform the following to define and configure an interface to support guest traffic:

- **Step 1** Click the **Controller** tab.
- **Step 2** In the left pane, click **Interfaces**.
- Step 3 Click New. (See Figure 10-8.)

 cısco	MONITOR	<u>W</u> LANs		WIRELESS	<u>S</u> ECURITY	MANAGEMEN	т с <u>о</u> м	Sa <u>v</u> e Co 4MANDS	nfiguration <u>P</u> in HELP	; Lo <u>q</u> out	<u>R</u> efres
Controller	Interfaces									New	
General	Interface N	Name	vi	AN Identifier	IP Address	Interfa	е Туре	Dynami	ic AP Manageme	nt	
Inventory	ap-manager	:	9		10.15.9.253	Static		Enabled			
Interfaces	managemer	nt	9		10.15.9.11	Static		Not Supp	ported		
Network Routes	service-port		N/	Ά	172.28.217.1	31 Static		Not Supp	ported		
Internal DHCP Server	virtual		N/	Ά	1.1.1.1	Static		Not Supp	ported		
Mobility Management											
Spanning Tree											

Figure 10-8 Controller Interfaces

Defining an Interface Name and VLAN ID

Step 4 Enter an interface name and VLAN ID. (See Figure 10-9.)

								nfiguration <u>P</u> ing	Logout <u>R</u> efresh
cisco	<u>M</u> ONITOR	<u>W</u> LANs	<u>C</u> ONTROLLER	W <u>I</u> RELESS	<u>S</u> ECURITY	MANAGEMENT	C <u>O</u> MMANDS	HE <u>L</u> P	
Controller	Interfaces	s > New						< Back	Apply
General	Interface	Name g	uest-dmz						
Inventory									
Interfaces	VLAN Id	3	1						
Network Routes									
Internal DHCP Server									
Mobility Management									

Figure 10-9 Interface Name and VLAN ID

Defining Interface Properties

Step 5 Define the following properties:

- Interface IP
- Mask
- Gateway (for the firewall or next hop router connected to the anchor controller)
- DHCP Server IP (If using an external DHCP server, use the IP address of that server in the Primary DHCP Server field.)

See Figure 10-10.

Figure 10-10	Defining Interface Properties
Figure 10-10	Demning interface Properties

սիսիս						Sa <u>v</u> e Cor	nfiguration Ping	Logout <u>R</u> efrest
cisco	MONITOR WLANS		W <u>I</u> RELESS	<u>S</u> ECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	
Controller	Interfaces > Edit						< Back	Apply
General Inventory	General Informat	ion						
Interfaces Network Routes	Interface Name MAC Address	guest-d 00:0b:8	mz 5:40:7e:e0					
Internal DHCP Server Mobility Management	Interface Address	5						
Spanning Tree Ports	VLAN Identifier IP Address	31	0.31.11					
Master Controller Mode	Netmask		255.255.0					
Network Time Protocol	Gateway		0.31.1					
▶ QoS	Physical Informat	ion						
▶ CDP	Port Number	1]					
	Backup Port	0]					
	Active Port	0						
	Enable Dynamic AP Management							
	Configuration							
	Quarantine							
	DHCP Information	1						
	Primary DHCP Serv	ver 10.2	0.30.11					
	Secondary DHCP S	erver						



If DHCP services are to be implemented locally on the anchor controller, populate the primary DHCP server field with the management IP address of the controller. See Anchor WLC Installation and Interface Configuration, page 10-15.

If guest N+1 redundancy is being implemented in the DMZ, repeat the above interface configuration for each additional anchor WLC being deployed.

Mobility Group Configuration

The following default mobility group parameters should already be defined on the foreign WLC(s) as part of a standard centralized WLAN deployment. To support auto-anchor mobility for guest access, the anchor WLC(s) must also be configured with a mobility group domain name.

Defining the Default Mobility Domain Name for the Anchor WLC

Configure a default mobility domain name for the anchor WLC. The anchor's mobility domain name should be different than what is configured for the foreign WLCs. In the examples below, the WLCs (foreign controllers) associated with the enterprise wireless deployment are all members of mobility group 'SRND'. The guest anchor WLC on the other hand, is configured with a different mobility group name: "ANC". This is done to keep the anchor WLC logically separate from the primary mobility domain associated with the enterprise wireless deployment.

- **Step 1** Click the Controller tab.
- **Step 2** Enter a name in the Default Mobility Domain Name field.
- Step 3 Click Apply. (See Figure 10-11.)

Figure 10-11 Defining a Default Mobility Domain Name on the Anchor WLC

uluilu cisco	MONITOR WLANS CONTROLLER	WIRELESS SECURITY	Saye Configuration <u>P</u> ing Logout <u>R</u> efresh MANAGEMENT C <u>O</u> MMANDS HELP
CISCO Controller General Inventory Interfaces Network Routes Internal DHCP Server Mobility Management	General 802.3x Flow Control Mode LWAPP Transport Mode LAG Mode on next reboot Ethernet Multicast Mode	Disabled w Layer 3 w Disabled w Disabled w Disabled w	MANAGEMENT COMMANDS HELP Apply (Current Operating Mode is Layer3) (LAG Mode is currently disabled).
Spanning Tree Ports Master Controller Mode Network Time Protocol QOS CDP	Aggressive Load Balancing Peer to Peer Blocking Mode Over The Air Provisioning of AP AP Fallback Apple Talk Bridging Fast SSID change Default Mobility Domain Name RF-Network Name User Idle Timeout (seconds)	Enabled w Disabled w Disabled w Disabled w ANC ANC 300	
	ARP Timeout (seconds) Web Radius Authentication 802.3 Bridging Operating Environment Internal Temp Alarm Limits	300 CHAP Disabled Commercial (0 to 40 C) 0 to 65 C	

Defining Mobility Group Members of the Anchor WLC

Every foreign WLC within the enterprise deployment that is going to support the guest WLAN must be defined as a mobility group member in the guest anchor WLC(s).

- **Step 1** Click the **Controller** tab.
- Step 2 In the left pane, click Mobility Management and then Mobility Groups. (See Figure 10-12.)

Figure 10-12 Defining Mobility Group Members

սիսիս							Sa <u>v</u> e Co	nfiguration <u>P</u> ing	Logout <u>R</u> efresl
CISCO	<u>M</u> ONITOR	<u>W</u> LANs	<u>C</u> ONTROLLER	WIRELESS	<u>S</u> ECURITY	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HELP	
Controller	Static Mot	oility Gro	oup Members					New	EditAll
General	Default	Mobility C	Group SRND						
Inventory	MAC Add	iress	IP Address	Group N	Name				
Interfaces Network Routes	00:0b:85	:40:7e:e0	10.15.9.11	(Local)					
Internal DHCP Server	00:0b:85	:40:23:a0	10.15.9.14	SRND					
💌 Mobility Management	00:0b:85	:40:40:00	10.20.2.2	SRND					
Mobility Groups Mobility Anchor Config	00:0b:85	:40:41:40	10.20.2.3	SRND					
Mobility Anchor Config Mobility Statistics	00:0b:85	:40:7f:c0	10.20.110.254	SRND					

Adding Foreign Controllers as Mobility Group Members

Step 3 Click **New** to define a MAC and IP address for each foreign controller that will support the guest access WLAN. (See Figure 10-13.)

Figure 10-13 Adding Foreign Controllers to Anchor WLC

 cısco	MONITOR	<u>W</u> LANs		WIRELESS	<u>s</u> ecurity	MANAGEMENT	Sa <u>v</u> e Co C <u>O</u> MMANDS	nfiguration <u>P</u> ing HELP	Lo <u>g</u> out <u>R</u> ef	fresh
Controller	Mobility (Group Me	ember > New					< Back	Apply	
General Inventory Interfaces	Member IP Member M		s							
Network Routes Internal DHCP Server Mobility Management Mobility Groups	Group Nam	10	SRND							



The 'Group Name' in Figure 10-13 above is the name configured under the foreign WLC's 'Default Mobility Domain Name', which should be different than the name used by the anchor WLC. The member IP and MAC address are those addresses shown by the **show mobility summary** command. Repeat the above steps for each additional foreign WLC that will support the guest WLAN. If more than one anchor is being deployed (guest N+1 redundancy), then repeat the steps in Defining the Default Mobility Domain Name for the Anchor WLC, page 10-18 and Defining Mobility Group Members of the Anchor WLC, page 10-19.

Adding the Anchor WLC as a Mobility Group Member of a Foreign WLC

As described in Auto Anchor Mobility to Support Wireless Guest Access, page 10-4, each foreign WLC maps the guest WLAN into an EoIP tunnel that terminates on the anchor WLC. Therefore, the anchor WLC(s) must be defined as a mobility group member in each foreign controller. In the example below, note that the group name entry for the anchor WLC is 'ANC' (see Defining Mobility Group Members of the Anchor WLC, page 10-19) whereas the other WLCs that comprise the enterprise wireless deployment are members of the mobility group: 'SRND'.

- Step 1 Click New to add the anchor WLC's IP, MAC address, and Group Name to the mobility members table.
- **Step 2** Repeat these steps for each additional foreign controller. (See Figure 10-14.)

Figure 10-14 Adding Anchor Controller(s) to Foreign WLC

ahaha							iguration <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> ONTROLLER	WIRELESS	<u>S</u> ECURITY	MANAGEMENT	C <u>O</u> MMANDS	HE <u>L</u> P	
Controller	Static Mobility Gro	up Members					New	EditAll
General	Default Mobility G	roup SRND						
Inventory	MAC Address	IP Address	Group N	ame				
Interfaces Network Routes	00:18:73:44:f6:a0	10.15.9.19	(Local)					
Internal DHCP Server	00:0b:85:40:23:a0	10.15.9.14	SRND					
Mobility Management	00:0b:85:40:40:00	10.20.2.2	SRND					
Mobility Groups Mobility Anchor Config	00:0b:85:40:41:40	10.20.2.3	SRND					
Mobility Anchor Coning Mobility Statistics	00:0b:85:40:7e:e0	10.15.9.11	ANC					
Spanning Tree	00:0b:85:40:7f:c0	10.20.110.254	SRND					
Ports	00:0b:85:40:80:00	10.15.9.12	SRND					
Master Controller	00:0b:85:40:8a:a0	10.15.9.13	SRND					
Mode	00:18:73:45:07:40	10.15.9.17	SRND					
Network Time	00:18:73:45:28:80	10.15.9.20	SRND					
Protocol	00:18:73:45:39:00	10.15.9.18	SRND					
▶ QoS	00:d0:2b:fc:28:40	10.20.100.254	SRND		•			
▶ CDP								

Note

If guest N+1 anchor redundancy capability is being deployed, two or more anchor WLC entries are added to each foreign WLC's Mobility Group Members list.

Guest WLAN Configuration

The following section describes how to configure a single guest WLAN. The guest WLAN is configured on every foreign WLC that manages APs where guest access is required. Even though the anchor WLC(s) is not specifically used to manage LAPs associated with a guest WLAN, it must also be configured with the guest WLAN because the anchor WLC is a logical extension of the WLAN where user traffic is ultimately bridged (using LWAPP between the AP and the foreign controller, and EoIP between the foreign controller and the anchor controller) to an interface/VLAN on the anchor WLC.



It is extremely important to note that *all* parameters defined in the WLAN Security, QoS, and Advanced settings tabs, *must be configured identically* in both the anchor and foreign WLC(s). Figure 10-15 shows a high level diagram illustrating the WLAN configuration discussed below.



Figure 10-15 WLAN Configuration

<u>Note</u>

The parameters defined in the WLAN Security, QoS, and Advanced settings tabs, *must be configured identically* in both the anchor and foreign controller(s).

Foreign WLC—Guest WLAN Configuration

Step 1 Click the WLANs tab and then click New. (See Figure 10-16.)

MONITOR WLANS CONTROLLE	ER W <u>I</u> REI	LESS <u>S</u> ECURITY MANAGEMEN		Configuration <u>P</u> ing Logout DS HELP	<u></u>
WLANs				New	
Profile Name	WLAN ID			Security Policies	
CCKM	3	ССКМ	Enabled	[WPA2][Auth(802.1X + CCKM)]	-
1	Profile Name	Profile Name WLAN ID	Profile Name WLAN ID WLAN SSID	Admin Profile Name WLAN ID WLAN SSID Status	Admin Profile Name WLAN ID WLAN SSID Status Security Policies

Figure 10-16	Guest WLAN Configuration
--------------	--------------------------

Defining a Guest WLAN SSID

Step 2 Define an SSID that is intuitive or easily recognized by potential guest users.

The controller automatically assigns a VLAN ID. Administrators have the option selecting 1 - 16, as long as the ID is not already in use by another SSID/ WLAN.

- **Step 3** Define a Profile Name.
- Step 4 Click Apply. (See Figure 10-17.)

Figure 10-17 Defining a Guest WLAN SSID

սիսիս							Sa <u>v</u> e Col	nfiguration <u>F</u>	2ing Logout <u>R</u> efresh
cisco	MONITOR	<u>W</u> LANs		WIRELESS	<u>S</u> ECURITY	MANAGEMENT	C <u>O</u> MMANDS	HE <u>L</u> P	
WLANs	WLANs >	New						< Back	Apply
WLANs WLANs	WLAN ID		1 💌						
AP Groups VLAN	Profile Na	me	Guest Acce	ss					
	WLAN SSI	D	Guest						

After creation of the new WLAN, the configuration page appears, as shown in Figure 10-18.

սիսիս						Sa <u>v</u> e Cor	figuration <u>P</u> ing	Logout <u>R</u> efresh
cisco	<u>m</u> onitor <u>w</u> l	ANS <u>C</u> ONTROLLE	R W <u>I</u> RELESS <u>S</u>	ECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	
WLANs	WLANs > Edi	t					< Back	Apply
WLANS WLANS	General	Security QoS	Advanced					
AP Groups VLAN	Profile Nam	e Guest	Access WLAN					
	WLAN SSID	Guest						
	WLAN Statu	s 🗆 En	abled					
	Security Pol	-][Auth(802.1X)] ations done under se	ecurity tab w	ill appear after ap	plying the chang	es.)	
	Radio Policy		~					
	Interface Broadcast S		ement 🔽					
	Foot Notes							
	2 Web Policy o	upported by 10xx mo annot be used in com I Switching is not sup,	bination with IPsec	RANITE and	FORTRESS authen	tication		

Figure 10-18 WLAN Configuration Page



The default interface used by the foreign WLC for the guest WLAN is the management interface. If the EoIP tunnel cannot be established with the anchor, the foreign controller will disassociate any wireless clients that were previously associated with the unreachable anchor and then assign new clients and reassociated clients to the interface configured under the guest WLAN of the foreign itself. Therefore, it is recommended to link the guest WLAN on the foreign to a non-routable network, or alternatively configure the DHCP server of the management interface with an unreachable IP address. If the anchor becomes unreachable, this prevents the guest clients to gain access to the management network.

Defining Guest WLAN Parameters and Policies

Under the General Configuration tab, perform the following steps.

- **Step 1** Enable the WLAN by clicking the box next to WLAN Status.
- **Step 2** Optionally, set the radio policy if you wish to restrict which bands support the guest access.
 - **a.** Broadcast SSID is enabled by default; leave enabled.
 - **b.** By default, the WLAN is assigned to the "management" interface of the WLC. Do not change this.
- **Step 3** Click the **Security** tab. (See Figure 10-19.)

 cısco	Sa <u>v</u> e Configuration <u>P</u> ing 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
WLANS	WLANs > Edit < Back
WLANs AP Groups VLAN	Profile Name Guest Access WLAN
	WLAN SSID Guest WLAN Status 🕑 Enabled
	Security Policies [WPA2][Auth(802.1X)] (Modifications done under security tab will appear after applying the changes.)
	Radio Policy B02.11b/g only V Interface management V
	Broadcast SSID

Figure 10-19 Defining Guest WLAN General Policies

Step 4 Set the Layer 2 Security to none from its default setting (802.1x WPA/WPA2). (See Figure 10-20.)

Figure 10-20 WLAN Layer 2 Security Configuration

սիսիս		onfiguration <u>P</u> ing Logout <u>R</u> efresh
cisco	<u>M</u> ONITOR <u>W</u> LAN₅ <u>C</u> ONTROLLER WIRELESS <u>S</u> ECURITY MANAGEMENT COMMANDS	HELP
WLANs	WLANs > Edit General Security QoS Advanced	< Back Apply
WLANS WLANS AP Groups VLAN	Layer 2 Layer 3 AAA Servers	
	Layer 2 Security None	

Step 5 Click the Layer 3 tab. (See Figure 10-21.)

Figure 10-21 Guest WLAN Layer 3 Security Configuration

	Save	Configuration <u>P</u> ing Logout <u>R</u> efresh
cısco	Monitor Wlans Controller Wireless Security Management Commani)S HELP
WLANS WLANS WLANS AP Groups VLAN	WLANs > Edit General Security QoS Advanced Layer 2 Layer 3 AAA Servers Layer 3 Security None V V Web Policy 2 Image: Conditional Web Redirect Preauthentication Preauthentication ACL None V None V	< Back Apply

Step 6 Click the Web Policy checkbox (a list of additional options will be presented).

A dialog warning box appears, indicating that the WLC will pass DNS traffic to and from clients prior to authentication.

Step 7 Select **Authentication** or **Pass-through** for the web policy. (See Guest User Authentication, page 10-11.)



L

A pre-authentication ACL can be used to apply an ACL that allows un-authenticated clients to connect to specific hosts or URL destinations before authentication. The ACL is configured under Security > Access Control Lists. If a pre-authentication ACL is used in conjunction with the web auth policy, it must include a rule to permit DNS requests; otherwise, the client will be unable to resolve and connect to a destination host/URL that would otherwise be allowed by the ACL.

Step 8 Select the **QoS** tab, as shown in Figure 10-22.

Sa<u>v</u>e Configuration | <u>P</u>ing | Lo<u>g</u>out | <u>R</u>efr CISCO WLANs WLANs > Edit < Back Apply General Security QoS Advanced WLANs WLANS AP Groups VLAN Quality of Service (QoS) Bronze (background) WMM WMM Policy Disabled 💌 7920 AP CAC Enabled 222546 7920 Client CAC Enabled

Figure 10-22 Guest WLAN QoS Configuration

- **Step 9** Optionally, set the upstream QoS profile for the guest WLAN. The default is 'Silver (Best Effort)'. In this example, the guest WLAN has been re-assigned to the lowest QoS class.
- **Step 10** Click the **Advanced** tab. (See Figure 10-23.)

Figure 10-23 Guest WLAN Advanced Configuration

ာါကျက cisco	Save Configuration Ping Logout Befresh MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
WLANS WLANS	WLANs > Edit Apply
AP Groups VLAN	Allow AAA Override Enabled DHCP H-REAP Local Switching 2 Enabled DHCP Server Override Session Timeout (secs) 0 DHCP Addr. Assignment Required Aironet IE Enabled DHCP Addr. Assignment Required
	Diagnostic Channel Enabled Management Frame Protection (MFP) IPv6 Enable Infrastructure MFP Override Interface ACL None Client Exclusion [±] Enabled 60 MPP Client Timeout Value (secs) Optional

Step 11 Set Session Timeout (this is optional).

<u>Note</u>

Any session timeout greater than 0 (default) forces de-authentication after expiration, and requires the user to re-authenticate through the web portal.

Step 12 Set DHCP Addr. Assignment to "Required".



Setting DHCP Addr. Assignment to "Required" is recommended to prevent guest users from attempting to use the guest network using a static IP configurations.

Step 13 Click Apply when finished.

Establishing the Guest WLAN Mobility Anchor(s)

- Step 1 From the WLAN menu on the foreign WLC find the newly created guest WLAN.
- Step 2 Highlight and click Mobility Anchors from the right-hand pull-down selection list. (See Figure 10-24.)

.ılı.ılı. cısco	MONITOR	<u>W</u> LANs	<u>C</u> ONTROLLER	WIRE	LESS	<u>S</u> ECURITY	MANAGEME			nfiguration HE <u>L</u> P	<u>P</u> ing Lo <u>q</u> ou	t <u>R</u> efresh
WLANs	WLANs										New.	
WLANS	Profile Na	me	WL	AN ID	WLAN	SSID		Admin Status	Se	curity Polici	es	
AP Groups VLAN	Guest Acces	ss WLAN	1		Guest			Enabled	W	eb-Auth		
	CCKM		3		сскм			Enabled	[W	/PA + WPA2][/	Auth Remove	
							_				Mobility Anchors	
	* WLAN IDs	9-16 will n	ot be pushed to 11	xx, 12x	ix and	13xx model AF	P5.					

Figure 10-24 WLAN Mobility Anchor

Step 3 In the Switch IP Address (Anchor) pull-down selection list, select the IP address corresponding to the management interface of the anchor WLC deployed in the network DMZ. This is the same IP address configured in Adding the Anchor WLC as a Mobility Group Member of a Foreign WLC, page 10-20.

Step 4 Click Mobility Anchor Create. (See Figure 10-26.)

Figure 10-25 Selecting Management Interface from Switch IP Address (Anchor)

ဂျက်၊ cisco	MONITOR WLANS CONTROLLER	WIRELESS <u>S</u> ECURITY	MANAGEMENT	Sa <u>v</u> e Configuration C <u>O</u> MMANDS HE <u>L</u> P	<u>P</u> ing Lo <u>q</u> out <u>R</u> efresh
WLANS • WLANS WLANS AP Groups VLAN	Mobility Anchors WLAN SSID Guest Switch IP Address (Anchor) Mobility Anchor Create Switch IP Address (Anchor)	10.15.9.19(local) ♥ 10.15.9.19(local) ♥ 10.29.2.4 10.20.2.3 10.20.15.9.11 10.20.10.254 10.15.9.13 10.15.9.13 10.15.9.13 10.15.9.13 10.15.9.13 10.15.9.20 10.15.9.24 10.20.100.254	Data Path	Control Path	< Back

،، ،،، ،، cısco	MONITOR	<u>W</u> LANs	<u>C</u> ONTROLLER	WIRELESS	<u>S</u> ECURITY	MANAGEMENT	Sa <u>v</u> e Conf C <u>O</u> MMANDS		<u>P</u> ing Logout <u>R</u> efresh
WLANS WLANS	Mobility A		st						< Back
AP Groups VLAN	Mobi	Address (A ility Anchor Address (Create	10.15.9.11		Data Path	Con	rol Path	

Figure 10-26 Selecting WLAN Mobility Anchor

Verifying the Guest WLAN Mobility Anchor

Once configured, the screen shown in Figure 10-27 shows the mobility anchor (selected from above), assigned to the Guest WLAN.

Figure 10-27 Verifying the Guest WLAN Mobility Anchor

MONITOR WLANS CONTROLLER WIRELESS SECURITY	MANAGEMENT	Sa <u>v</u> e Configuration <u>P</u> i C <u>O</u> MMANDS HELP	ng Lo <u>q</u> out <u>R</u> efre
Mobility Anchors			< Back
WLAN SSID Guest Switch IP Address (Anchor)	Data Path	Control Path	
10.15.9.11	up	up	
Mobility Anchor Create			
Switch IP Address (Anchor) 10.15.9.19(local)			
	Mobility Anchors WLAN SSID Guest Switch IP Address (Anchor) 10.15.9.11 Mobility Anchor Create	Mobility Anchors WLAN SSID Guest Switch IP Address (Anchor) Data Path 10.15.9.11 up Mobility Anchor Create Image: Content of the second sec	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP Mobility Anchors

For ease of verification, the page displays whether or not the mobility tunnel data path and LWAPP control path have been established with the anchor. If either or both show "down", see Troubleshooting Guest Access, page 10-54 for troubleshooting tips. The pull-down selection list to the right offers the option to send a ping to the destination anchor WLC.

- **Step 5** When finished, click **Back**.
- **Step 6** Repeat the steps above for each additional anchor WLC being deployed (guest N+1 redundancy).

This completes the guest WLAN configuration. Repeat all steps from Foreign WLC—Guest WLAN Configuration, page 10-21 through Verifying the Guest WLAN Mobility Anchor, page 10-27 for each additional foreign WLC that will support the guest WLAN.

Guest WLAN Configuration on the Anchor WLC

Guest WLAN configuration on the anchor controller(s) is identical to that of the foreign controller except for minor differences in the WLAN interface and mobility anchor configuration, which are detailed below.



The SSID defined for the guest WLAN must be exactly the same as what is defined on the foreign WLCs.

Anchor WLC—Guest WLAN Interface

As indicated above, the parameters configured for the guest WLAN on the anchor WLC are the same except the interface to which the WLAN is mapped. In this case, the guest WLAN is assigned to an interface/VLAN on the anchor WLC, which connects to an interface on a firewall or Internet border router.

- Step 1 Click the WLANs tab.
- **Step 2** Create, configure, and enable the guest WLAN the same way it was configured on the foreign WLC(s) except for the following:

In the WLANs general configuration, under **Interface**, choose the interface name created in Guest VLAN Interface Configuration, page 10-16. (See Figure 10-28.)

Step 3 Click Apply.

Figure 10-28 Anchor WLC Guest WLAN Interface Configuration

սիսիս				Sa <u>v</u> e Cor	nfiguration <u>P</u> ing	Logout <u>R</u> efresh	þ
CISCO	<u>M</u> ONITOR <u>W</u> LANS <u>C</u> ONT	OLLER W <u>I</u> RELESS <u>S</u> ECU	RITY M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HE <u>L</u> P		
WLANs	WLANs > Edit				< Back	Apply	^
▼ WLANs	General Security	QoS Advanced					
WLANs							
AP Groups VLAN	Profile Name	Guest Access WLAN					
	WLAN SSID	Guest					
	WLAN Status	Enabled					
		[WPA2][Auth(802.1X)] Modifications done under securit	y tab will appear after a	pplying the chang	jes.)		
	Radio Policy Interface	802 <u>.11b/g only</u>					2
	Broadcast SSID	✓ Enabled					221877

Anchor WLC—Defining the Guest WLAN Mobility Anchor

The second parameter that differs in configuration from the foreign WLC is the WLAN mobility anchor configuration. The guest WLAN mobility anchor is the anchor WLC itself.

- Step 1 Click the WLANs tab.
- Step 2 Find the Guest WLAN and click Mobility Anchors.
- **Step 3** From the pull-down selection list, choose the IP address representing the anchor controller. The IP address has (Local) next to it.
- Step 4 Click Mobility Anchor Create. (See Figure 10-29.)

ာါကျက cisco	MONITOR WLANS CONTROL	.er w <u>i</u> reless <u>s</u> ecuri	TY M <u>A</u> NAGEMENT		<u>P</u> ing Logout <u>R</u> efresh
WLANs	Mobility Anchors				< Back
WLANS WLANS AP Groups VLAN	WLAN SSID Guest Switch IP Address (Anchor)		Data Path	Control Path	
	Mobility Anchor Create		_		
	Switch IP Address (Anchor)	10.15.9.11(local) 💌	>		

Figure 10-29 Defining the Guest WLAN Mobility Anchor

Note that the guest WLAN mobility anchor is *local*. (See Figure 10-30.)

Figure 10-30 Verifying Guest Mobility Anchor

սիսիս			Sa <u>v</u> e Configuration	<u>P</u> ing Lo <u>q</u> out <u>R</u> efresh
cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY	MANAGEMENT	C <u>o</u> mmands he <u>l</u> p	
WLANs	Mobility Anchors			< Back
▼ WLANS WLANS AP Groups VLAN	WLAN SSID Guest Switch IP Address (Anchor)	Data Path	Control Path	
	Mobility Anchor Create Switch IP Address (Anchor) 10.15.9.14	up	up	

Because the mobility anchor for the guest WLAN is the anchor WLC itself, the Data and Control Path status will always show "up". If not, check to ensure that you have selected the local WLC as the anchor from the 'Switch IP Address (Anchor) drop down menu.

Step 5 If guest N+1 redundancy is being implemented, repeat the WLAN configuration for each additional anchor WLC being deployed. Otherwise, this completes the configuration steps required to create the guest WLAN on the anchor WLC.

Guest Account Management

- If guest credentials are going to be managed locally on the anchor controller, there are two methods by which they can be created and applied:
- Through a WCS lobby ambassador admin or super user/root admin account
- Directly on the controller via a local lobby admin account or other management account with read/write access

Guest Management Using WCS

The following configuration examples assume WCS version 4.1.83 or later has been installed and configured, and a lobby ambassador account has been created. For more information on installing and configuring WCS, see the following URL:

http://www.cisco.com/en/US/products/ps6305/products_installation_and_configuration_guides_list.ht ml.

Regarding the creation of guest accounts, see the following URL: http://www.cisco.com/en/US/products/ps6305/products_configuration_guide_chapter09186a00808318 41.html#wp1075155.

Note

Ensure that the individual WLC configurations are synchronized with WCS before creating guest templates.

Log in to WCS using the Lobby Ambassador credentials assigned by the system administrator. (See Figure 10-31.)



Figure 10-31 WCS Login

After logging in, the screen shown in Figure 10-32 appears.

Figure 10-32 WCS Lobby Admin Interface

սիսիս	Wireless Control Sy	stem	Usern	ame: lobbyadmin Logout	Refresh Print View 🖉
cisco	Help 🔻				
Guest Users	Guest Users			Add Gu	est User 💌 🖸
	User Name	<u>Profile</u>	Description	Applied To	Status

There are two types of guest templates:

- The Add Guest User template allows administrators to create and immediately apply guest credentials to one or more anchor WLCs.
- The **Schedule Guest User** template allows administrators to create guest credentials that are applied to one or more anchor WLCs at some future month, day, and time. (See Figure 10-33.)

Figure 10-33 Guest User Template Option

ahaha	Wireless Control Sy	vstem	Usern	ame: lobbyadmin Logout Refresh Print View
CISCO	<u>H</u> elp ▼			
Guest Users	Guest Users			Add Guest User 🕑 GO
	User Name	<u>Profile</u>	Description	Add Guest User Applied Delets Guest User Schedule Guest User Print/Email User Details

Using the Add Guest User Template

- Step 1 From the pull-down selection list, select Add Guest User and click Go.
- **Step 2** The template shown in Figure 10-34 appears.

cisco	Wireless Control System	Username: lobbyadmin Logout Refresh Print View
CISCO	<u>H</u> elp ▼	
Guest Users	Guest Users > New User	
	Guest Information	
	User Name	
	Generate Password Password	
	Confirm Password	
	Account Configuration	
	Profile	None
	Life Time	⊙ Limited ○ Unlimited
	End Time	16 💌 Hour 55 💌 Min. 07/19/07 💽 Day
	Apply To	Indoor Area
	Campus	Root Area 💌
	Building	None
	Floor	All Floors
	Description	Wireless Network Guest Ac
	Disclaimer	Guests understand and acknowledge that we exercise no control over the nature, content or v
		Make this Disclaimer default
	Save Cancel	

Figure 10-34 Add Guest User Template

Figure 10-35 shows an example of guest user account creation.

ahaha	Wireless Control System	Username: lobbyadmin Logout Refresh Print Viev
cisco	<u>H</u> elp ▼	
luest Users	Guest Users > New User	
	Guest Information	
	User Name	guest1
	Generate Password	
	Password	•••••
	Confirm Password	•••••
	Account Configuration	
	Profile	Guest
	Life Time	⊙ Limited ○ Unlimited
	End Time	8 🕑 Hour 🛛 4 💌 Min. 07/20/07 🔤 Day
	Apply To	Controller List 💌
		IP Address Name
		✓ 10.15.9.11 Controller1
		V 10.15.9.13 Controller3
		10.15.9.19 Controller9
	Description	Wireless Network Guest Ac
	Disclaimer	Guests understand and acknowledge that we exercise no control over the nature, content or v
		Make this Disclaimer default
	Save Cancel	

Figure 10-35 Guest User Account Creation

Step 3 Under Guest Information, enter a User Name and Password.

Passwords are case sensitive. User names are restricted to 24 characters or less. Administrators also have an option to allow the system to automatically generate a password by clicking on the **Generate Password** check box.

- Step 4 Under Account Configuration, select the following:
 - Profile—The pull-down selection list displays a list of WLANs (SSIDs) configured with a L3 Web Policy.
 - Life Time—Select "limited" or "unlimited"
 - End Time—If the guest account is "limited", select the month, day, and time the credentials are to expire.
 - Apply To—From the pull-down selection list, select **Controller List** and click the check box next to the controller(s) representing anchor WLCs. Note that there will be other controllers listed; however, these represent the foreign WLCs. There is no need to apply user credentials on the foreign WLCs because the authentication enforcement point is the anchor WLC.



As seen in Figure 10-35, there are various options for where the credentials can be applied, including being able to control the physical/geographic location where a user can access the guest WLAN. These include outdoor areas, indoor areas, building, floor, and so on. This location-based access method can only be used if: 1) the WLAN deployment has been integrated into the WCS mapping database, and 2) the guest WLAN (a WLAN with web policy) does not use mobility anchors.

• Description—Enter a description. The description is displayed on the WLC to which the credentials are applied under Security > Local Net Users. It is also included in the e-mail that can be sent to a guest informing them of what credentials to use to access the network.

L

- Disclaimer—Used in the e-mail that can be sent to a guest user informing them of what credentials to use to access the network
- Step 5 Click Save when finished. The summary screen shown in Figure 10-36 appears, acknowledging that credentials have been applied to the anchor controller(s). The admin is also presented with an option to print or e-mail the credentials to the guest user.

Figure 10-36	Successful Guest Account Creation
--------------	-----------------------------------

ahaha	Wireless (Control System	Userr	iame: lobbyadmin Logout Re	fresh Print Viev
cisco	<u>H</u> elp 🔻				
lest Users	Guest User	Account application result to t	he Selected controllers		
	IP Address	Controller Name	Operation Status	Reason	
	10.15.9.11	Controller1	Success	-	
	10.15.9.13	Controller3	Success	-	
			Guest User Credentials		
	Guest User Name	Guest1			
	Password	test			
	Profile	Guest			
	Start Time	8: 17: 07/19/2007			
	End Time	9: 0: 07/19/2007			
	Disclaimer	Guests understand and acknowledge t and/or data passing through our netwo	hat we exercise no control over ork.	the nature, content or reliability o	f the information
	Print/Email Gu	est User Credentials			

Step 6 Click **Print/Email Guest User Credentials**. The screen shown in Figure 10-37 appears.

Gues	t Users Details E-mail Print Back
	Email To Subject Send Cancel Credentials for Guest User Guest1
Guest Use Name	
Password	test
Profile	Guest
Start Time	8: 17: 07/19/2007
End Time	9: 0: 07/19/2007
Disclaimer	Guests understand and acknowledge that we exercise no control over the nature, content or reliability of the information and/or data passing through our network.

Figure 10-37 Print/Email Guest User Details



For details on setting up an SMTP mail server to support e-mailing guest account information to users, see the WCS Configuration guide at the following URL: http://www.cisco.com/en/US/docs/wireless/wcs/4.1/configuration/guide/wcsadmin.html.

After printing and or e-mailing the account details, the screen shown in Figure 10-38 appears. By clicking the **User Name**, an admin can go back and edit the guest account or remove it by checking the box next to the User Name and selecting **Delete Guest User** from the pull-down selection list.

221894

cisco	Wireless Contro	ol System	Username:	lobbyadmin Logout Re	fresh Print View
	<u>H</u> elp ▼				
est Users	Guest Users			Add Guest Us	ser 💌 GO
	User Name	Profile	Description	Applied To	Status
	Guest1	Guest	Wireless Network Guest Access	Controller List	Active

Figure 10-38 WCS Guest Users Summary

Using the Schedule Guest User Template

For details about configuring guest accounts, see the WCS Configuration guide at the following URL: http://www.cisco.com/en/US/docs/wireless/wcs/4.1/configuration/guide/wcsadmin.html.

Figure 10-39 shows the guest user template option.

Figure 10-39 Guest User Template Option

ahaha	Wireless Control Sy	stem	Userna	ime: lobbyadmin Logout	Refresh Print View
cisco	<u>H</u> elp ▼				
Guest Users	Guest Users			Schedu	le Guest User 🔽 GO
	User Name	Profile	Description	Applied To	Status

Step 1From the pull-down selection list, select Schedule Guest User and click Go.The template shown in Figure 10-40 appears.

ahaha	Wireless Control System	Username: lobbyadmin Logout Refresh Print View 🔄
CISCO	<u>H</u> elp ▼	
Guest Users	Guest Users > Scheduling	
	Guest Information	
	User Name	
		Generate new on every schedule
	Account Configuration	
	Profile	None
	Life Time	💿 Limited 🔘 Unlimited
	Start Time	10 🗸 (Hours) 15 🖌 (Minutes) 07/19/07
	End Time	10 🗸 (Hours) 15 🔽 (Minutes) 07/20/07
		Days of the week Sun Mon Tues Wed Thur Fri Sat
	Apply to	Indoor Area 💌
	Campus	Root Area 💌
	Building	None
	Floor	All Floors
	Email credentials to	
	Description	Wireless Network Guest Ac
	Disclaimer	Guests understand and acknowledge that we exercise no control over the nature, content or
		Make this Disclaimer default
	Save Cancel	

Figure 10-40 Schedule Guest User Template

Figure 10-41 shows an example of a schedule guest user account creation.

սիսին	Wireless Control System	Username: lobbyadmin Logout Refresh Print View
CISCO	Help 🔻	
Guest Users	Guest Users > Scheduling	
	Guest Information	
	User Name	test2
		Generate new on every schedule
	Account Configuration Profile	Guest 🗸
	Life Time	 Limited Unlimited
	Start Time	8 V (Hours) 0 V (Minutes) 07/19/07
	End Time	17 💙 (Hours) 0 💙 (Minutes) 07/27/07
		Days of the week Y Y Y Y Sun Mon Tues Wed Thur Fri Sat
	Apply to	Controller List
		IP Address Name
		V 10.15.9.11 Controller1
		V 10.15.9.13 Controller3
		10.15.9.19 Controller9
	Email credentials to	johndoe@crisco.com
	Description	Wireless Network Guest Ac
	Disclaimer	Guests understand and acknowledge that we exercise no control over the nature, content or
		Make this Disclaimer default
	Save Cancel	

Figure 10-41 Schedule Guest User Account Creation

- Step 2 Under Guest Information, enter a User Name. User names can be up to 24 characters long. When using the schedule-based template, administrators have the option to allow the system to automatically generate the user name for each new day that access is being offered. Also, when using this template, the system automatically generates the user password. There is no option to manually assign a password.
- **Step 3** Under Account Configuration, select the following:
 - Profile—The pull-down selection list displays a list of WLANs (SSIDs) configured with an L3 Web Policy.
 - Life Time—Select "limited" or "unlimited".
 - Start Time—Select the time, month, and day when the account is to become active.

\$

- **Note** The start time cannot begin within the current day that the account is being created. The start day must be one or more days beyond the day the account is being created.
- End Time—If the account is limited, select the stop time, month, and day.



Note The stop day can be a period no longer than 30 days from the start day.

• Days of Week—Depending on the lifetime of the account, administrators have the ability to control for which days of the week access is available. Click the check boxes next to those days of the week access is permitted.


If "Days of the Week" is selected, the start and stop times represent the period within each day that access is available. Upon expiry within a given day, WCS removes the credentials from the applicable controllers. For each new day/interval that access is permitted, WCS automatically generates a new password (and optionally a username), e-mails it to the guest user, and re-applies the new credentials to the applicable WLCs. If "Days of the Week" is not defined, access begins based on the start day and time and is continuously active until the end day and time.

• Apply To—From the pull-down selection list, select **Controller List** and click the check box next to the controller(s) representing anchor WLCs. Note that there will be other controllers listed; however, these represent the foreign WLCs. There is no need to apply user credentials on the foreign WLCs because the authentication enforcement point is the anchor WLC.



As seen in Figure 10-41, there are various options for where the credentials can be applied, including being able to control the physical/geographic location where a user can access a guest WLAN. These include outdoor areas, indoor areas, building, floor, and so on. This location-based access method can only be used if: 1) the WLAN deployment has been integrated into the WCS mapping database, and 2) the guest WLAN (a WLAN with web policy) does not use mobility anchors.

• E-mail Credentials to—Enter the e-mail address for whom an account is being established. This is a mandatory field.



An SMTP mail server must be configured in WCS so that it can use to send guest account information. For details, see the following URL: http://www.cisco.com/en/US/docs/wireless/wcs/4.1/configuration/guide/wcsadmin.html.

- Description—Provide a description. The description is displayed on the WLC to which the credentials are applied under Security > Local Net Users. The description is also included in an e-mail that can be sent to the guest, informing them of what credentials to use to access the network.
- Disclaimer—Used in the e-mail that is sent to a guest user, informing them of what credentials to use to access the network.
- **Step 4** Click **Save** when finished. The screen shown in Figure 10-42 appears, acknowledging that the scheduled account has been created. The admin is also presented with an option to print or e-mail the credentials to the guest user.

ahaha	Wireless	Control System Username: lobbyadmin Logout Refresh Print View								
cisco	<u>H</u> elp ▼									
Guest Users	Guest User	Guest User Account Scheduled on the selected controllers								
		Guest User Credentials								
	Guest User Name	test2								
	Password	Frla4urF								
	Profile	Guest								
	Start Time	8: 0: 07/20/2007								
	End Time	17: 0: 08/03/2007								
	Disclaimer	Guests understand and acknowledge that we exercise no control over the nature, content or reliability of the information and/or data passing through our network.								
	Print/Email Gu	est User Credentials								

Figure 10-42 Successful Scheduled Account Creation

L

Step 5 Optionally, click Print/Email Guest User Credentials. The screen shown in Figure 10-43 appears.

Gu	est Users Details E-mail Print Back
	Email To
Guest Name	User test2
Passv	ord Frla4urF
Profile	Guest
Start	me 8: 0: 07/20/2007
End Ti	ne 17: 0: 08/03/2007
Discla	Guests understand and acknowledge that we exercise no control over the nature, content or reliability of the information and/or data passing through our network.

Figure 10-43 Print/E-mail Guest User Details

After printing and/or e-mailing the account details, the summary screen shown in Figure 10-44 appears. By clicking the **User Name**, an admin can go back and edit the guest account or remove it by checking the box next to the User Name and selecting **Delete Guest User** from the pull-down selection list.

Figure 10-44 WCS Guest Users Summary

ahaha	Wireless Control	ol System	Usernam	ie: lobbyadmin Logout	Refresh Print View
cisco	<u>H</u> elp ▼				
Guest Users	Guest Users			Add Gue	st User 💌 🔽 GO
	User Name	Profile	Description	Applied To	Status
	test2	Guest	Wireless Network Guest Access	Controller List	Scheduled



If a user template is deleted from WCS while a user is active, they are de-authenticated.

This completes the steps required to create a guest account using the lobby ambassador interface in WCS.

Managing Guest Credentials Directly on the Anchor Controller

The following procedure assumes that a network administrator has established a local management account with lobby admin privileges on one or more anchor controllers.

Step 1 Login to the anchor controller using the lobby admin credentials assigned by the system administrator. Remember that conduits might need to be opened through a firewall to permit HTTP/HTTPS for web administration of the controller. See Anchor Controller Positioning, page 10-6.

After login, the screen shown in Figure 10-53 appears.

uluulu cisco	Lobby Ambassador Guest Management			Logout Re	fresh
Guest Management	Guest Users List			New	
	It	ems 0	to O	of O	
	User Name WLAN SSID Account Remaining Time Description				

Figure 10-45 Anchor Controller Login

Step 2 Click New.

The screen shown in Figure 10-46 appears.

Figure 10-46	Creating Local WLC Guest Credentials
--------------	--------------------------------------

	Lobby Ambassador Gues	t Management	Logout Refresh
Guest Management	Guest Users List > N	eW < Back	Apply
	User Name	test3	
	Generate Password		
	Password	••••	
	Confirm Password	••••	
	Lifetime	1 days 0 hours 0 mins secs 0	
	WLAN SSID	Guest 💌	
	Description	Guest Access WLAN	

- **Step 3** To create user credentials, perform the following steps:
 - a. Enter a username and password (manual or auto).
 - **b.** Select the WLAN/SSID to which the guest account applies (only WLANs configured with an L3 web policy are displayed).
 - c. Enter a lifetime for the credentials.
 - **d**. Enter a description for the user.

Step 4 Click Apply.

The screen shown in Figure 10-47 appears and shows the newly-added guest user.

Figure 10-47 Anchor WLC Guest Users List

ແມ່ນເມ່ນ cisco	Lobby Ambassador Guest	t Management			Logout Refres
Guest Management	Guest Users List				New
				Items 1	to 1 of 1
	User Name	WLAN SSID	Account Remaining Time	Descrip	rtion
	test3	Guest	1 d	Guest A	ccess WLAN

From this screen you have the option to do the following:

- Edit the existing user (link at far right; not visible)
- Delete the existing user (link at far right; not visible)
- Add a new user

Configuring the Maximum Number of User Accounts

The default number of guest user accounts that can be defined on the controller is 512. This value can be changed by completing the following steps.

Step 1 Click the **Security** tab. (See Figure 10-48.)



uluili. cisco	MONITOR	<u>W</u> LANs		WIRELESS	<u>S</u> ECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	Logout <u>R</u> efre
Security	General								Apply
▼ AAA General ▼ RADIUS	Maximun	n Local Dat	abase entries (on	next reboot).	512	(Current Maximum	is 512)		

Step 4 Click Apply.

Step Step

Maximum Concurrent User Logins

The maximum number of concurrent logins for a local user account on the WLC can be configured. Values include 0 for unlimited concurrent logins or can be limited from 1 to 8. The maximum user logins is configured by completing the following steps:

Step 1 Click the **Security** tab. (See Figure 10-49.)

սիսիս							Sa <u>v</u> e Con	figuration	<u>P</u> ing	Logout <u> </u>	<u>R</u> efresh
CISCO	<u>M</u> ONITOR	<u>W</u> LANs	<u>C</u> ONTROLLER	W <u>I</u> RELESS	<u>S</u> ECURITY	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HE <u>L</u> P			
Security	User Poli	cies								Apply	
AAA General AADIUS Authentication Accounting TACACS+ LDAP LoCal Net Users MAC Filtering Disabled Clients User Login Policies AP Policies	Maximum	n Number of	f Concurrent Logi	ns for a single	user name				0		

Figure 10-49 User Login Policies

Step 2 In the left pane, click User Login Policies under AAA.

Step 3 Configure the maximum number of concurrent user logins (between 0–8).

Step 4 Click Apply.

Guest User Management Caveats

Note the following caveats:

- Guest accounts can be added using either method above or both methods together.
- When using WCS, the lobby admin may not have visibility of user accounts that might have been created locally on the anchor controller if the controller configuration has not been recently synchronized with WCS. If this is the case and a WCS lobby admin attempts to add an account with a user name that is already configured on the WLC, the WCS configuration overrides the local configuration.
- When adding user accounts locally on the controller, the local admin will have visibility of all accounts that have been created, including those that were created via WCS.
- If a guest user is currently authenticated to a WLAN and their credentials are deleted from WCS or locally on the controller, the user traffic stops flowing, and the user is de-authenticated.

Other Features and Solution Options

Web Portal Page Configuration and Management

The internal web server and associated functionality is hosted locally on the anchor controller. When a WLAN is configured to use the web policy, either for authentication or pass-through, the internal web server is invoked by default. No further configuration is required. The internal portal includes a few optional configuration parameters.

Internal Web Page Management

- Step 1 Click the Security tab.
- **Step 2** In the left pane, click **Web Auth** and then **Web Login Page**.

The configuration screen shown Figure 10-50 is displayed. You can change the heading and message information that appears on the portal page. You can also choose a post-authentication redirect URL.

								nfiguration <u>P</u> ing	Logout <u>R</u> efres
CISCO	<u>M</u> ONITOR	<u>W</u> LANs		WIRELESS	<u>S</u> ECURITY	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HELP	
Security	Web Log	in Page						Preview	Apply
 AAA General RADIUS Authentication Accounting TACACS+ LDAP Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies Local EAP Priority Order Access Control Lists IPSec Certs Wireless Protection Policies Web Login Page Certificate CIDS 	page. The Li	llows you to ogin page is b Authentic	customize the co presented to we ation' is turned or	b users the firs (under WLAN Hide the Cisco winner ased to providi	arance of the t time they acc Security Polici eless network a the Wireless	cess the	ork.		

Figure 10-50 Web Login Page Configuration Screen

Step 3 Click Apply.

Step 4 Optionally, click **Preview** to view what the user sees when redirected.

Importing A Web Page

You can download a customized web page and store it locally on the anchor controller. To import a customized web page, perform the following steps.

Step 1 Click the **Commands** tab. (See Figure 10-51.)

Figure 10-51 Importing a Web Page

սիսիս									Lo <u>q</u> out <u>R</u> efresh
CISCO	<u>M</u> ONITOR		<u>C</u> ONTROLLER	WIRELESS	<u>S</u> ECURITY	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HE <u>L</u> P	
Commands	Download	l file to (Controller					Clear	Download
Download File	File Type			Webauth	Bundle	~			
Upload File									
Reboot	TFTP Serve	er							
Reset to Factory Default	IP Address	;		10.20.30	200				
Set Time	Maximum	retries		10					
	Timeout (s	econds)		6					
	File Path			7					
	File Name								

- Step 2 Under File Type, select Web Auth Bundle.
- **Step 3** Define the IP address and file path on the TFTP server where the files reside.
- Step 4 Click Download to begin.

Be aware of these caveats when downloading a web auth bundle:

- Select **Web Auth Bundle** from the pull-down selection list to ensure that the files are stored in the correct directory on the controller.
- The **Web Auth Bundle** must be a **.tar** file of the HTML and image files associated with the custom web login page. When downloaded, the WLC un-tars the files and places them in the appropriate directory.
- The Web Auth Bundle (.tar file) cannot be larger than 1 MB.
- The file name for the HTML login page must be **login.html**.

See the following URL for more information about downloading and using customized web pages: http://www.cisco.com/en/US/docs/wireless/wcs/4.1/configuration/guide/wcssol.html#wp1065703.

Selecting an Imported Web Auth Page

To use a customized web-auth page that has been downloaded to the controller, perform the following steps:

- Step 1 Click the Security tab.
- Step 2 In the left pane, click Web auth and then Web Login Page.
- **Step 3** From the Web Authentication Type pull-down selection list, select **Customized** (Downloaded).
- **Step 4** Click **Preview** to view the downloaded page.
- **Step 5** Click **Apply** when finished. (See Figure 10-52.)

Figure 10-52 Selecting an Imported Web Auth Page

սիսիս							onfiguration Ping Logout Refrest
CISCO	<u>M</u> ONITOR <u>W</u> LANS (ONTROLLER	WIRELESS	<u>S</u> ECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP
Security	Web Login Page						Preview Apply
 AAA General RADIUS Authentication Accounting TACACS+ LDAP Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies A Ccess Control Lists IPSec Certs Wireless Protection Policies Web Auth Web Auth Web Auth Web Login Page Certificate CIDS 	Web Authentication This page allows you to co page. The Login page is p WLAN if 'Web Authentication Cisco Logo Redirect URL after login Headline Message	Ustomize the co resented to well on' is turned on Show Welcome to Cisco is ple	 us[External (F (under WLAN) Hide Hide the Cisco wire ased to provide 	Default) d (Downloade) sedirect to ext Security Polici Security Polici eless network	() ernal server) 295).	rk.	

221885

Internal Web Certificate Management

The web auth login page uses SSL for safeguarding user credentials. For simplicity, the controller uses a self-signed certificate. Because the certificate is self-signed, guest users can expect to see a pop-up alert similar to the following when they are redirected to the authentication page shown in Figure 10-53.

Figure 10-53 Web Certificate Security Alert (IE6)

Securit	Alert	
₽	Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.	
	The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.	
	The security certificate date is valid.	
	The security certificate has a valid name matching the name of the page you are trying to view.	
	Do you want to proceed?	
	Yes No View Certificate	

At this point, you can proceed by either clicking **Yes** or you can select **View Certificate** and manually install it as a trusted site. The web server uses the virtual interface IP address configured in Anchor WLC Installation and Interface Configuration, page 10-15, as its source address. If a hostname is defined along with the IP address, that host name must be resolvable by DNS so that:

- The client is redirected to the web auth page.
- The user does not encounter a web certificate error because of conflicts between hostname and host IP address.

Importing an External Web Certificate

For cases where a legitimate web certificate issued by a trusted root CA is required, one can be downloaded to the controller by performing the following steps:

Step 1 Click the Security tab.

In the left pane, click Web Auth and then Certificate. (See Figure 10-54.)

Security	Web Auther	ntication	Certificate				Apply	/	Regenerate	Certificate
 AAA General RADIUS Authentication Accounting TACACS+ LOAP Local Net Users MAC filtering Disabled Clients User Login Policies Local EAP Priority Order Access Control Lists IPSec Certs Wireless Protection Policies Web Auth Web Login Page Certificate CIDS 	Current Certificate Name: Type: Serial Number: Valid: Subject Name: Issuer Name: MD5 Fingerprint: SHA1 Fingerprint: SHA1 Fingerprint: SHA1 Certificate * * Controller must be rebooted for the new certificate to take effect.	C=US, O= C=US, O= 98:11:37:	90 6 May 31st, 00 =Cisco System =Cisco System 65:ea:07:2c:e	s Inc., OU=De	viceSSL (WebA viceSSL (WebA :e0:a4:d9:9a	:1st, 00:00:01 GMT uth), CN=1.1.1.1 uth), CN=1.1.1.1 3:f0:db:2d				
	<									

Figure 10-54 Importing an External Web Certificate

- Step 2
- Step 3 Complete the required fields for downloading the certificate.
- Step 4 Click Apply.
- Step 5 After the certificate has been downloaded, reboot the server.

Support for External Web Redirection

In some cases, an enterprise might already have deployed a web-portal system to support wired guest access or NAC functionality. If this is the case, the anchor controller can be configured to redirect wireless guest users to an external web portal using the following steps:

Step 1 Click the Security tab.

In the left pane, click Web auth and then Web Login Page. (See Figure 10-55.) Step 2

ululu cisco	Sa <u>v</u> e Configuration <u>P</u> ing Logout <u>R</u> efresh MONITOR <u>W</u> LANS <u>C</u> ONTROLLER W <u>I</u> RELESS <u>S</u> ECURITY M <u>A</u> NAGEMENT C <u>O</u> MMANDS HE <u>L</u> P
Security	Web Login Page Preview Apply
AAA General AADIUS Authentication Accounting TACACS+ LDAP Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies	Web Authentication Type External (Redirect to external server) URL https://10.20.30.41 External Web Servers Web Server IP Address Add Web Server
Local EAP	
Priority Order	
Access Control Lists	
IPSec Certs	
 Wireless Protection Policies 	
 Web Auth Web Login Page Certificate 	
► CIDS	

Figure 10-55 Supporting External Web Redirection

Step 3 Fill in the Web Server IP and URL fields.

Step 4 Click Apply.

See the following URL for more information on the use of external web servers with controller web authentication:

http://www.cisco.com/en/US/tech/tk722/tk809/technologies_configuration_example09186a008076f97 4.shtml

Anchor WLC-Pre-Authentication ACL

A pre-authentication ACL (pre-auth ACL) can be applied to the guest WLAN, which allows unauthenticated clients to connect to specific hosts or URL destinations prior to authenticating. The pre-auth ACL is applied under the guest WLAN Layer 3 Security settings and, if enabled, is performed only on the anchor WLC(s). (See Figure 10-56.)

ANs > Edit						HELP	
Seneral Security		Advanced				< Back	Apply
Layer 3 Security							
Preauthentication	O Pass O Con ACL Cisco	sthrough ditional Web Re o Open Garden					
L	Layer 3 Security	Layer 3 Security None V Web Poli Auti Pass Con Preauthentication ACL None	Layer 3 Security None Web Policy 2 Authentication Passthrough Conditional Web Re	Layer 3 Security None Web Policy 2 Authentication Passthrough Conditional Web Redirect Cisco Open Garden V None	Layer 3 Security None Web Policy 2 Authentication Passthrough Conditional Web Redirect Cisco Open Garden V None	Layer 3 Security None Web Policy 2 Authentication Passthrough Conditional Web Redirect Preauthentication ACL Cisco Open Garden	Layer 3 Security None Web Policy 2 Authentication Passthrough Conditional Web Redirect Preauthentication ACL Cisco Open Garden

Figure 10-56 WLAN Pre-authentication ACL

The specific ACL is configured under Security > Access Control Lists. (See Figure 10-57 and Figure 10-58.)

Figure 10-57 WLC Access Control Lists



Figure 10-58 Pre-Auth ACL Example

ဂျက်က cisco	MONI	itor <u>w</u>	<u>/</u> LANs <u>C</u> ONTRO	DLLEI	R W <u>I</u> RELESS	<u>S</u> I	ECURITY	MANAGEMENT	Sa <u>v</u> e Col C <u>O</u> MMANDS	nfiguration HE <u>L</u> P	n <u>P</u> ing L	.ogout <u>R</u> efi
Security	Acce	ess Cor	ntrol Lists > Ec	lit					< Ba	c k	Add New	Rule
 AAA General RADIUS Authentication Accounting 	Gene Acces	e ral is List Nam	ne Cisco -	Open	Garden							
▶ TACACS+	Seq	Action	Source IP/Ma	sk	Destination IP/Mask		Protocol	Source Port	Dest Port	DSCP	Direction	
LDAP Local Net Users MAC Filtering	1	Permit	10.20.31.0 255.255.255.0	7	0.0.0.0 0.0.0.0	/	UDP	Any	DNS	Any	Any	
Disabled Clients User Login Policies AP Policies	_2	Permit	0.0.0.0	/	10.20.31.0 255.255.255.0	/	UDP	DNS	Any	Any	Апу	
Local EAP	_3	Permit	10.20.31.0 255.255.255.0	/	171.71.181.19 255.255.255.255	1	ТСР	Any	нттр	Any	Апу	
 Priority Order Access Control Lists 	4	Permit	171.71.181.19 255.255.255.25	5	10.20.31.0 255.255.255.0	/	ТСР	НТТР	Any	Any	Any	
Access Control Lists CPU Access Control Lists												



If a pre-authentication ACL is used in conjunction with the web auth policy, it must include a rule to permit DNS requests; otherwise, the client is unable to resolve and connect to a destination host/URL that is otherwise allowed by the ACL.

Anchor Controller DHCP Configuration

If the anchor controller is going to manage DHCP services for the guest access WLAN, proceed with the steps below.



The anchor controller cannot be used to manage DHCP services if guest N+1 redundancy is being implemented, because there is no mechanism to synchronize address leases for a single guest VLAN/subnet across two or more WLCs.

Adding a New DHCP Scope to the Anchor Controller

- **Step 1** Click the **Controller** tab.
- Step 2 In the left pane, click Internal DHCP Server.
- Step 3 Click New. (See Figure 10-59.)

Figure 10-59 Adding a New DHCP Scope

սիսիս							Sa <u>v</u> e Col	nfiguration	l <u>P</u> ing	Lo <u>q</u> out <u>R</u> efr	esh
CISCO	<u>M</u> ONITOR	<u>W</u> LANs	<u>C</u> ONTROLLER	W <u>I</u> RELESS	<u>S</u> ECURITY	MANAGEMENT	C <u>O</u> MMANDS	HE <u>L</u> P			
Controller	DHCP So	copes						New			
General	Scope Na	me	Addres	s Pool	Lea	ase Time	Status				
Inventory											
Interfaces											
Network Routes											
Internal DHCP Server											
Mobility Management											

Defining a Scope Name

Step 4 Define a name for the scope and click **Apply**. (See Figure 10-60.)

Figure 10-60 Defining a Scope Name

սիսիս								Configuration <u>P</u> ing Lo <u>g</u> out <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		
Controller	DHCP Sc	ope > N	ew					< Back	Apply	
General	Scope Na	me Guest	t Scope							
Inventory										
Interfaces										
Network Routes										
Internal DHCP Server										
Mobility Management										

Step 5 Click Scope Name to edit. (See Figure 10-61.)

221960

սիսիս								nfiguration <u>P</u>	ing Logout <u>R</u> efre
CISCO	MONITOR	<u>W</u> LANs		WIRELESS	<u>S</u> ECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	
Controller	DHCP Sco	pes						New	l
General	Scope Name	e	Add	lress Pool		Lease Time		Status	
Inventory	Guest Scope		0.0.	0.0 - 0.0.0.0		1 d		Disabled	
Interfaces									
Network Routes									
Internal DHCP Server									
Mobility Management									

Figure 10-61 Editing DHCP Scope

Defining Scope Properties

Step 6 Define the following minimum information:

- Pool start and stop
- Network
- Mask
- Default routers
- DNS servers
- Step 7 For Status, select Enabled and click Apply. (See Figure 10-62.)

Figure 10-62 Configuring and Enabling Scope Properties

սիսիս						nfiguration <u>P</u> ing	Logout <u>R</u> efresh
cisco	MONITOR WLANS CONTR	ROLLER W <u>I</u> RELESS	<u>s</u> ecurity M <u>A</u>	NAGEMENT	C <u>O</u> MMANDS	HELP	
Controller	DHCP Scope > Edit					< Back	Apply
General	Scope Name	Guest Scope					
Inventory	Pool Start Address	10.20.31.100					
Interfaces Network Routes	Pool End Address	10.20.31.200					
Internal DHCP Server	Network	10.20.31.0					
Mobility Management	Netmask	255.255.255.0					
Spanning Tree Ports	Lease Time (seconds)	86400					
Master Controller	Default Routers	10.20.31.1	0.0.0		0.0.0		
Mode	DNS Domain Name						
Network Time Protocol	DNS Servers	171.68.226.120	171.70.168	.183	0.0.0		
QoS	Netbios Name Servers	0.0.0	0.0.0		0.0.0		
CDP	Status	Disabled V Enabled Disabled					

External Radius Authentication

As described in Guest User Authentication, page 10-11, an external RADIUS server can be used to authenticate guest users in place of creating and storing guest credentials locally on the anchor controller. If this method is used, the lobby admin features described in Guest Account Management, page 10-29 cannot be used. It is assumed that some other guest management system will be used in conjunction with the external RADIUS server.

To configure a guest WLAN to use an external RADIUS server, perform the following configuration steps on the anchor controller.

Adding a RADIUS Server

Step 1 Click the Security tab.

A summary screen is displayed. (See Figure 10-63.)

Figure 10-63 Summary Screen

 cısco	MONITOR	<u>W</u> LANs	<u>C</u> ONTROLLER	. WIRELESS		MANAGEMENT	Sa <u>v</u> e Conf C <u>O</u> MMANDS	iguration HE <u>L</u> P	<u>P</u> ing Log	gout <u>R</u> efresh
Security	RADIUS	Authentic	ation Serve	rs				Appl	y Ne	ew
▼ AAA General ▼ RADIUS	Call Stat	ion ID Type	IP Address	*						
Authentication	Credenti	ials Caching	3 🗖							
Accounting TACACS+ LDAP Local Net Users	Use AES	Key Wrap	🔲 (Design	ed for FIPS custom	iers and rec	quires a key wrap o	ompliant RADIU	S server)		
MAC Filtering Disabled Clients	Network User	Manageme	Server nt Index	Server Address	Port	IPSec	Adm	in Status		
User Login Policies AP Policies		~	1	10.20.30.16	1812	Disabled	Enab	led		
Local EAP		\checkmark	2	10.20.30.15	1812	Disabled	Enab	led		
Priority Order										

Step 2 Click New.

The screen shown in Figure 10-64 appears.

Figure 10-64 Defining RADIUS Server Settings

ahaha					Sa <u>v</u> e Co	nfiguration Ping	Logout <u>R</u> efresh
cisco	MONITOR WLANS CONTRO	LLER WIRELESS	<u>S</u> ECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	
Security	RADIUS Authentication Se	ervers > New				< Back	Apply
Security • AAA General • RADIUS Authentication Accounting • TCACS+ LDAP Local Net Users MAC Filtering Disabled Clents User Login Policies AP Policies • Local EAP • Priority Order • Access Control Lists • IPSec Certs • Wireless Protection • Policies • Web Auth • CIDS	Server Index (Priority) Server IPAddress Shared Secret Format Shared Secret Confirm Shared Secret Key Wrap Port Number Server Status Support for RFC 3576 Retransmit Timeout	3 V 10.20.30.17 ASCII V ••••••• •(Designed for 1812 Enabled V Enabled V 2 seconds	FIPS customer	s and requires a k	ey wrap complia	< Back	Αρρίγ
	Network User Management	🗆 Enable					
	Network User	Enable					
	IPSec	🗌 Enable					

221908

Step 3 To define RADIUS server settings, configure the IP address, shared secret, and authentication port number as defined on the RADIUS server.

If the Network User check box is cleared, the RADIUS server is used only for user authentication when it is specifically selected under the RADIUS setting of a given WLAN. Otherwise, if the Network User check box is checked, the server is used globally for all user authentications based on its server priority.

Step 4 Click Apply.

The summary screen shown in Figure 10-65 shows the newly-added server.

Figure 10-65 Summary Screen

MONITOR	<u>W</u> LANS <u>C</u> C	ONTROLLER	WIRELESS		MANAGEMENT	COMMANDS	HELP	ng Lo <u>q</u> out <u>R</u> efresh
RADIUS	Authenticati	ion Server	ſS				Apply	New
Credentia	als Caching		ed for FIPS custom	ers and req	uires a key wrap c	ompliant RADIUS	S server)	
Network User	Management	Server Index	Server Address	Port	IPSec	Admi	in Status	
	v	1	10.20.30.16	1812	Disabled	Enabl	ed 🔽	Ī
	V	2	10.20.30.15	1812	Disabled	Enabl	ed 🔽	Ē.
		3	10.20.30.17	1812	Disabled	Enabl	ed 🔽	- -
	Call Stati Call Stati Use AES I Network User	RADIUS Authenticat Call Station ID Type Credentials Caching Use AES Key Wrap Network User Management	RADIUS Authentication Server Call Station ID Type IP Address Credentials Caching	RADIUS Authentication Servers Call Station ID Type IP Address Credentials Caching Use AES Key Wrap (Designed for FIPS custom) Network Server User Management Index Server Address Imagement 1 1 10.20.30.16 Imagement 2	RADIUS Authentication Servers Call Station ID Type IP Address Credentials Caching Use AES Key Wrap User Management Index Server Address I 10.20.30.16 1812 Image: 2 10.20.30.15 1812	RADIUS Authentication Servers Call Station ID Type IP Address Credentials Caching Use AES Key Wrap (Designed for FIPS customers and requires a key wrap or Network User Management Index Server Address Port IPSec Image:	RADIUS Authentication Servers Call Station ID Type IP Address Credentials Caching Image: Credentials Caching Use AES Key Wrap (Designed for FIPS customers and requires a key wrap compliant RADIUS) Network Server User Management Index Server Address Image: Ima	Apply Apply Call Station ID Type IP Address Credentials Caching Image: Credentials Caching Use AES Key Wrap (Designed for FIPS customers and requires a key wrap compliant RADIUS server) Network Server Server Address Port IPSec Admin Status Image: Im

Step 5 To select a RADIUS server, click the **WLANs** tab.

The screen shown in Figure 10-66 appears.

uluulu cisco	MONITOR WLANS	<u>C</u> ontroller W <u>I</u> RI	ELESS <u>S</u> ECURITY	Sa <u>v</u> e M <u>A</u> NAGEMENT C <u>O</u> MMAN	Configuration <u>P</u> ing Logout DS HE <u>L</u> P	<u>R</u> efr
LANs	WLANs				New	
WLANs WLANs	Profile Name	WLAN ID	WLAN SSID	Admin Status	Security Policies	
AP Groups VLAN	SRND	1	SRND	Enabled	802.1X	
	WEP	2	WEP	Enabled	WEP	
	CCKM	3	ССКМ	Enabled	[WPA + WPA2][Auth(802.1X)]	
	PKC	4	РКС	Enabled	[WPA + WPA2][Auth(802.1X)]	
	WPA	5	WPA	Enabled	[WPA + WPA2][Auth(PSK)]	
	Guest	6	Guest	Enabled	Web-Auth, MAC Filtering	
	Guest2	7	Guest2	Enabled	Web-Auth, MAC Filtering	

Figure 10-66 WLANs Tab

Step 6 Find the guest WLAN and click on its Profile Name.

The guest WLAN configuration screen is displayed, as shown in Figure 10-67.

221910

Ns ANs	WLANs > Edi General	Security Q	S Adv	anced				< Back	Apply
LANs 9 Groups VLAN	Layer 2	Layer 3 A	AA Server	5					
	Select AAA	servers below t	o override	use of default servers	on this !	WLAN			
	Radius Serv	vers			L	DAP Serve	rs		
		Authentication 9	ervers	Accounting Servers		Server 1	None 💌		
				Enabled		Server 2	None 💙		
	Server 1	IP:10.20.30.17,	Port:1812 🔽	None	*	Server 3	None 💙		
	Server 2	None	~	None	~				
	Server 3	None	~	None	*				
	Local EAP #	Authentication							
	Local EAF	9 Authentication	Enabled						

Figure 10-67 Guest WLAN Configuration Screen

- Step 7 Select AAA Servers under the WLAN Security tab
- **Step 8** Select the RADIUS server to be used for web authentication from the pull-down selection list under Authentication Servers.

External Access Control

The centralized guest access topology described in this chapter can be integrated with an external access control platform such the Cisco NAC Appliance.

In this scenario, an enterprise might have already deployed an access control platform in their Internet DMZ to support wired guest access services (see Figure 10-68).



Figure 10-68 Wireless Guest Access with External Access Control

As shown in Figure 10-68, the wireless guest access topology remains the same except that the guest VLAN interface on the anchor controller, instead of connecting to a firewall or border router, connects to an inside interface on an access control platform such as the Cisco NAC Appliance.

In this scenario, the NAC Appliance is responsible for redirection, web authentication, and subsequent access to the Internet. The campus and anchor controllers are used only to tunnel guest WLAN traffic across the enterprise into the DMZ, where the NAC appliance or some other platform is used to control guest access.

Configuration of the guest WLAN, campus, and anchor controllers is the same as described in the previous examples. The only exception is that Layer 3 web policy is not enabled under the guest WLAN security settings (see Figure 10-69 and Figure 10-70).



սիսիս	Sa <u>v</u> e Configuration <u>P</u> ing Logou	ut <u>R</u> efresh
CISCO	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP	
WLANs • WLANs	WLANs > Edit General Security QoS Advanced	pply
WLANS AP Groups VLAN	Layer 2 Layer 3 AAA Servers	040400

iliilii cisco	MONITOR WLANS	<u>C</u> ONTROLLER	WIRELESS	<u>S</u> ECURITY	MANAGEMENT	Sa <u>v</u> e Co C <u>O</u> MMANDS	nfiguration <u>P</u> ing HELP	Logout <u>R</u> efres
WLANs	WLANs > Edit						< Back	Apply
WLANS WLANS AP Groups VLAN	General Secu Layer 2 Lay Layer 2 Securi	er 3 AAA Se	~	<u> </u>				

Figure 10-70 Guest WLAN L2 Security Settings

The configurations above establishes a WLAN with no security policies. Guest traffic passes through the anchor controller to the inside or untrusted interface of the Cisco NAC Appliance, where it is blocked until the user has authenticated.

DHCP can be hosted locally on the controller or externally via the NAC Appliance or dedicated server.

Its beyond the scope of this chapter to address Cisco NAC Appliance or other external access control platform specific configurations. See the specific platform documentation for additional configuration guidelines.

Verifying Guest Access Functionality

The guest access service is working correctly if a user:

- · Can associate to the guest WLAN
- Receives an IP address via DHCP
- Opens their browser and is redirected to the web authentication page
- Enters their credentials and connects to the Internet (or other authorized upstream services)

Troubleshooting Guest Access

The following verifications and troubleshooting tasks assume the following:

- The solution is using the web authentication functionality resident in the anchor controller(s).
- User credentials are created and stored locally on the anchor controller(s).

Before attempting to troubleshoot the various symptoms below, at the very least you should be able to ping from the campus (foreign) controller to the anchor controller(s). If not, verify routing.

Next, you should be able to perform the following advanced pings. These can only be performed via the serial console interfaces of the controllers:

• mping neighbor WLC ip

This pings the neighbor controller through the LWAPP control channel.

• eping neighbor WLC ip

This pings the neighbor controller through the LWAPP data channel.

If a standard ICMP ping goes through, but mpings do not, ensure that the default mobility group name of each WLC is the same, and ensure that the IP, MAC, and mobility group name of each WLC is entered in the mobility members list of every WLC.

If pings and mpings are successful, but epings are not, check the network to make sure that IP protocol 97 (Ethernet-over-IP) is not being blocked.

User Cannot Associate to the Guest WLAN

- Verify that the guest WLAN is enabled on the anchor controller and all foreign controllers that support the guest WLAN
- Verify that the guest WLAN SSID is being broadcast.
- Verify client adapter/software configuration.

User Does Not Obtain an IP Address via DHCP

- Verify that WLAN configuration settings are identical on the anchor and foreign controllers (except for WLAN interface and mobility anchors; see Guest WLAN Configuration on the Anchor WLC, page 10-27)
- Verify that the guest WLAN is enabled on the anchor WLC(s)
- Check for a proper DHCP server address under the guest VLAN interface settings on the anchor controller(s)
 - If using an external DHCP server, the IP address should be that of the external server.
 - Verify reachability to the external DHCP server from the anchor controller.
 - If using the anchor controller for DHCP services, the DHCP server IP address should be the management IP address of the controller.
 - Verify that a DHCP scope has been configured and enabled on the controller.
 - Verify that the network mask of the DHCP scope is consistent with the mask on the guest VLAN interface.
 - Verify that the DHCP scope does not overlap with any addresses assigned to the network infrastructure.

User is Not Redirected to Web Auth Page

The following assumes the user is able to associate to the guest WLAN and obtain an IP address:

- Verify that valid DNS servers are being assigned to the client via DHCP.
- Ensure that the DNS servers are reachable from the anchor controller.
- Verify that the URL being opened in the web browser is resolvable.
- Verify that the URL being opened in the web browser is connecting to HTTP port 80.



• The internal web auth server does not redirect incoming requests on ports other than 80 and one other user defined port number (see User Redirection, page 10-9).

User Cannot Authenticate

• Verify that user credentials are active on the anchor controller(s).

Guest credentials typically have a lifetime associated with them. If the credentials have expired, they do not appear under the Security > Local Net Users list on the anchor controller. Use WCS to re-apply the user template or re-create user credentials locally on the controller. See Guest Management Using WCS, page 10-30 and Guest Credentials Management, page 10-10.

• Verify user password.

User Cannot Connect to Internet or Upstream Service

- Verify routing to and from the anchor controller from the firewall or border router connecting to the anchor controller(s)
- Verify NAT configuration on firewall or Internet border router (if applicable)

System Monitoring

Following are some monitoring commands that might be helpful in troubleshooting.

Anchor Controller

From the serial console port:

Cisco Controller)	>show client summar	У				
Number of Clients.		1				
MAC Address	AP Name	Status	WLAN	Auth	Protocol	Port
00:40:96:ac:5f:f8	10.15.9.19	Associated	3	Yes	Mobile	1

Note that the protocol is mobile. The Auth field reflects the actual status of the user. If the user has passed web auth, the field displays YES. If not, the field shows NO.

Also notice the AP name. This is the management IP address of the foreign controller (originating controller).

From the summary information, use the client MAC to show more detail:

(Cisco Controller) >show client detail 00:40:96:ac:5f:f8
Client MAC Address
Client Username romaxam
AP MAC Address
Client State Associated
Wireless LAN Id 3
BSSID
ChannelN/A
IP Address 10.20.31.100
Association Id0
Authentication Algorithm Open System
Reason Code 0
Status Code 0
Session Timeout
Client CCX version No CCX support
Mirroring Disabled
QoS Level Silver
Diff Serv Code Point (DSCP) disabled
802.1P Priority Tag disabled
WMM Support Disabled
Mobility State Anchor
Mobility Foreign IP Address 10.15.9.19
Mobility Move Count 1
Security Policy Completed Yes
Policy Manager State RUN
Policy Manager Rule Created Yes
NPU Fast Fast Notified Yes
Policy TypeN/A

Encryption Cipher	
Management Frame Protection	
ЕАР Туре	
Interface	wlan-user
VLAN	31
Client Capabilities:	
CF Pollable	Not implemented
CF Poll Request	Not implemented
Short Preamble	Not implemented
PBCC	Not implemented
Channel Agility	Not implemented
Listen Interval	0
Client Statistics:	
Number of Bytes Received	0
Number of Bytes Sent	0
Number of Packets Received	0
Number of Packets Sent	0
Number of Policy Errors	0
Radio Signal Strength Indicator	Unavailable
Signal to Noise Ratio	Unavailable
Nearby AP Statistics:	
TxExcessiveRetries: 0	
TxRetries: 0	
RtsSuccessCnt: 0	
RtsFailCnt: 0	
TxFiltered: 0	
TxRateProfile: [0,0,0,0,0,0,0,0,0,0,0,0,0]	

The same information can be obtained through the web configuration and management interface of the controller under Clients > Detail. (See Figure 10-71.)

،، ،،، ،، cısco	MONITOR WLANS CONTI	ROLLER W <u>I</u> RELESS <u>S</u> EC		Sa <u>v</u> e Configuration <u>P</u> ing Logout <u>R</u> efres MANDS HELP		
Monitor	Clients > Detail		< Back	Apply Link Test Remove		
Summary	Client Properties		AP Properties			
Statistics	MAC Address	00:40:96:ac:5f:f8	AP Address	Unknown		
CDP	IP Address	10.20.31.100	AP Name	10.15.9.19		
Wireless	Client Type	Regular	АР Туре	Mobile		
	User Name	romaxam	WLAN Profile	Guest2 Associated		
	Port Number	1	Status			
	Interface	wlan-user	Association ID	0		
	VLAN ID	31	802.11 Authentication	Open System		
	CCX Version	Not Supported	Reason Code	0		
	E2E Version	Not Supported	Status Code	0		
	Mobility Role	Export Anchor	CF Pollable	Not Implemented		
	Mobility Peer IP Address	10.15.9.19	CF Poll Request	Not Implemented		
	Policy Manager State	RUN	Short Preamble	Not Implemented		
	Mirror Mode	Disable 💌	PBCC	Not Implemented		
	Management Frame Protection	No	Channel Agility	Not Implemented		
	Security Information		Timeout	0		
			WEP State	WEP Disable		
	Security Policy Completed	Yes				
	Policy Type	N/A				
	Encryption Cipher	None				
	ЕАР Туре	N/A				
	Quality of Service Proper	ties				
	WMM State	Disabled				

Figure 10-71 Anchor WLC Monitor > Client Detail

Campus (Foreign) Controller

From the serial console port:

(WiSM-slot3-1) >sh	ow client summary					
Number of Clients.		2				
MAC Address	AP Name	Status	WLAN	Auth	Protocol	Port
00:40:96:ac:5f:f8	AP318e5.7fdc	Associated	1	Yes	802.11g	29

Note that the protocol field is 802.11g, whereas the protocol field on the anchor controller for the same client is mobile. The campus (foreign) controller always shows the user as authenticated and the AP name reflects the actual AP to which the client is associated.

Additional details can be obtained using the following:

(WiSM-slot3-1) >show client detail 00:40:96:ac:5f	•f8
Client MAC Address	
Client Username	
AP MAC Address	- ,
Client State	
Wireless LAN Id	
BSSID	
Channel	
IP Address	
Association Id	
Authentication Algorithm	
Reason Code Status Code	
Session Timeout	
Client CCX version	
Mirroring	
QoS Level	
Diff Serv Code Point (DSCP)	
802.1P Priority Tag	
WMM Support	
Mobility State	
Mobility Anchor IP Address	
Mobility Move Count	
Security Policy Completed	
Policy Manager State	
Policy Manager Rule Created	
NPU Fast Fast Notified	
Policy Type	
Encryption Cipher	
Management Frame Protection	
EAP Type	
Interface	-
VLAN	9
Client Capabilities:	Make involution and a d
CF Pollable	
CF Poll Request	
Short Preamble	
PBCC	
Channel Agility	-
Listen Interval	0
Client Statistics:	200244
Number of Bytes Received	
Number of Bytes Sent	
Number of Packets Received	
Number of Packets Sent	T020

The same information can be obtained through the controller web configuration and management interface under Clients > Detail (see Figure 10-72).

ဂျကျက cisco	<u>M</u> ONITOR <u>W</u> LANS <u>C</u> ONT	ROLLER WIRELESS <u>S</u> EC		Sa <u>v</u> e Configuration <u>P</u> ing Logout <u>R</u> efresh MANDS HE <u>L</u> P
Monitor	Clients > Detail		< Back	Apply Link Test Remove
Summary	Client Properties		AP Properties	
Statistics	MAC Address	00:40:96:ac:5f:f8	AP Address	00:17:df:35:86:50
CDP	IP Address	0.0.0	AP Name	AP318e5.7fdc
Wireless	Client Type	Regular	АР Туре	802.11g
	User Name		WLAN Profile	Guest2
	Port Number	29	Status	Associated
	Interface	management	Association ID	1
	VLAN ID	9	802.11 Authentication	Open System
	CCX Version	Not Supported	Reason Code	0
	E2E Version	Not Supported	Status Code	0
	Mobility Role	Export Foreign	CF Pollable	Not Implemented
	Mobility Peer IP Address	10.15.9.13	CF Poll Request	Not Implemented
	Policy Manager State	RUN	Short Preamble	Implemented
	Mirror Mode	Disable 💌	PBCC	Not Implemented
	Management Frame Protection	No	Channel Agility	Not Implemented
	Security Information		Timeout	0
			WEP State	WEP Disable
	Security Policy Completed	Yes		
	Policy Type	N/A		
	Encryption Cipher	None		
	ЕАР Туре	N/A		
	Quality of Service Prope	rties		
	WMM State	Disabled		

Figure 10-72 Foreign WLC Monitor > Client Detail

Debug Commands

Additional debug commands that might be used from the serial console include the following:

```
debug mac addr <client mac address>
debug mobility handoff enable
debug mobility directory enable
debug dhcp packet enable
debug pem state enable
debug pem events enable
debug dot11 mobile enable
debug dot11 state enable
```

