CHAPTER 12

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 and possibly 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 the guest 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 centralized controller and lightweight AP (LWAPP) architecture. 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

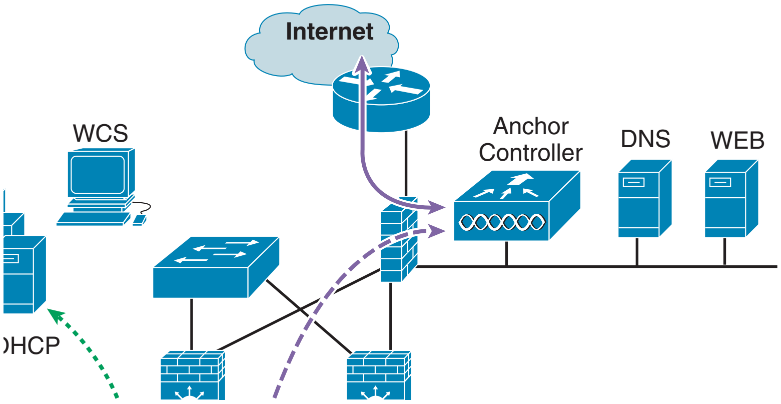
Ideally, the implementation of a wireless guest network uses as much of an enterprise's existing wireless and wired infrastructure as possible to avoid the cost and complexity of building a physical overlay network. Assuming this is the case, the following additional elements and functions are needed:

- A dedicated guest WLAN/SSID—Implemented throughout the campus wireless network wherever guest access is needed
- 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 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.

Wireless Guest Access using a Centralized Controller Architecture

The Cisco Centralized 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 WLAN controller 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 12-1 for an example of guest access topology using a centralized WLAN architecture.

Figure 12-1 Centralized Controller Guest Access



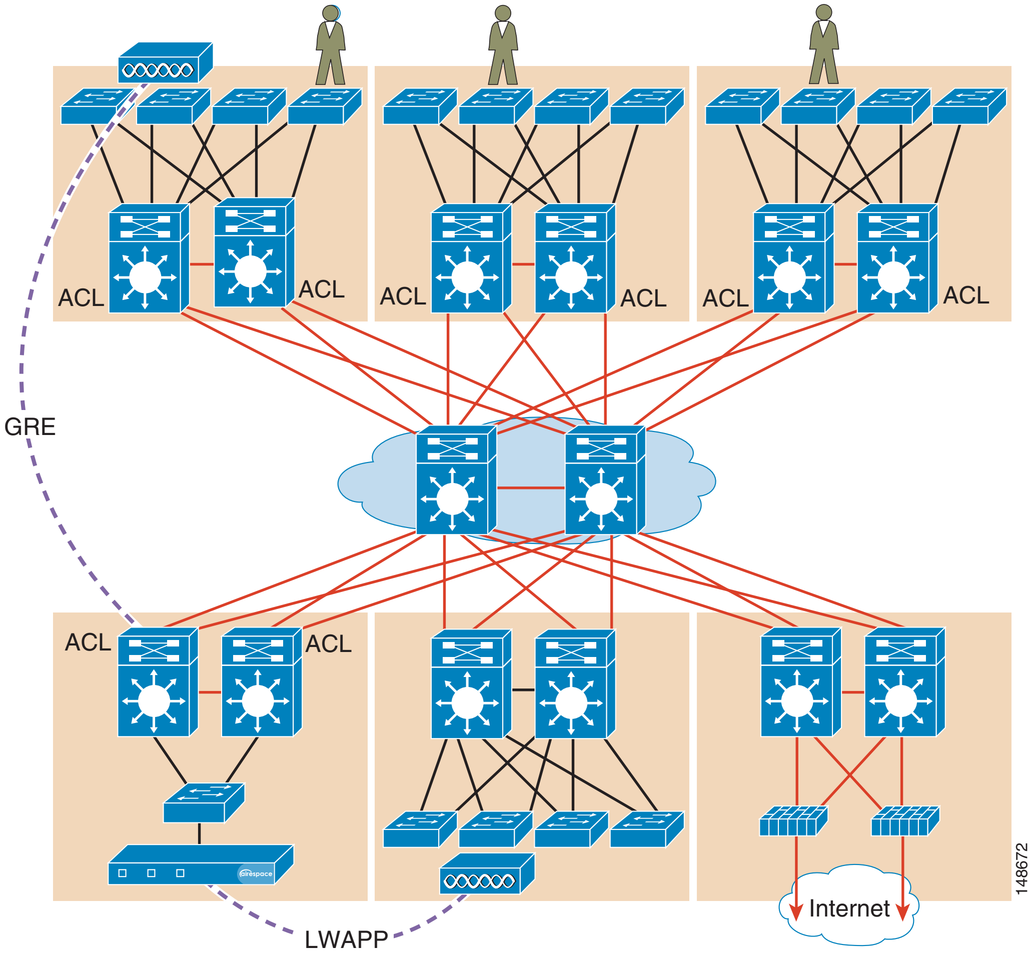
As shown in Figure 12-1, a controller is located in the enterprise's DMZ where it performs an anchor function. This anchor controller is responsible for terminating EoIP tunnels that originate from other campus WLAN controllers throughout the network. Remote controllers are responsible for termination, management, and standard operation of the various WLANs provisioned throughout the enterprise, including one or more guest WLANs. Guest WLANs, instead of being bridged locally to a corresponding VLAN, are bridged via an EoIP tunnel to the anchor controller. Specifically, guest WLAN data frames are bridged via LWAPP to the remote controller and via EoIP for the campus WLC to a guest VLAN defined at 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.

Non-Controller Based Wireless Guest Access

In place of using a centralized WLAN architecture, the biggest challenge in implementing guest access services is the segmentation (isolation) of guest traffic from the rest of the enterprise. This is especially true for wired networks or wireless networks that use autonomous (fat) APs. Some method of traffic segmentation must be implemented beginning with a separate WLAN or VLAN, coupled with a policy that is applied at the first Layer 3 hop in the network. Possible options include the following:

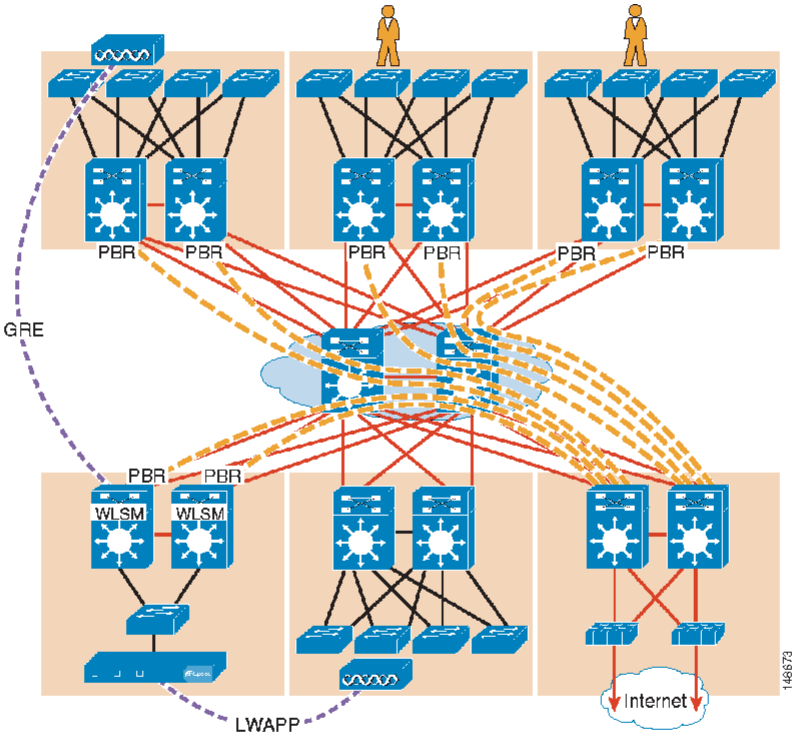
- Distributed ACLs—This method involves implementing ACLs throughout the enterprise to restrict guests from accessing network resources within the host enterprise network (see Figure 12-2).

Figure 12-2 Segmentation using Distributed ACLs



- Policy based routing (PBR) and GRE tunnels—GRE tunnels are used to create a logical overlay network through which guest traffic is directed to the Internet edge or DMZ. Policy-based routing is used to classify and enforce guest traffic into the tunnels. Companies that have deployed, or are looking to deploy, a PBR/GRE should seriously consider, if at all possible, VRF-lite with GRE (see Figure 12-3).

Figure 12-3 Segmentation using PBR into GRE Tunnels



- VRF-Lite and GRE or mGRE tunnels—This technique is similar to the PBR/GRE method. An overlay network is created through the implementation of GRE tunnels. However, instead of policy routing traffic into the tunnels, the guest access VLAN and interfaces, along with the tunnel interfaces, are assigned to a virtual routing and forwarding (VRF) instance. This ensures guest traffic can be forwarded only through the tunnels (see Figure 12-4 and Figure 12-5).

Figure 12-4 Segmentation using VRF-lite and GRE

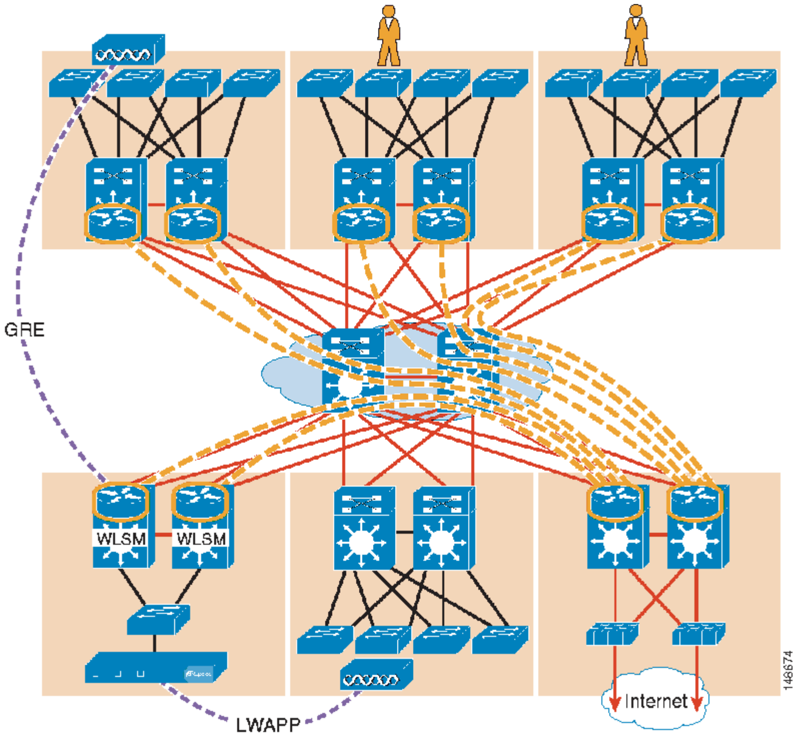
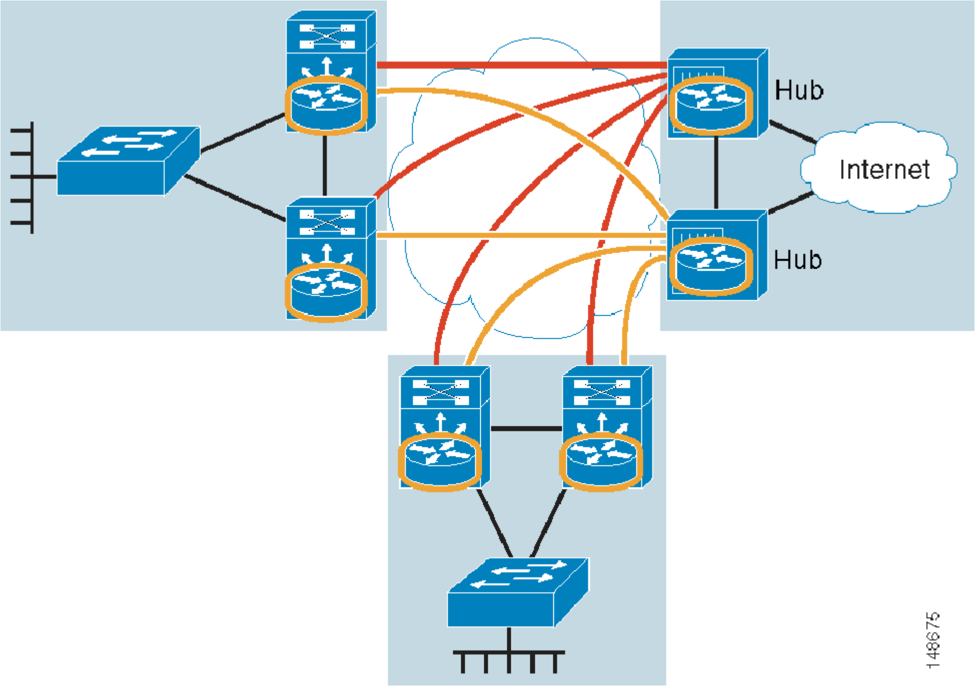


Figure 12-5 Segmentation with VRF-Lite and mGRE



Each of the methods described here has benefits and drawbacks. Additional challenges for the enterprise include the following:

- Determining which method to use
- Modifying existing topologies to accommodate a given segmentation method or introducing new versions of code into the network
- The added complexity of managing a logical overlay network

In addition, it simply might not be practical or possible for an enterprise to implement one of the segmentation methods described in this chapter. In that case, and if wireless guest access is all that is needed, deploying guest services using a centralized WLAN controller architecture is a good alternative.

Otherwise, if an enterprise requires both wireless and wired guest access, see the guest access documentation at the following URL:
http://www.cisco.com/en/US/docs/solutions/Enterprise/Network_Virtualization/GuestAcc.html.

The remainder of this chapter focuses on the implementation of wireless guest networking using the Cisco Centralized Controller solution.

Wireless Controller Guest Access

The Cisco Wireless Controller 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 that is covered 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 normal controller operations and guest tunnel origination to an anchor controller:

- Cisco WLAN Controller Module for Integrated Service Routers (ISR)
- Cisco 2000 Series

WLAN Anchors and Ethernet in IP to Support Guest Access

A key feature of the Cisco centralized controller architecture is the ability to statically map one or more provisioned WLANs to a specific controller (anchor) within the network, using an EoIP tunnel. By using this technique, a guest WLAN and all associated guest traffic can be transported transparently across the enterprise network to an anchor controller that resides in the Internet DMZ (see Figure 12-6).

Figure 12-6 Static EoIP Tunnels

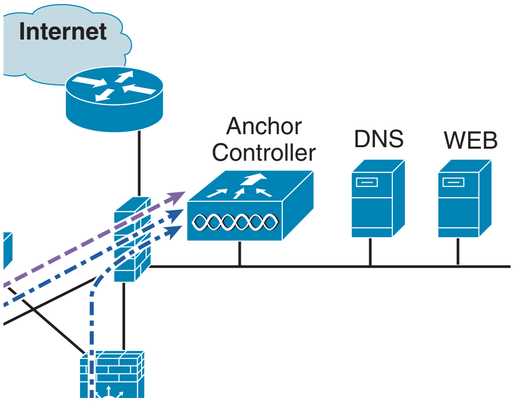
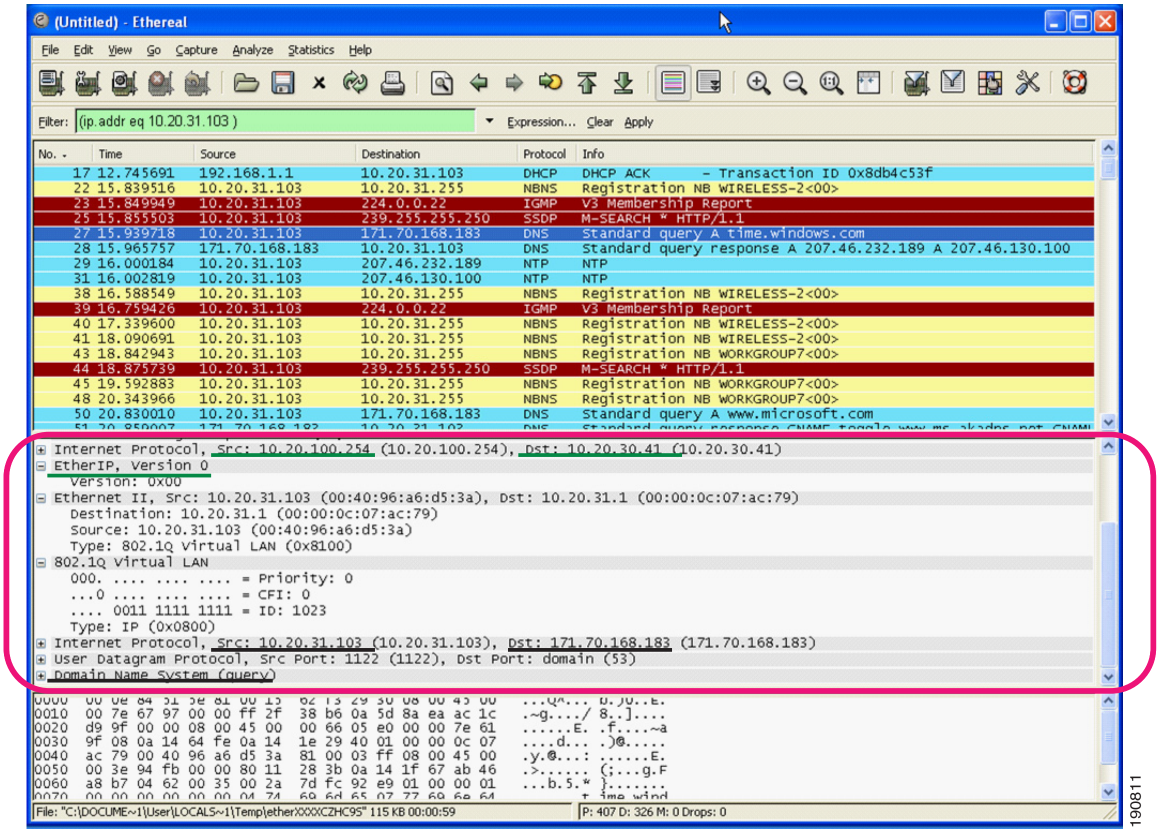


Figure 12-7 shows a sniffer trace of an Ethernet in IP tunnel (highlighted) between a branch wireless controller with a guest WLAN provisioned and an anchor controller that is performing local web authentication. The first IP detail shown represents the Ethernet in IP tunnel between the branch and anchor controllers. The second IP detail is that of guest traffic (in this case, a DNS query).

Figure 12-7 Sample Ethernet in IP Sniffer Trace



Filter: (ip.addr eq 10.20.31.103)

```
No. .  Time       Source          Destination      Protocol  Info
   17 12.745691  192.168.1.1     10.20.31.103     DHCP      DHCP ACK      - Transaction ID 0x8db4c53f
   22 15.839516  10.20.31.103    10.20.31.255     NBNS      Registration NB WIRELESS-2<00>
   23 15.849949  10.20.31.103    224.0.0.22       IGMP      V3 Membership Report
   25 15.855503  10.20.31.103    239.255.255.250  SSDP      M-SEARCH * HTTP/1.1
   27 15.939718  10.20.31.103    171.70.168.183   DNS       Standard query A time.windows.com
   28 15.965757  171.70.168.183  10.20.31.103     DNS       Standard query response A 207.46.232.189 A 207.46.130.100
   29 16.000184  10.20.31.103    207.46.232.189   NTP       NTP
   31 16.002819  10.20.31.103    207.46.130.100   NTP       NTP
   38 16.588549  10.20.31.103    10.20.31.255     NBNS      Registration NB WIRELESS-2<00>
   39 16.759426  10.20.31.103    224.0.0.22       IGMP      V3 Membership Report
   40 17.339600  10.20.31.103    10.20.31.255     NBNS      Registration NB WIRELESS-2<00>
   41 18.090691  10.20.31.103    10.20.31.255     NBNS      Registration NB WIRELESS-2<00>
   43 18.842943  10.20.31.103    10.20.31.255     NBNS      Registration NB WORKGROUP7<00>
   44 18.875739  10.20.31.103    239.255.255.250  SSDP      M-SEARCH * HTTP/1.1
   45 19.592883  10.20.31.103    10.20.31.255     NBNS      Registration NB WORKGROUP7<00>
   48 20.343966  10.20.31.103    10.20.31.255     NBNS      Registration NB WORKGROUP7<00>
   50 20.830010  10.20.31.103    171.70.168.183   DNS       Standard query A www.microsoft.com
```

```
⊞ Internet Protocol, Src: 10.20.100.254 (10.20.100.254), Dst: 10.20.30.41 (10.20.30.41)
⊟ EtherIP, Version 0
    Version: 0x00
⊟ Ethernet II, Src: 10.20.31.103 (00:40:96:a6:d5:3a), Dst: 10.20.31.1 (00:00:0c:07:ac:79)
    Destination: 10.20.31.1 (00:00:0c:07:ac:79)
    Source: 10.20.31.103 (00:40:96:a6:d5:3a)
    Type: 802.1Q Virtual LAN (0x8100)
⊟ 802.1Q Virtual LAN
    000. .... .... .... = Priority: 0
    ...0 .... .... .... = CFI: 0
    .... 0011 1111 1111 = ID: 1023
    Type: IP (0x0800)
⊞ Internet Protocol, Src: 10.20.31.103 (10.20.31.103), Dst: 171.70.168.183 (171.70.168.183)
⊞ User Datagram Protocol, Src Port: 1122 (1122), Dst Port: domain (53)
⊞ Domain Name System (query)
```

```
0010  00 7e 67 97 00 00 ff 2f  38 b6 0a 5d 8a ea ac 1c   .~g..../ 8..]....
0020  d9 9f 00 00 08 00 45 00  00 66 05 e0 00 00 7e 61   ......E. .f....~a
0030  9f 08 0a 14 64 fe 0a 14  1e 29 40 01 00 00 0c 07   ....d... .)@.....
0040  ac 79 00 40 96 a6 d5 3a  81 00 03 ff 08 00 45 00   .y.@...: ......E.
0050  00 3e 94 fb 00 00 80 11  28 3b 0a 14 1f 67 ab 46   .>...... (;...g.F
0060  a8 b7 04 62 00 35 00 2a  7d fc 92 e9 01 00 00 01   ...b.5.* }.......
```

File: "C:\DOCUME~1\User\LOCALS~1\Temp\etherXXXXCZHC9S" 115 KB 00:00:59   P: 407 D: 326 M: 0 Drops: 0

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 should be positioned in the enterprise's Internet DMZ. By 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 LWAPP APs 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 12-17 for configuration examples.

Routing

Guest traffic egress occurs at the anchor controller. Guest WLANs are mapped to a specific physical interface or VLAN on the anchor. Depending on the topology, this interface or VLAN 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 or 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 and tunnel termination functions only, the 4402 with support for 12 APs is sufficient because it is assumed the controller is not going to be used to manage LWAPP APs in the network.

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

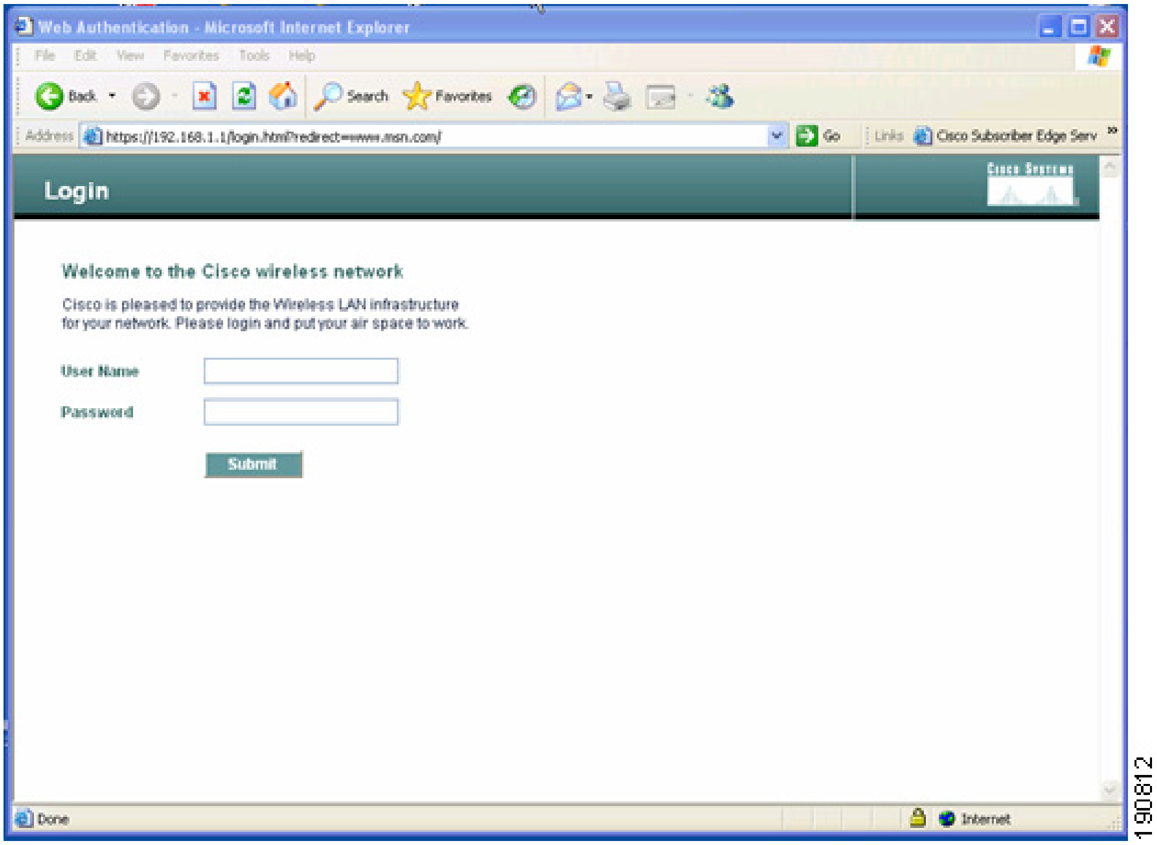
Anchor Controller Redundancy

Anchor controller redundancy is expected to be supported in future releases.

Web Portal Authentication

The Cisco Centralized Guest Access solution can make use of 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 12-8).

Figure 12-8 Controller Web Authentication Page


Web Authentication - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address
https://192.168.1.1/login.html?redirect=www.msn.com/
Go
Links
Cisco Subscriber Edge Serv
Cisco Systems
Done
Internet
190812

Login

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.

User Name

Password

Submit

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 complex 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 12-17 for web page configuration guidelines.

User Redirection

As is typical for most web-based authentication access, for guest clients to be redirected to the controller 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 before authentication. When a client associates to a web policy WLAN for authentication, all traffic is blocked except DHCP and DNS. Therefore, 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.

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

- Resolvable Home Page URL—A guest user home page URL 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 a user home page connects to a web server on a port other than HTTP port 80, they are not redirected. Again, the user needs to open a URL that uses port 80 to be redirected to the controllers 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 establish a limited privilege administrative account within WCS that permits lobby ambassador access for the purpose of creating guest credentials. The only function a lobby ambassador is permitted to do is create and assign guest credentials to a controller serving as an anchor for wireless guest access. See Guest Access Configuration, page 12-17 for configuration guidelines.

As with many configuration tasks within WCS, guest credentials are created using templates. For more information regarding administration and use of WCS, see Chapter 8, “Cisco Unified Wireless Control System.” A guest user template includes the following information:

- User name
- Auto generate password (check box) or Administrator assigned password
- Confirm password
- SSID (select box)—Only WLANs configured for Layer 3 web policy authentication are displayed
- Description
- Credentials lifetime—days:hours:minutes

After a lobby ambassador has created a guest template, it can be applied to one or more controllers. Only controllers with web policy-configured WLANs are listed as a candidate controller to which the template can be applied.

Guest credentials, when applied, are stored locally on the anchor controller and remain there until expiration of the Lifetime variable defined in the guest template. If a wireless guest is associated and active when their credentials expire, the WLAN controller stops passing traffic from that user, causing them to be disconnected. Unless the guest credentials are re-applied (to the controller), the user is no longer able to authenticate and access the network.

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

Local Controller Lobby Admin Access

In the event a centralized WCS management system is not deployed, a network administrator can establish a local user management account on the anchor controller, which has lobby admin privileges only. A person who logs in to the controller using the lobby admin account has access only to guest user management functions. Options available for local guest management are the same as for guest template creation in WCS:

- User name
- Auto generate password (check box) or administrator-assigned password
- Confirm the password
- SSID (check box)

  Only WLAs configured for Layer 3 web policy authentication are displayed.
- Description
- Credentials lifetime—days:hours:minutes

Any credentials that may have been applied to the controller by WCS are shown when an admin logs into the controller using the lobby admin account. The lobby admin account has rights to modify or delete any guest credentials that were created by WCS.

Guest User Authentication

As was previously covered in Guest Credentials Management, page 12-13, when an administrator uses WCS or a local admin 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 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 servers have network user selected, and the user has not authenticated as a result of 1 or 2 above, the 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 global settings. However, to do so, that server must be explicitly selected under a given WLANs RADIUS server settings. See External Radius Authentication, page 12-38 for a configuration example.

External Authentication

The guest account creation (Lobby Ambassador) capabilities available in WCS and locally on the controller can be used only to create and store guest user information locally on the controller. An enterprise may already have developed similar functionality in conjunction with a wired guest access or NAC-type deployment. In this 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 12-14.

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 method is configured under the general configuration settings of the controller by using the web administrative interface of the controller, or through WCS.

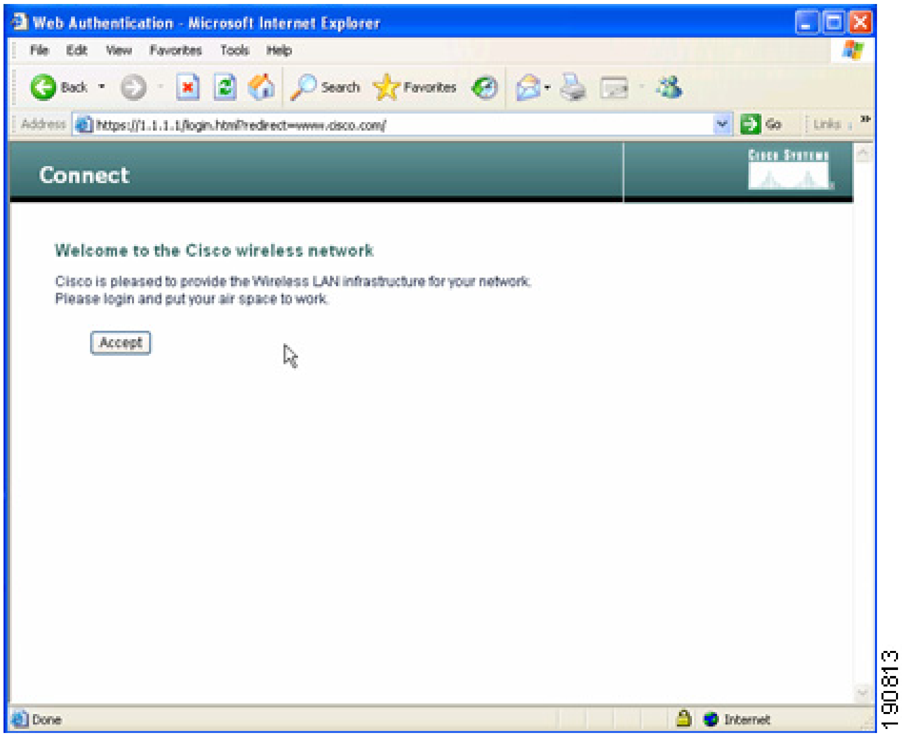
External Authentication using Cisco Secure ACS and Microsoft User Databases

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/installation/guide/windows/postin.html.

Guest Pass-through

Another variation of wireless guest access is to bypass user authentication altogether and allow open access. However, an enterprise might still want 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 12-9 and Figure 12-10 for sample pages). See Guest Access Configuration, page 12-17 for configuration examples.

Figure 12-9 Pass-through Welcome AUP Page

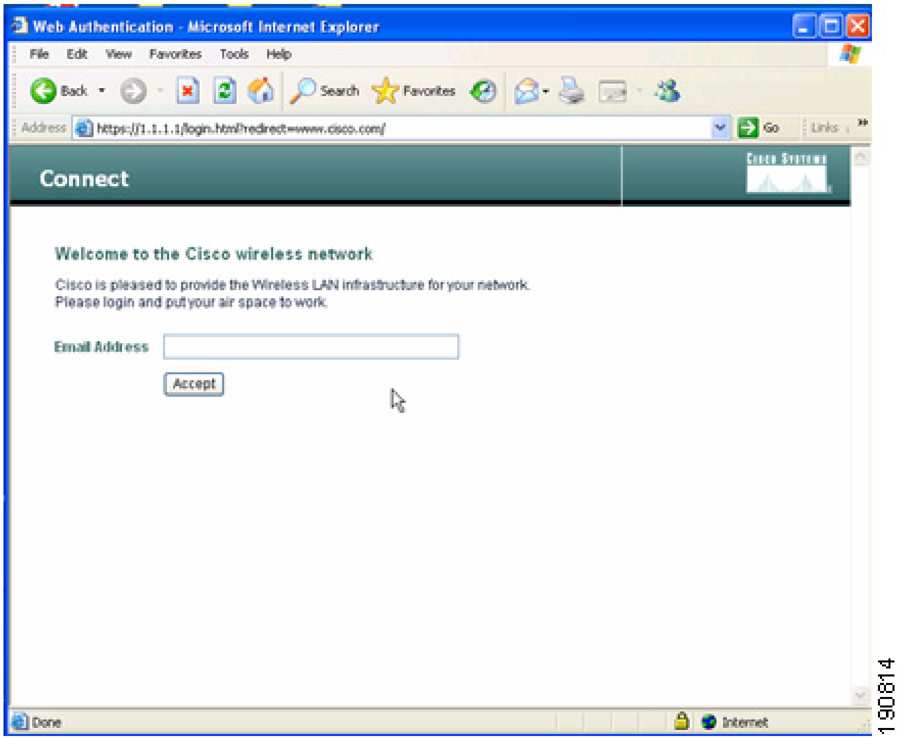

Web Authentication - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address
Go
Links
Connect
Cisco Systems
Accept
Done
Internet
190813

https://1.1.1.1/login.html?redirect=www.cisco.com/

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.

Figure 12-10 Pass-through Page with Email


Web Authentication - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address
Go
Links
Connect
Cisco Systems
Accept
Done
Internet
190814

https://1.1.1.1/login.html?redirect=www.cisco.com/

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

Guest Access Configuration

This section describes how to enable a wireless guest access service using the Cisco Centralized WLAN Controller 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 lightweight APs with the possible exception of the anchor controller platform. See Anchor Controller Deployment Guidelines, page 12-10 for more information.

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

The following references are used throughout the configuration sections:

- Remote Controller—Refers to the one or more controllers deployed in an enterprise campus or branch location that are used for managing and controlling a group of lightweight APs. Remote controllers map a guest WLAN into a static EoIP tunnel.
- Anchor Controller—Refers to a controller deployed in the enterprise DMZ that is used to perform EoIP tunnel termination, web redirection, and user authentication.

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

Anchor Controller Interface Configuration

As described in Anchor Controller Positioning, page 12-10, Cisco strongly recommends that the anchor controller be dedicated to guest access functions and not be used to control and manage lightweight APs in the enterprise.

This section does not address all aspects of interface configuration on the anchor controller. It is assumed the reader is familiar with the controller initialization and configuration process required upon initial boot-up using the serial console interface.

This section offers specific information and caveats as it pertains to configuring interfaces on a controller being deployed as an anchor in a guest access topology.

As part of the initial configuration (through serial console interface), you are required to define 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 remote controllers.

- AP Manager interface—Even though the controller is not used to manage APs, you are still required to configure this interface. The easiest thing to do is to configure the interface to be on the same VLAN and subnet as the primary management interface.

Note This would not otherwise be recommended in a traditional deployment where the controller is managing lightweight APs.

- Virtual Interface—The controller quick start 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. This virtual interface is also used as the source IP address when the controller performs 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 12-10, the guest interface will likely connect to a port on a firewall or be switched to an interface on an Internet border router.

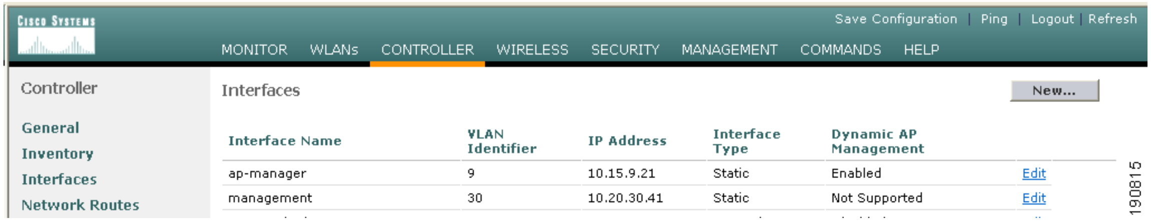
Defining a New Interface

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**. (See Figure 12-11.)

Figure 12-11 Interfaces



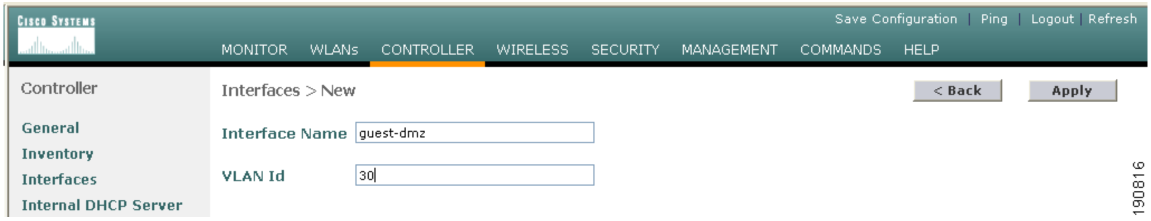
Interfaces

Interface Name	VLAN Identifier	IP Address	Interface Type	Dynamic AP Management	
ap-manager	9	10.15.9.21	Static	Enabled	Edit
management	30	10.20.30.41	Static	Not Supported	Edit

Defining an Interface Name and VLAN ID

Step 3 Enter an interface name and VLAN ID. (See Figure 12-12.)

Figure 12-12 Interface Name and VLAN ID



Interfaces > New

Interface Name: guest-dmz

VLAN Id: 30

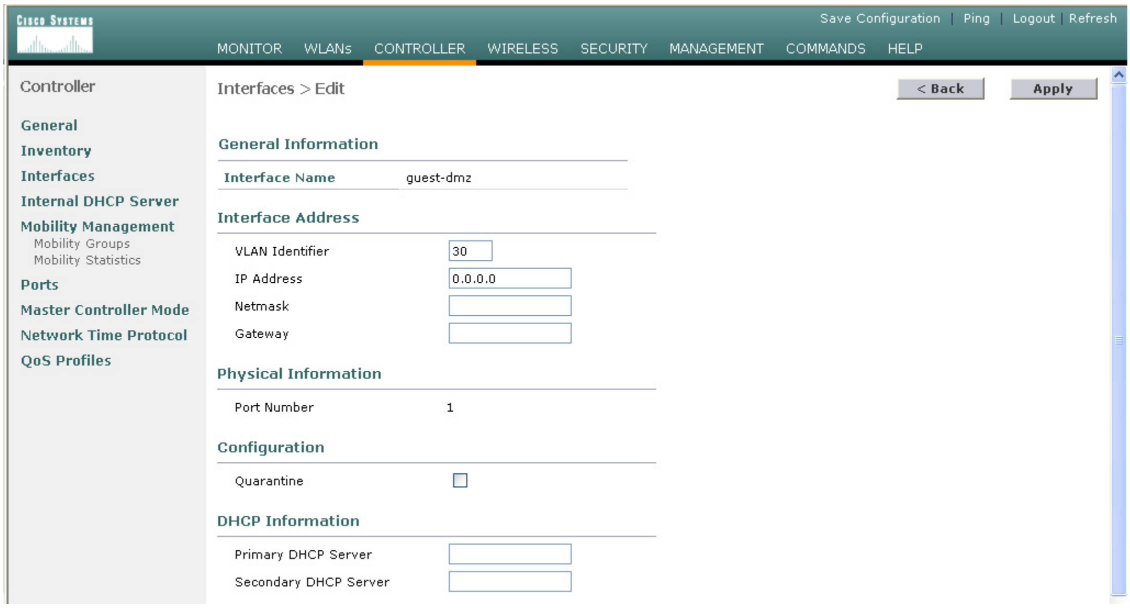
Defining Interface Properties

Step 4 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 12-13.

Figure 12-13 Defining Properties



Interfaces > Edit

General Information

Interface Name: guest-dmz

Interface Address

VLAN Identifier: 30
IP Address: 0.0.0.0
Netmask:
Gateway:

Physical Information

Port Number: 1

Configuration

Quarantine □

DHCP Information

Primary DHCP Server:
Secondary DHCP Server:

Note If DHCP services are to be managed locally on the anchor controller, populate the primary DHCP server field with the controller management IP address. See Anchor Controller Interface Configuration, page 12-17.

Anchor Controller DHCP Configuration (Optional)

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

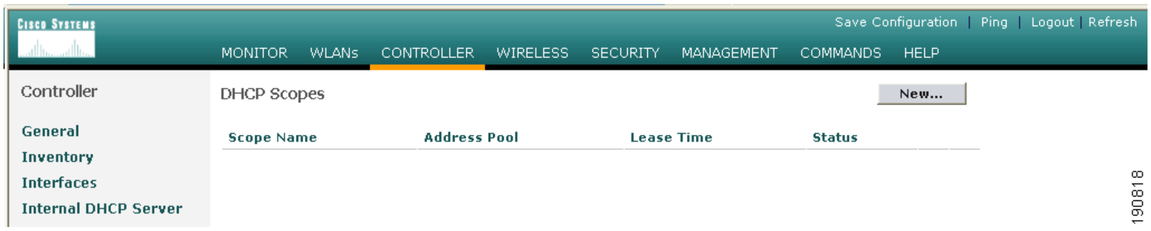
Adding a New DHCP Scope to the Anchor Controller

Step 1 Click the **Controller** tab.

Step 2 In the left pane, click **Internal DHCP Server**.

Step 3 Click **New**. (See Figure 12-14.)

Figure 12-14 Adding a New DHCP Scope



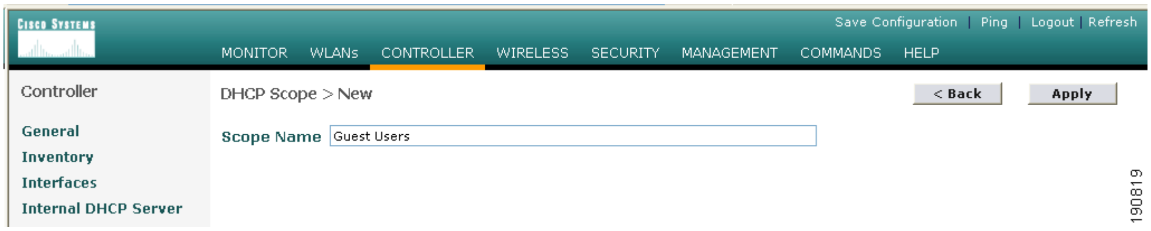
DHCP Scopes

Scope Name	Address Pool	Lease Time	Status

Defining a Scope Name

Step 4 Define a name for the scope and click **Apply**. (See Figure 12-15.)

Figure 12-15 Defining a Scope Name

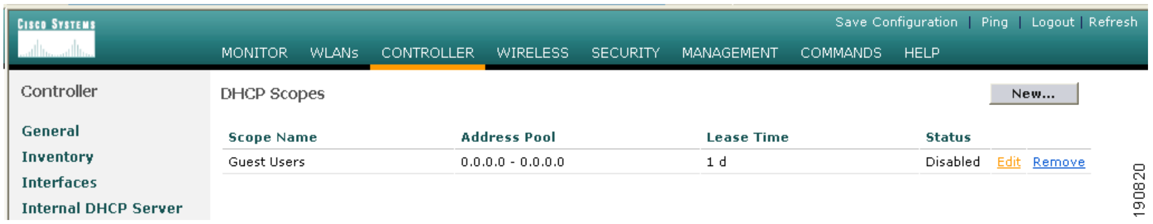


DHCP Scope > New

Scope Name: Guest Users

Step 5 Click **Edit**. (See Figure 12-16.)

Figure 12-16 Editing Scope Name



DHCP Scopes

Scope Name	Address Pool	Lease Time	Status		
Guest Users	0.0.0.0 - 0.0.0.0	1 d	Disabled	Edit	Remove

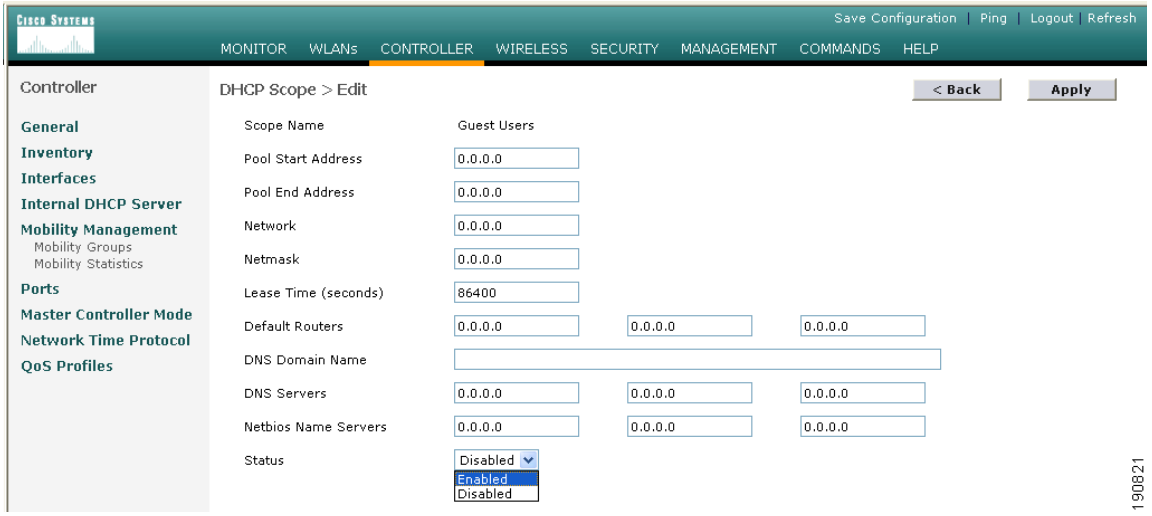
Defining Scope Properties

Step 6 Define the following minimum information:

- Pool start and stop
- Network
- Mask
- Default routers
- DNS servers

Step 7 For Status, choose **Enabled** and click **Apply**. (See Figure 12-17.)

Figure 12-17 Enabling Scope Properties



DHCP Scope > Edit

Scope Name	Guest Users		
Pool Start Address	0.0.0.0		
Pool End Address	0.0.0.0		
Network	0.0.0.0		
Netmask	0.0.0.0		
Lease Time (seconds)	86400		
Default Routers	0.0.0.0	0.0.0.0	0.0.0.0
DNS Domain Name			
DNS Servers	0.0.0.0	0.0.0.0	0.0.0.0
Netbios Name Servers	0.0.0.0	0.0.0.0	0.0.0.0
Status	Disabled Enabled Disabled		

Mobility Group Configuration

The following mobility group parameters should already be defined on the remote controllers as part of a standard centralized WLAN deployment. The anchor controller can also be configured with a mobility domain name, but it is not required to support termination of guest WLAN EoIP tunnels.

Defining a Default Mobility Domain Name for the Anchor Controller (Optional)

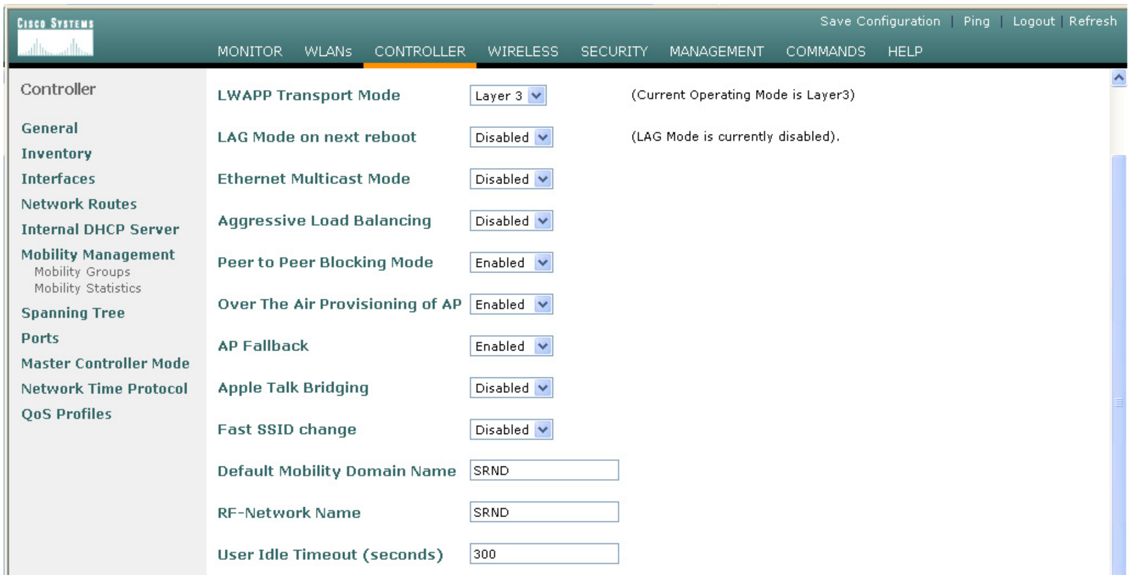
Assign a default mobility domain name for the anchor controller.

Step 1 Click the **Controller** tab.

Step 2 Enter a name in the **Default Mobility Domain Name** field.

Step 3 Click **Apply**. (See Figure 12-18.)

Figure 12-18 Defining a Default Mobility Domain Name



LWAPP Transport Mode: Layer 3 (Current Operating Mode is Layer3)
LAG Mode on next reboot: Disabled (LAG Mode is currently disabled).
Ethernet Multicast Mode: Disabled
Aggressive Load Balancing: Disabled
Peer to Peer Blocking Mode: Enabled
Over The Air Provisioning of AP: Enabled
AP Fallback: Enabled
Apple Talk Bridging: Disabled
Fast SSID change: Disabled
Default Mobility Domain Name: SRND
RF-Network Name: SRND
User Idle Timeout (seconds): 300

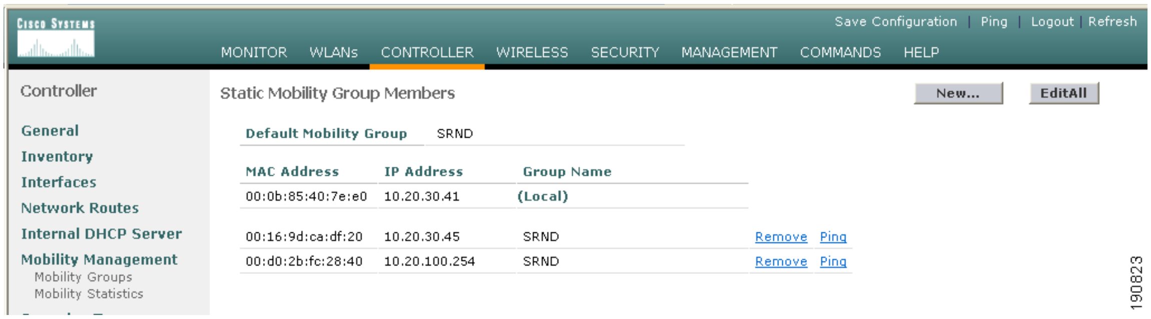
Defining Mobility Group Members for the Anchor Controller

Each campus (foreign) controller in the enterprise that will support the guest WLAN must be defined as a mobility group member in the anchor controller.

Step 1 Click the **Controller** tab.

Step 2 In the left pane, click **Mobility Groups**. (See Figure 12-19.)

Figure 12-19 Defining Mobility Group Members



Static Mobility Group Members

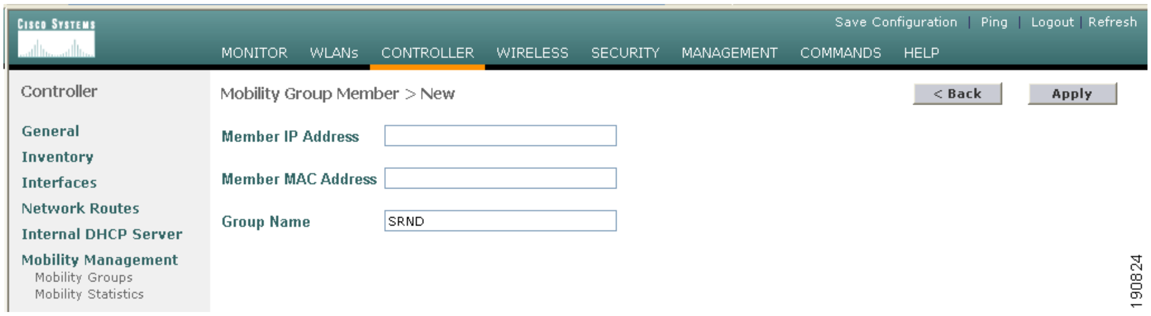
Default Mobility Group SRND

MAC Address	IP Address	Group Name	
00:0b:85:40:7e:e0	10.20.30.41	(Local)	
00:16:9d:ca:df:20	10.20.30.45	SRND	Remove Ping
00:d0:2b:fc:28:40	10.20.100.254	SRND	Remove Ping

Adding Remote Controllers as Mobility Group Members

Step 3 Click **New** to define a MAC and IP address for each remote controller that will support a guest access WLAN. (See Figure 12-20.)

Figure 12-20 Adding Remote Controllers



Mobility Group Member > New

Member IP Address

Member MAC Address

Group Name SRND

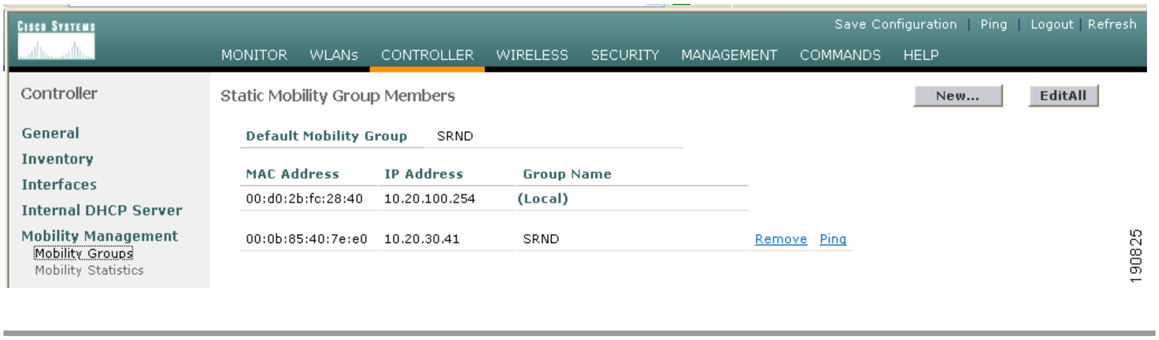
Adding an Anchor Controller as a Mobility Group Member in the Remote Controller

As described in WLAN Anchors and Ethernet in IP to Support Guest Access, page 12-8, each remote controller maps the guest WLAN into an EoIP tunnel that terminates on the anchor controller. Therefore, the anchor controller must be added as a member of the mobility group in each remote controller.

Step 1 Click **New** to add the anchor controller IP and MAC address to the mobility members table.

Step 2 Repeat these steps for each remote controller. (See Figure 12-21.)

Figure 12-21 Adding an Anchor Controller



Static Mobility Group Members

Default Mobility Group SRND

MAC Address	IP Address	Group Name
00:d0:2b:fc:28:40	10.20.100.254	(Local)
00:0b:85:40:7e:e0	10.20.30.41	SRND

Guest WLAN Configuration

The following section describes how to configure a single guest WLAN. The guest WLAN is configured on each remote controller that manages APs where guest access is required.

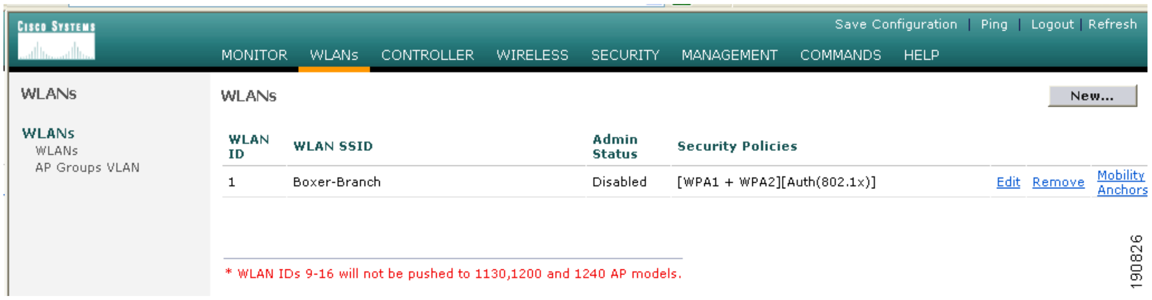
Even though the anchor controller is not specifically used to manage lightweight APs, it must also be configured with the guest WLAN because the anchor controller represents an extension of the guest WLAN where user traffic is bridged (using LWAPP between the AP and the remote controller and EoIP between the remote controller and the anchor controller) to a physical interface and VLAN.

Note The parameters defined in the WLAN policies page must be configured identically between the anchor and any given remote controller.

Guest WLAN Configuration for the Remote Controller

Step 1 Click the **WLANs** tab and then click **New**. (See Figure 12-22.)

Figure 12-22 Guest WLAN Configuration



WLANs

WLAN ID	WLAN SSID	Admin Status	Security Policies
1	Boxer-Branch	Disabled	[WPA1 + WPA2][Auth(802.1x)]

* WLAN IDs 9-16 will not be pushed to 1130,1200 and 1240 AP models.

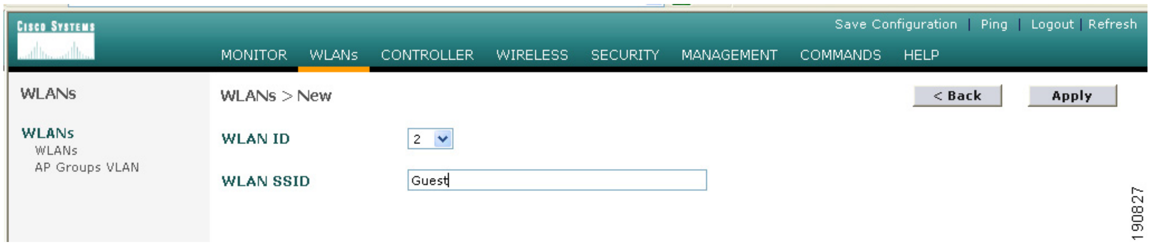
Defining a Guest WLAN SSID

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 Click **Apply**. (See Figure 12-23.)

Figure 12-23 Defining a Guest WLAN SSID



WLANs > New

WLAN ID: 2

WLAN SSID: Guest

Defining Guest WLAN Policies

The following list represents typical parameter settings used for a guest WLAN:

Step 1 Set the Layer 2 security policy to **None** (802.1x is default).

Step 2 Place a check mark in the Web Policy check box and in either the Authentication check box or Pass-through check box. See Guest User Authentication, page 12-14.

- Broadcast SSID is enabled by default.
- Session time-out default = **0**. (no time out).

  Anything greater than 0 forces de-authentication after expiration and requires the user to re-authenticate through web portal.
- No specific RADIUS servers defined. Authentication is handled by the anchor controller.
- QOS: **Best Effort**.

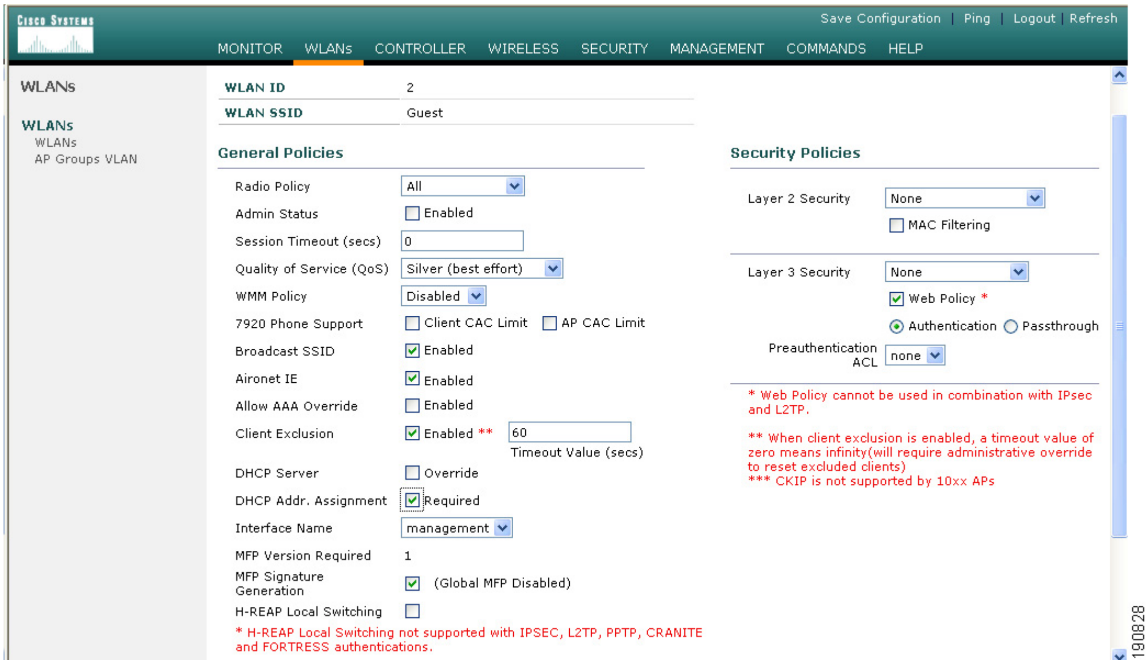
  This value can be changed.
- DHCP Addr Assignment: **Required**.

  This forces client to use DHCP. Statically configured clients are not accepted.
- Interface name: **Management**.

Note The interface name must be set to the management interface. This causes the remote controller to initiate an EoIP tunnel via its management IP.

Step 3 Click **Apply**. (See Figure 12-24.)

Figure 12-24 Defining Guest WLAN Policies



WLAN ID 2

WLAN SSID Guest

General Policies

Radio Policy	All
Admin Status	□ Enabled
Session Timeout (secs)	0
Quality of Service (QoS)	Silver (best effort)
WMM Policy	Disabled
7920 Phone Support	□ Client CAC Limit □ AP CAC Limit
Broadcast SSID	☑ Enabled
Aironet IE	☑ Enabled
Allow AAA Override	□ Enabled
Client Exclusion	☑ Enabled ** 60 Timeout Value (secs)
DHCP Server	□ Override
DHCP Addr. Assignment	☑ Required
Interface Name	management
MFP Version Required	1
MFP Signature Generation	☑ (Global MFP Disabled)
H-REAP Local Switching	□

* H-REAP Local Switching not supported with IPSEC, L2TP, PPTP, CRANITE and FORTRESS authentications.

Security Policies

Layer 2 Security	None □ MAC Filtering
Layer 3 Security	None ☑ Web Policy * ● Authentication ○ Passthrough
Preauthentication ACL	none

* Web Policy cannot be used in combination with IPsec and L2TP.

** When client exclusion is enabled, a timeout value of zero means infinity(will require administrative override to reset excluded clients)

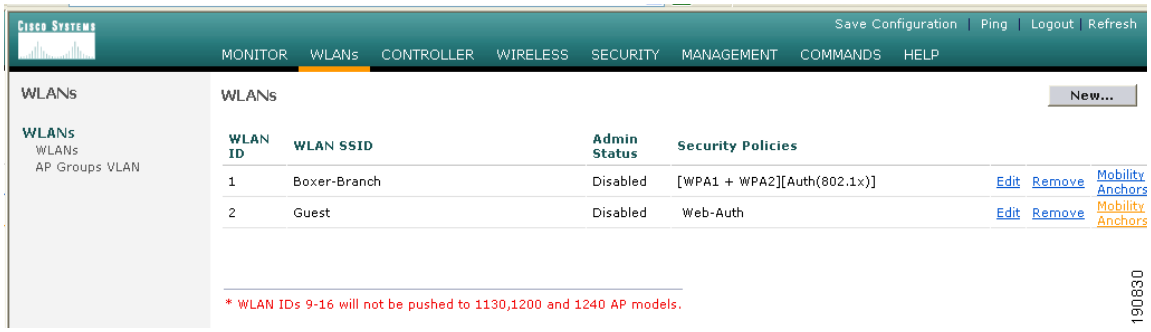
*** CKIP is not supported by 10xx APs

Defining the Guest WLAN Anchor

Step 1 From the WLAN menu, find the newly created guest WLAN.

Step 2 Click **Mobility Anchors**. (See Figure 12-25.)

Figure 12-25 Defining Guest WLAN Anchors



WLANs

WLAN ID	WLAN SSID	Admin Status	Security Policies			
1	Boxer-Branch	Disabled	[WPA1 + WPA2][Auth(802.1x)]	Edit	Remove	Mobility Anchors
2	Guest	Disabled	Web-Auth	Edit	Remove	Mobility Anchors

* WLAN IDs 9-16 will not be pushed to 1130,1200 and 1240 AP models.

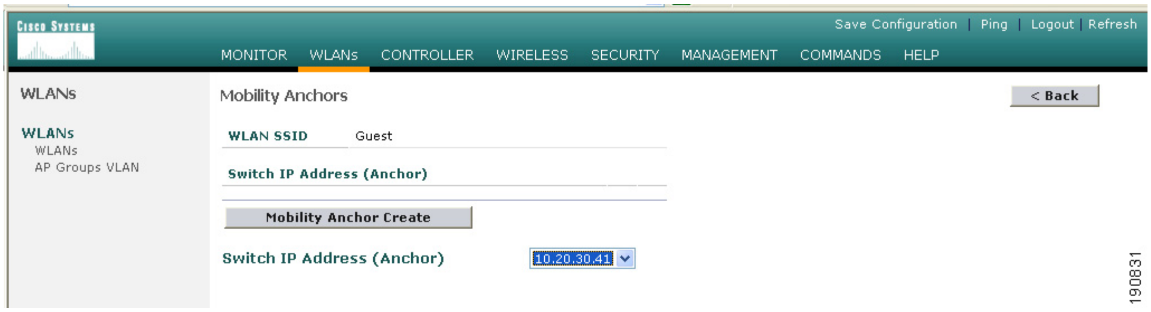
A drop-down list of eligible controller IP addresses is displayed.

Selecting and Creating an Anchor

Step 3 Select the IP address representing the guest access anchor controller deployed in the network DMZ. This is the IP address configured in Adding an Anchor Controller as a Mobility Group Member in the Remote Controller, page 12-23.

Step 4 Click **Mobility Anchor Create**. (See Figure 12-26.)

Figure 12-26 Selecting and Creating an Anchor


Cisco Systems
Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
WLANs
WLANs
WLANs
AP Groups VLAN
< Back
Mobility Anchor Create
190831

Mobility Anchors

WLAN SSID	Guest
Switch IP Address (Anchor)	

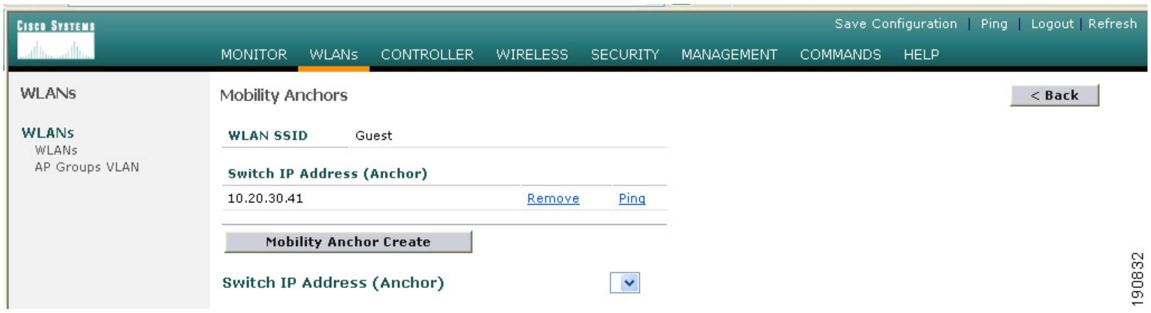
Switch IP Address (Anchor) 10.20.30.41

Verifying the Guest WLAN Mobility Anchor

The following screenshot shows a mobility anchor assigned to the guest WLAN. You can verify that it can be reached by clicking the **Ping** link as shown above.

Step 5 When finished, click **Back**. (See Figure 12-27.)

Figure 12-27 Verifying the Guest WLAN Mobility Anchor


Cisco Systems
Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
WLANs
WLANs
WLANs
AP Groups VLAN
< Back
Mobility Anchor Create
190832

Mobility Anchors

WLAN SSID	Guest	
Switch IP Address (Anchor)		
10.20.30.41	Remove	Ping

Switch IP Address (Anchor)

Step 6 After defining the mobility anchor, remember to go back and enable the WLAN.

Enabling the Guest WLAN

Perform the following steps to enable the WLAN.

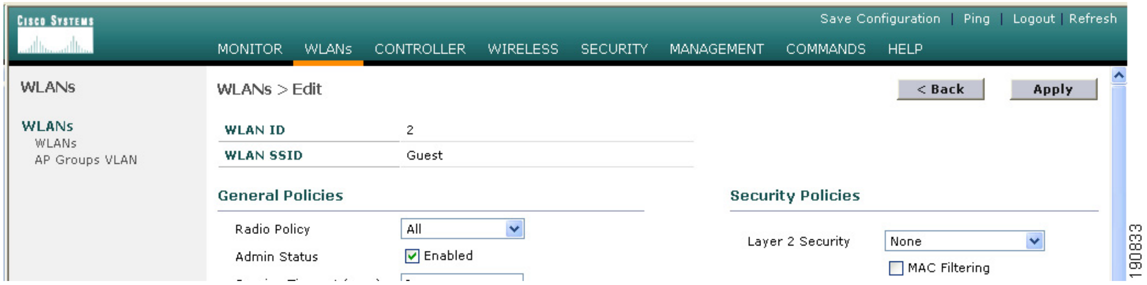
Step 1 Go back to the WLAN configuration page, find the guest WLAN created in Guest WLAN Configuration for the Remote Controller, page 12-24.

Step 2 Click **Edit**.

Step 3 Click the **Admin Status – Enabled** check box.

Step 4 Click **Apply**. (See Figure 12-28.)

Figure 12-28 Enabling the Guest WLAN



WLANs > Edit

WLAN ID	2
WLAN SSID	Guest

General Policies

Radio Policy	All
Admin Status	☑ Enabled

Security Policies

Layer 2 Security	None
	□ MAC Filtering

This completes the guest WLAN configuration. Repeat all steps from Guest WLAN Configuration for the Remote Controller, page 12-24 through Enabling the Guest WLAN, page 12-27 for any additional remote controllers.

Guest WLAN Configuration on the Anchor Controller

Guest WLAN configuration on the anchor controller is identical to that performed on the remote controller except for minor differences in the WLAN policies configuration and mobility anchor definition. Repeat all steps from Guest WLAN Configuration for the Remote Controller, page 12-24 through Enabling the Guest WLAN, page 12-27 on the anchor controller.

Note The SSID used for the guest WLAN must be exactly the same as what was configured on the remote controllers.

Guest WLAN Policies for the Anchor Controller

The policies defined for the guest WLAN on the anchor controller are the same except for the interface to which the WLAN is mapped. In this case, the guest WLAN is going to use the interface created in Guest VLAN Interface Configuration, page 12-18.

Step 1 Click the **WLANs** tab.

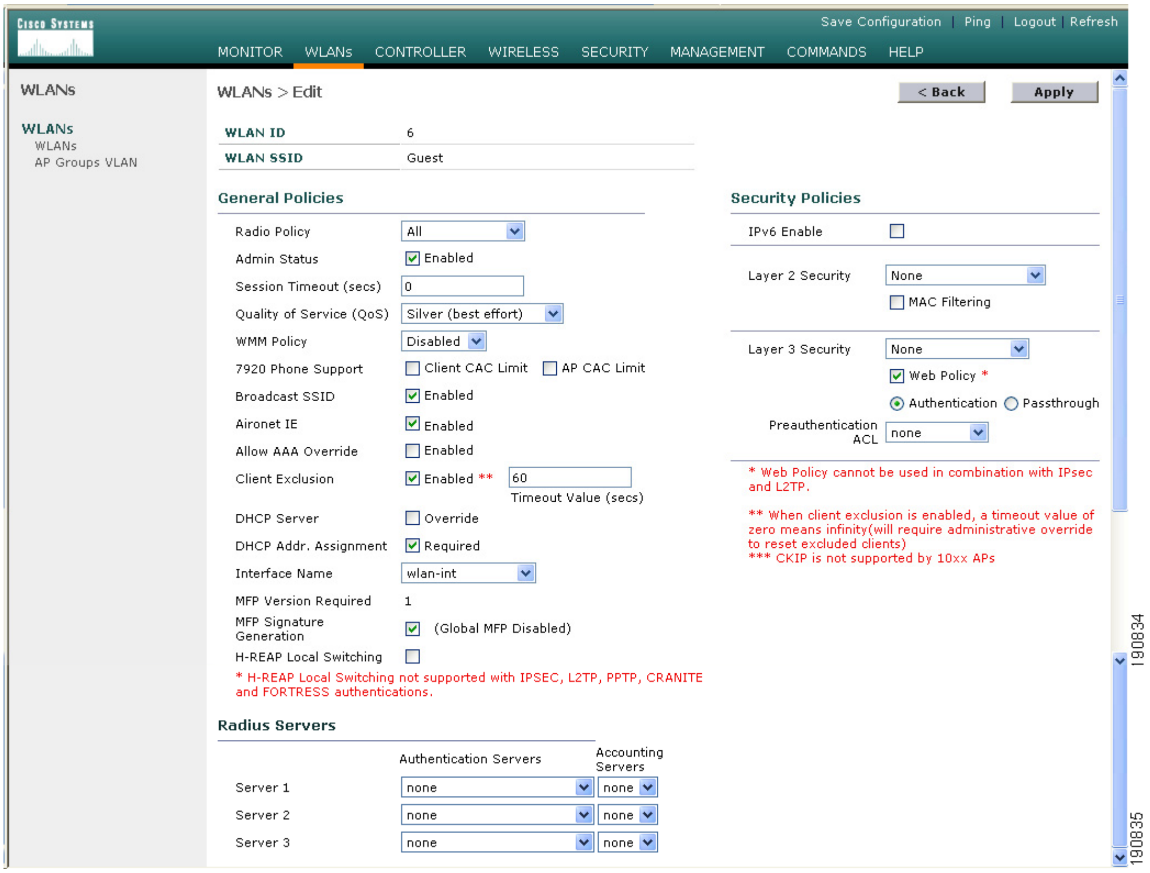
Step 2 Find the guest WLAN and click **Edit**.

Step 3 Configure the same settings used in Defining a Guest WLAN SSID, page 12-25 except under **Interface Name** choose the interface name created in Guest VLAN Interface Configuration, page 12-18.

Note No RADIUS servers are selected for this WLAN. User authentication of user credentials is handled locally on the controller. See Guest User Authentication, page 12-14.

Step 4 Click **Apply**. (See Figure 12-29.)

Figure 12-29 Configuring Guest WLAN Policies



WLANs > Edit

WLAN ID	6
WLAN SSID	Guest

General Policies

Radio Policy	All
Admin Status	☑ Enabled
Session Timeout (secs)	0
Quality of Service (QoS)	Silver (best effort)
WMM Policy	Disabled
7920 Phone Support	□ Client CAC Limit □ AP CAC Limit
Broadcast SSID	☑ Enabled
Aironet IE	☑ Enabled
Allow AAA Override	□ Enabled
Client Exclusion	☑ Enabled ** 60 Timeout Value (secs)
DHCP Server	□ Override
DHCP Addr. Assignment	☑ Required
Interface Name	wlan-int
MFP Version Required	1
MFP Signature Generation	☑ (Global MFP Disabled)
H-REAP Local Switching	□

* H-REAP Local Switching not supported with IPSEC, L2TP, PPTP, CRANITE and FORTRESS authentications.

Radius Servers

	Authentication Servers	Accounting Servers
Server 1	none	none
Server 2	none	none
Server 3	none	none

Security Policies

IPv6 Enable	□
Layer 2 Security	None □ MAC Filtering
Layer 3 Security	None ☑ Web Policy * ● Authentication ○ Passthrough
Preauthentication ACL	none

* Web Policy cannot be used in combination with IPsec and L2TP.

** When client exclusion is enabled, a timeout value of zero means infinity(will require administrative override to reset excluded clients)

*** CKIP is not supported by 10xx APs

Defining the Guest WLAN Mobility Anchor

The mobility anchor that is used for the guest WLAN is the anchor controller itself.

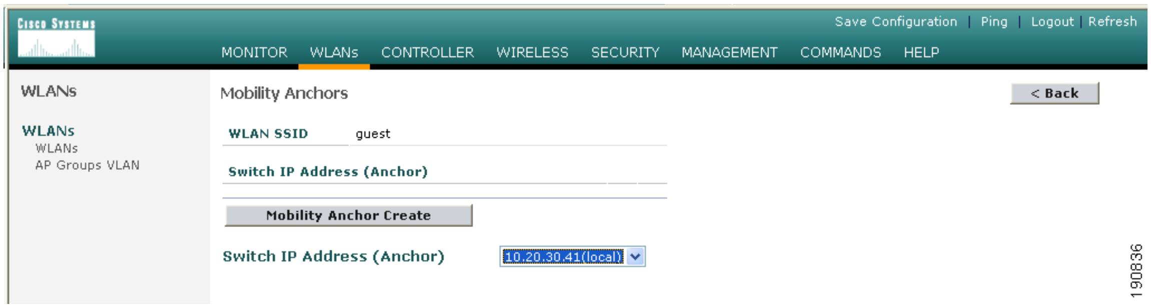
Step 1 Click the **WLANs** tab.

Step 2 Find the Guest WLAN and click **Mobility Anchors**.

Step 3 From the drop-down 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 12-30.)

Figure 12-30 Defining the Guest WLAN Mobility Anchor


Cisco Systems
Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
WLANs
WLANs
WLANs
AP Groups VLAN
< Back
Mobility Anchor Create
190836

Mobility Anchors

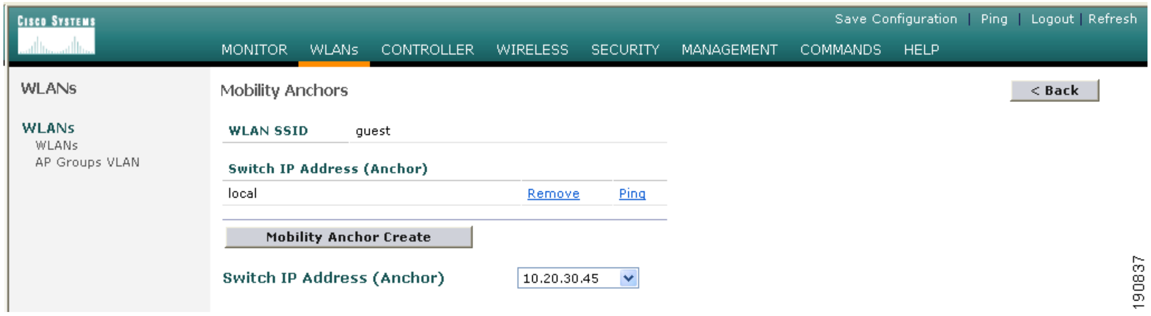
WLAN SSID guest

Switch IP Address (Anchor)

Switch IP Address (Anchor) 10.20.30.41(local)

Note that the guest WLAN mobility anchor is *local*. (See Figure 12-31.)

Figure 12-31 Verifying Guest Mobility Anchor is local


Cisco Systems
Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
WLANs
WLANs
WLANs
AP Groups VLAN
< Back
Remove
Ping
Mobility Anchor Create
190837

Mobility Anchors

WLAN SSID guest

Switch IP Address (Anchor)

local

Switch IP Address (Anchor) 10.20.30.45

Step 5 Enable the WLAN. Follow the instructions given in Enabling the Guest WLAN, page 12-27.

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 a 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.

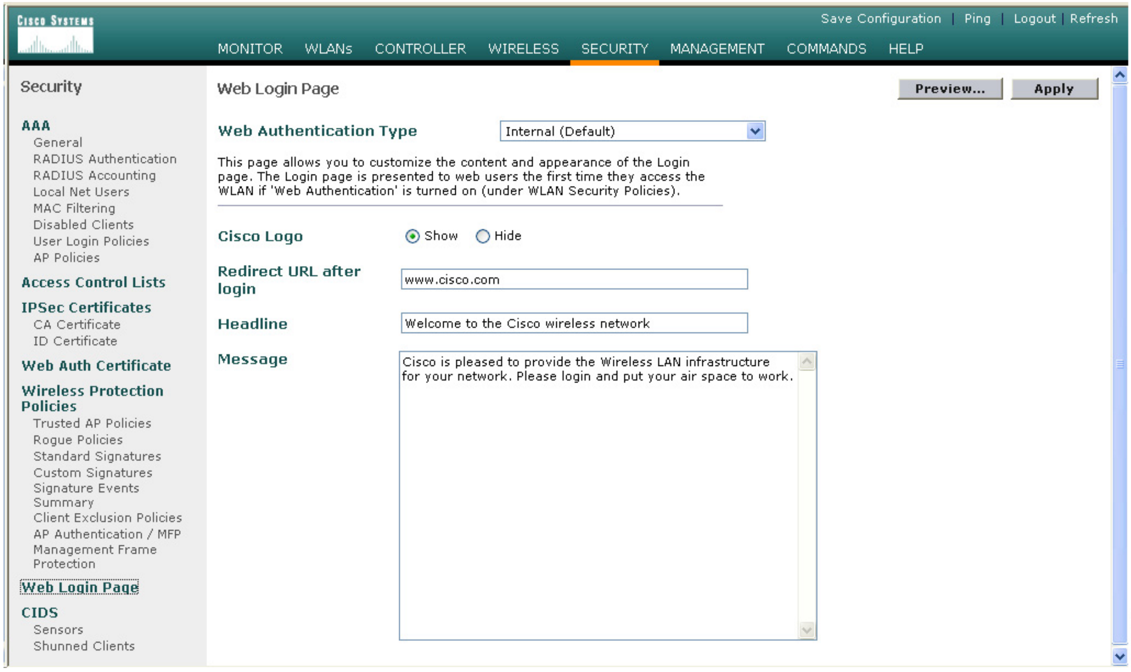
Internal Web Page Management

Step 1 Click the **Security** tab.

Step 2 In the left pane, click **Web Login Page**.

The configuration screen shown in Figure 12-32 is displayed. You can change the heading and message information that will appear on the portal page. You can also choose a post authentication redirect URL.

Figure 12-32 Configuration Screen



Web Login Page

Web Authentication Type: Internal (Default)

This page allows you to customize the content and appearance of the Login page. The Login page is presented to web users the first time they access the WLAN if 'Web Authentication' is turned on (under WLAN Security Policies).

Cisco Logo: ● Show ○ Hide

Redirect URL after login: www.cisco.com

Headline: Welcome to the Cisco wireless network

Message: Cisco is pleased to provide the Wireless LAN infrastructure for your network. Please login and put your air space to work.

Step 3 Click **Apply**.

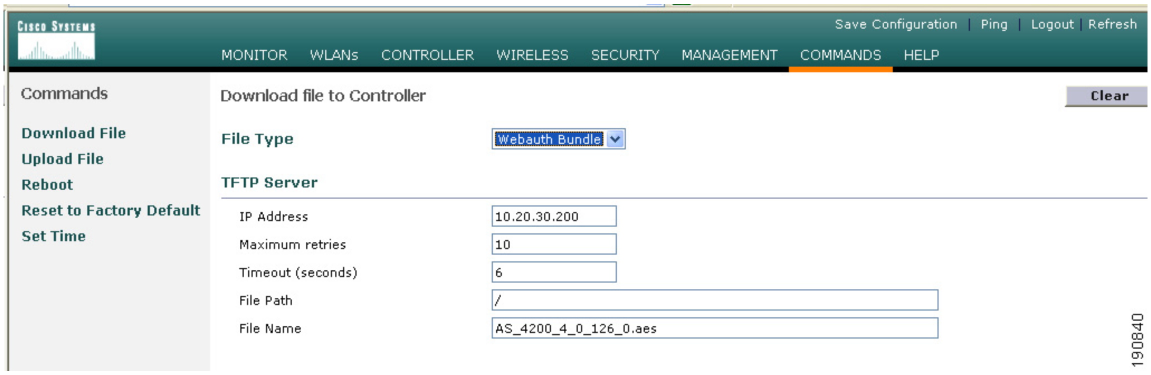
Step 4 Optionally, click **Preview** to view what the user will see when redirected.

Importing A Web Page

If you want a customized web page, one can be downloaded and stored locally on the anchor controller. To import a customized web page, perform the following steps:

Step 1 Click the **Commands** tab. (See Figure 12-33.)

Figure 12-33 Importing a Web Page



Download file to Controller

File Type: Webauth Bundle

TFTP Server

IP Address: 10.20.30.200

Maximum retries: 10

Timeout (seconds): 6

File Path: /

File Name: AS_4200_4_0_126_0.aes

Step 2 Under File Type choose **Web Auth Bundle**.

Step 3 Define IP address and file path on TFTP server where the files reside.

Step 4 Click **Download** to begin.

There are some caveats to be aware of with regard to downloading a web auth bundle:

- Choose **Web Auth Bundle** from the drop-down 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 being used to create the web login page. When downloaded, the controller will untar the files and place them in the appropriate directory.
- The Web Auth Bundle (tar file) cannot be larger than 1 MB.
- The file name for the html logon page must be **login.html**.

Selecting an Imported Web Auth Page

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

Step 1 Click the **Security** tab.

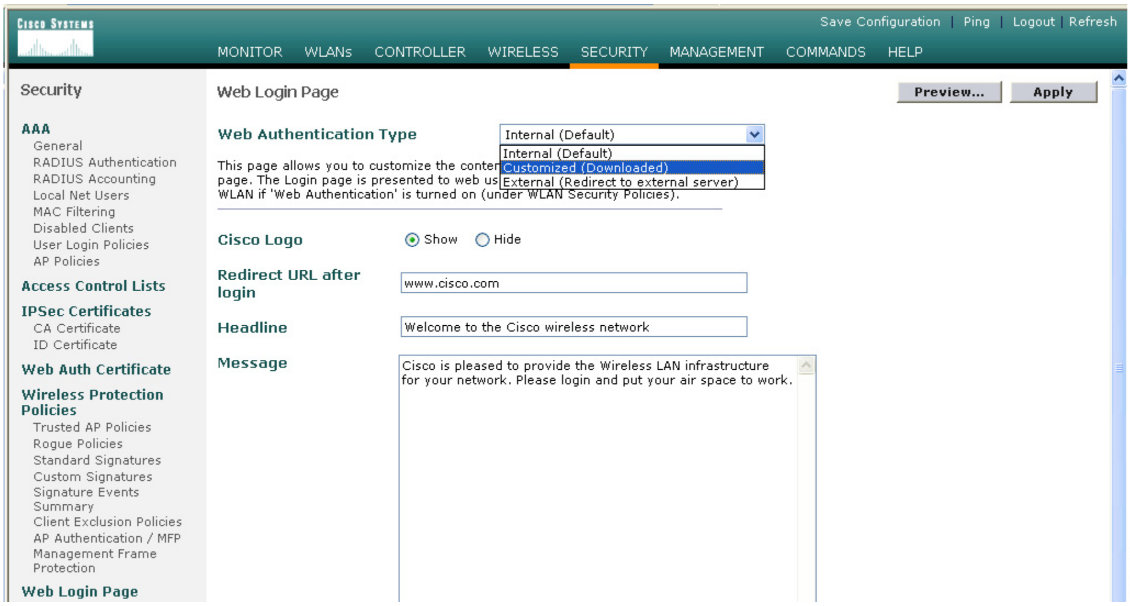
Step 2 In the left pane, click **Web Login Page**.

Step 3 From the Web Authentication Type drop-down list choose **Customized** (Downloaded)

Step 4 Click **Preview** to view the downloaded page.

Step 5 Click **Apply** when finished. (See Figure 12-34.)

Figure 12-34 Selecting an Imported Web Auth Page



Web Login Page

Web Authentication Type: Internal (Default)

This page allows you to customize the conten[t] page. The Login page is presented to web us[ers] WLAN if 'Web Authentication' is turned on (under WLAN Security Policies).

Cisco Logo: ● Show ○ Hide

Redirect URL after login: www.cisco.com

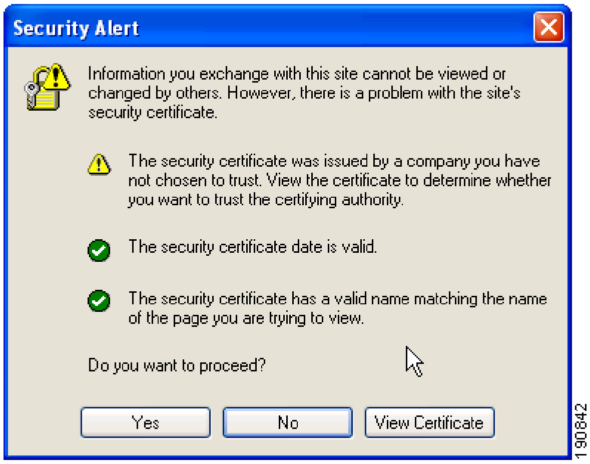
Headline: Welcome to the Cisco wireless network

Message: Cisco is pleased to provide the Wireless LAN infrastructure for your network. Please login and put your air space to work.

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 12-35.

Figure 12-35 Authentication Page



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?

At this point, the user can proceed by either clicking **Yes** or they can choose **View Certificate** and manually install it as a trusted site.

The web server uses the virtual interface IP address configured inAnchor Controller Interface Configuration, page 12-17 as its source address. If a host name 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.

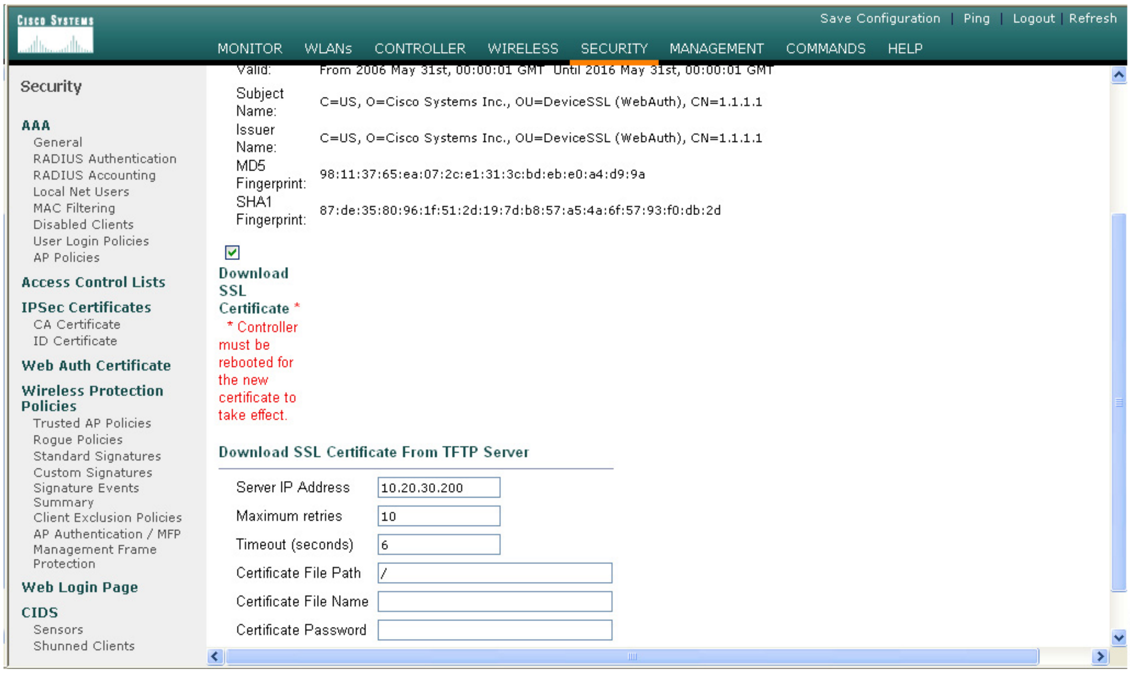
Importing an External Web Certificate

In those 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:

Step 1 Click the **Security** tab.

Step 2 In the left pane, click **Web Auth Certificate**. (See Figure 12-36.)

Figure 12-36 Importing an External Web Certificate



Valid:	From 2006 May 31st, 00:00:01 GMT Until 2016 May 31st, 00:00:01 GMT
Subject Name:	C=US, O=Cisco Systems Inc., OU=DeviceSSL (WebAuth), CN=1.1.1.1
Issuer Name:	C=US, O=Cisco Systems Inc., OU=DeviceSSL (WebAuth), CN=1.1.1.1
MD5 Fingerprint:	98:11:37:65:ea:07:2c:e1:31:3c:bd:eb:e0:a4:d9:9a
SHA1 Fingerprint:	87:de:35:80:96:1f:51:2d:19:7d:b8:57:a5:4a:6f:57:93:f0:db:2d

☑ Download SSL Certificate *

* Controller must be rebooted for the new certificate to take effect.

Download SSL Certificate From TFTP Server

Server IP Address	10.20.30.200
Maximum retries	10
Timeout (seconds)	6
Certificate File Path	/
Certificate File Name	
Certificate Password	

Step 3 Place a check mark in the **Download SSL Certificate** check box

Step 4 Complete the required fields for downloading the certificate.

Step 5 Click **Apply**.

Step 6 After the certificate has been downloaded, reboot the server.

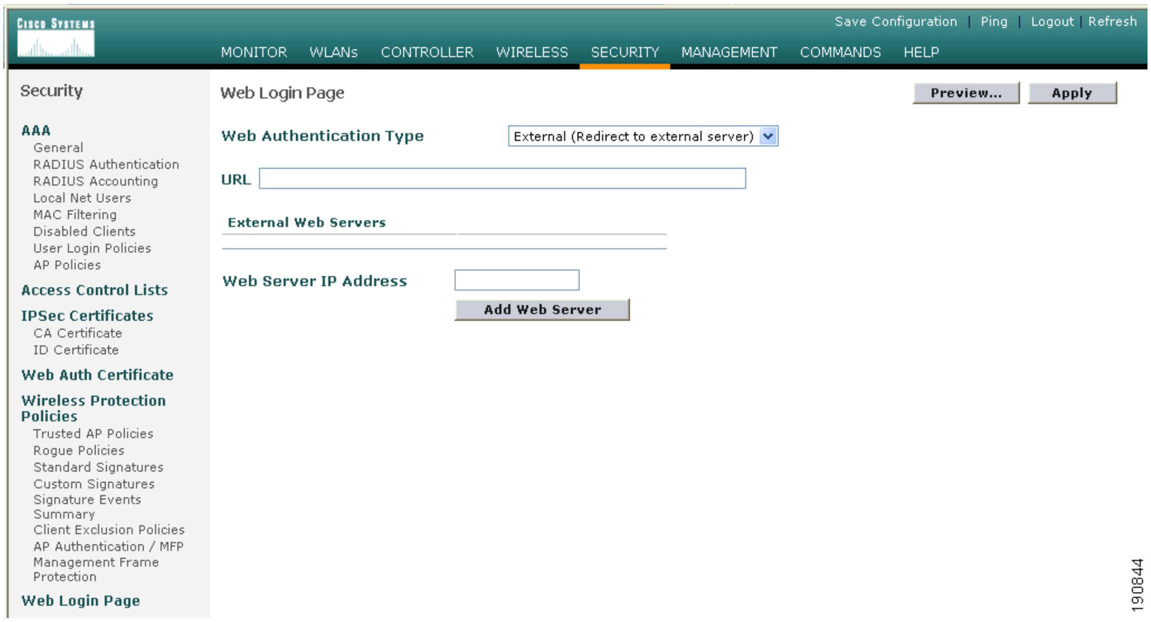
Support for External Web Redirection

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:

Step 1 Click the **Security** tab.

Step 2 In the left pane, click **Web Login Page**. (See Figure 12-37.)

Figure 12-37 Supporting External Web Redirection



Web Login Page

Web Authentication Type: External (Redirect to external server)

URL:

External Web Servers

Web Server IP Address:

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

Step 4 Click **Apply**.

Guest Management

If guest credentials are going to be stored locally on the anchor controller, there are two methods by which they can be created and posted to the controller:

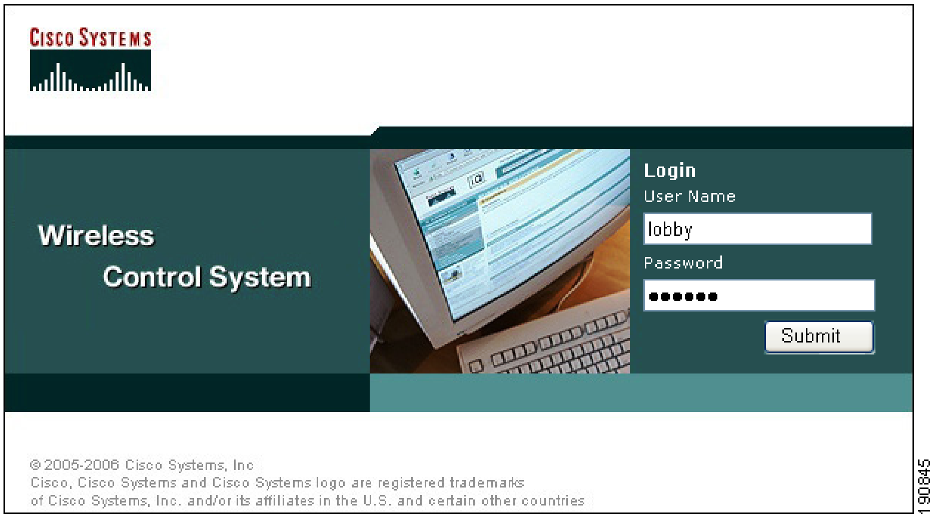
- Through the WCS lobby administration interface
- Directly on the controller through a local lobby admin account

Guest Management Using WCS

The following configuration examples assume WCS version 4.0 has been installed, configured, and a lobby ambassador account has been established. See Chapter 8, "Cisco Unified Wireless Control System," for more information on installing and configuring WCS.

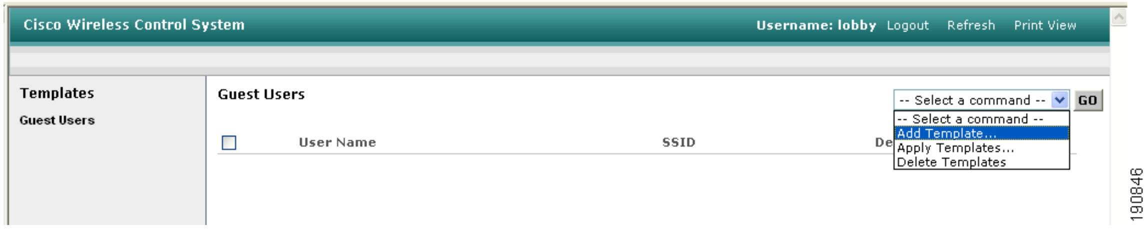
Step 1 Log in to WCS using the Lobby Ambassador credentials assigned by the system administrator. (See Figure 12-38.)

Figure 12-38 Using WCS


Cisco Systems
Wireless
Control System
Login
User Name
lobby
Password
●●●●●●
Submit
© 2005-2006 Cisco Systems, Inc
Cisco, Cisco Systems and Cisco Systems logo are registered trademarks
of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries
190845

After logging in, the screen shown in Figure 12-39 is displayed.

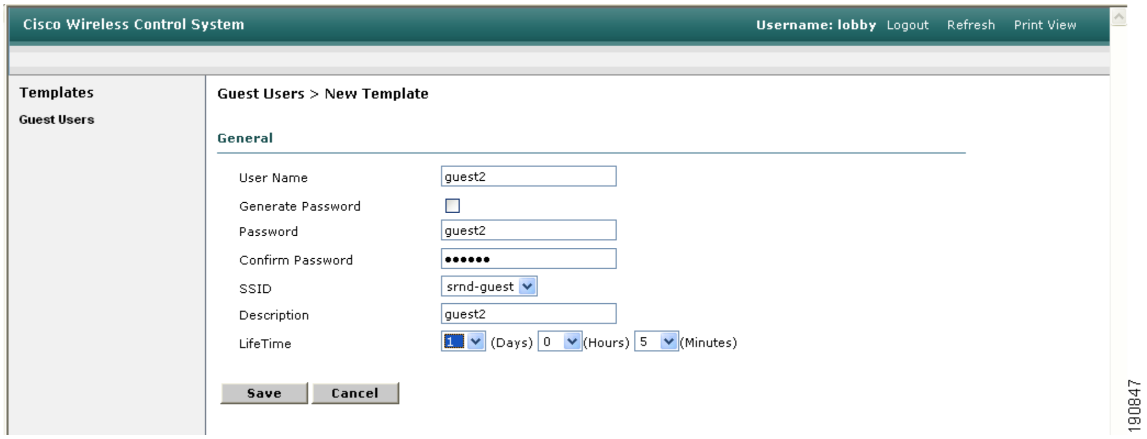
Figure 12-39 Adding a Template



Step 2 To add a user template, from the drop-down list, choose **Add Template** and click **Go**.

The screen shown in Figure 12-40 appears.

Figure 12-40 Guest User Template



Cisco Wireless Control System

Username: lobby

Guest Users > New Template

General

User Name	guest2
Generate Password	□
Password	guest2
Confirm Password	••••••
SSID	srnd-guest
Description	guest2
LifeTime	1 (Days) 0 (Hours) 5 (Minutes)

Step 3 To creating user credentials, enter a username and password (auto or manual).

Step 4 Select the WLAN / SSID the guest account applies to. (only WLANs configured to use a web policy are displayed).

Step 5 Enter the lifetime for credentials.

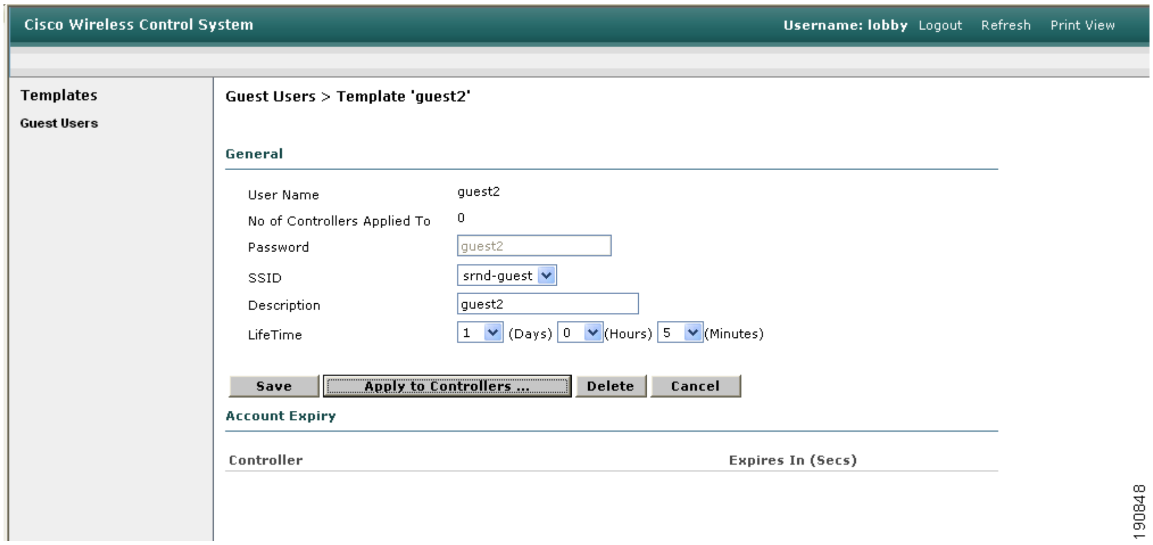
Step 6 Enter a description for the user.

Step 7 Click **Save**.

Applying Credentials

After the credentials have been created, the screen shown in Figure 12-41 offers the option to apply them to one or more controllers.

Figure 12-41 Applying Credentials



Guest Users > Template 'guest2'

General

User Name	guest2
No of Controllers Applied To	0
Password	guest2
SSID	srnd-guest
Description	guest2
LifeTime	1 (Days) 0 (Hours) 5 (Minutes)

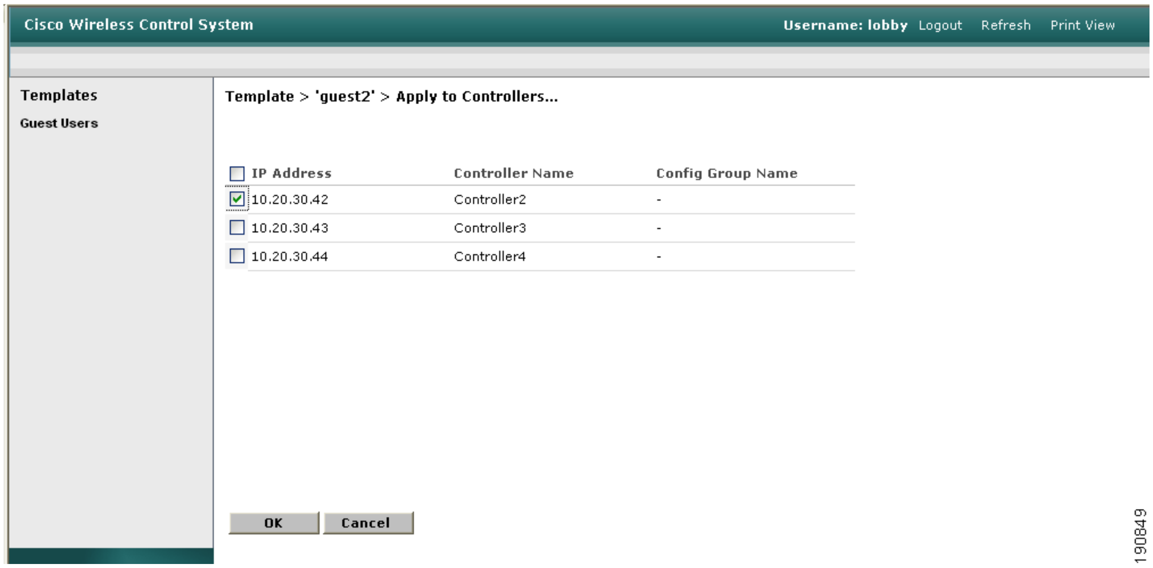
Account Expiry

Controller	Expires In (Secs)

Step 1 Click **Apply to Controllers**.

As shown in Figure 12-42, a list of eligible controllers is displayed (only those controllers that have been configured with the guest WLAN are displayed).

Figure 12-42 Apply to Controllers Screen



Template > 'guest2' > Apply to Controllers...

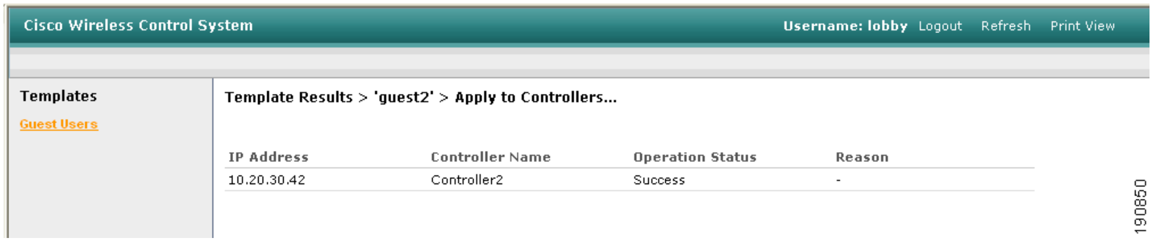
□ IP Address	Controller Name	Config Group Name
☑ 10.20.30.42	Controller2	-
□ 10.20.30.43	Controller3	-
□ 10.20.30.44	Controller4	-

Note The guest WLAN will have been configured on the anchor controller and one or more remote controllers. The anchor controller is the only controller where the guest credentials need to be applied.

Step 2 To apply credentials to the anchor controller, from the list of controllers, choose the anchor controller, and click **OK**.

A confirmation page that verifies that the user credentials were saved to the anchor controller is displayed. (See Figure 12-43.)

Figure 12-43 Confirmation Page

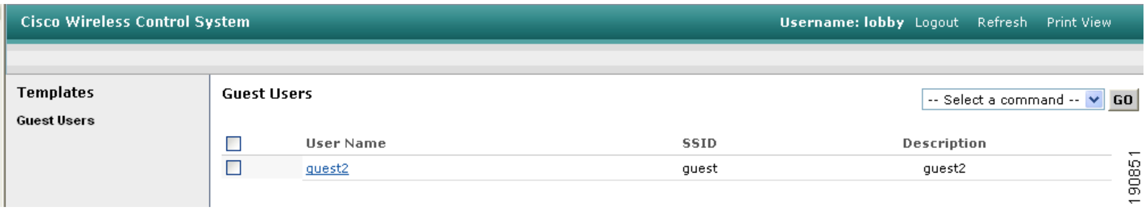


Template Results > 'guest2' > Apply to Controllers...

IP Address	Controller Name	Operation Status	Reason
10.20.30.42	Controller2	Success	-

Step 3 In the left pane, click **Guest Users** to return to the summary page. (See Figure 12-44.)

Figure 12-44 Summary Page



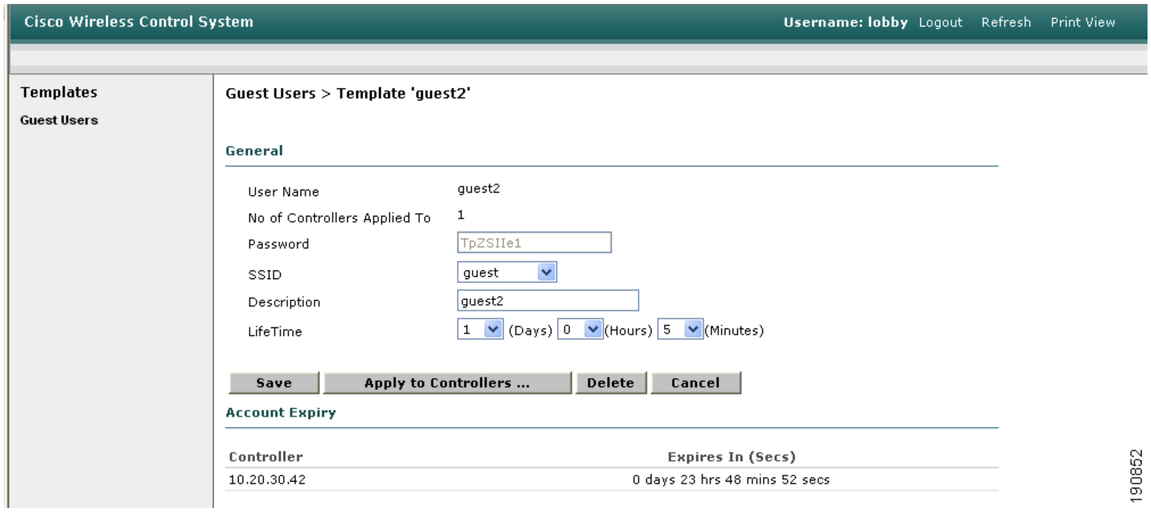
Guest Users

	User Name	SSID	Description
□	guest2	guest	guest2

Step 4 To edit guest credentials, from the summary page, click the user name that you want to edit.

The user template is displayed, as shown in Figure 12-45.

Figure 12-45 Editing Guest Credentials



Guest Users > Template 'guest2'

General

User Name	guest2
No of Controllers Applied To	1
Password	TpZSIIe1
SSID	guest
Description	guest2
LifeTime	1 (Days) 0 (Hours) 5 (Minutes)

Account Expiry

Controller	Expires In (Secs)
10.20.30.42	0 days 23 hrs 48 mins 52 secs

In this page, you can make the following modifications if desired:

- Change the WLAN to which the credentials apply.
- Change the user description.
- Change the Lifetime of the credentials.
- Apply the credentials to other controllers.
- Delete the user template.

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

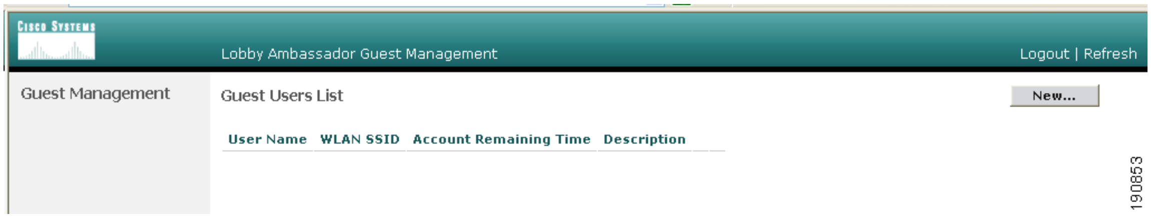
Managing Guest Credentials Directly on the Anchor Controller

The following procedure assumes a network administrator has established a Local Management User account with Lobby Admin privileges on the controller.

Step 1 Log in 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 12-10.

After login, the screen shown in Figure 12-46is displayed.

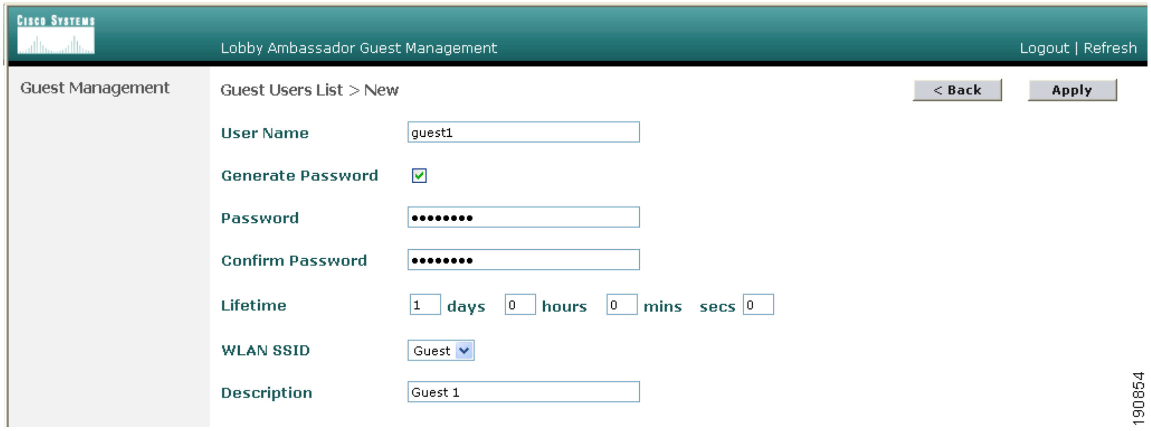
Figure 12-46 Anchor Controller Login



Step 2 Click **New**.

The screen shown in Figure 12-47 appears.

Figure 12-47 Creating User Credentials



Guest Users List > New

User Name	guest1
Generate Password	☑
Password	••••••••
Confirm Password	••••••••
Lifetime	1 days 0 hours 0 mins secs 0
WLAN SSID	Guest
Description	Guest 1

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 web policy will be displayed).

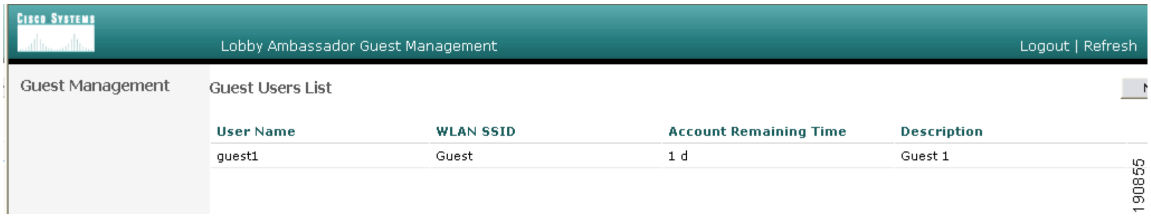
c. Enter a lifetime for the credentials.

d. Enter a description for the user.

Step 4 Click **Apply**.

The screen shown in Figure 12-48 appears and shows the newly added guest user.

Figure 12-48 Guest Users List



Guest Users List

User Name	WLAN SSID	Account Remaining Time	Description
guest1	Guest	1 d	Guest 1

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

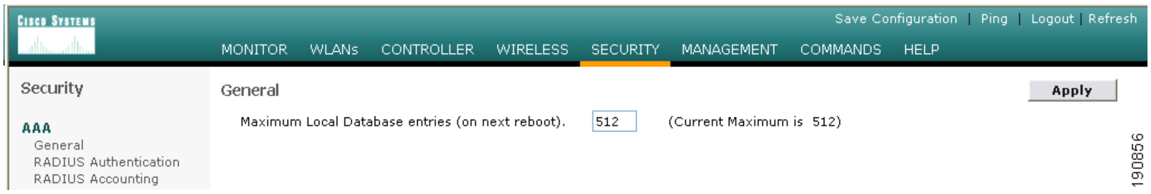
- Edit the existing user
- Delete the existing user
- Add a new user

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 12-49.)

Figure 12-49 Configuring the Maximum Number of User Accounts



General

Maximum Local Database entries (on next reboot). 512 (Current Maximum is 512)

Step 2 In the left pane, click **General** under AAA properties.

Step 3 Configure the maximum number of user database entries (between 512 and 2048).

Step 4 Click **Apply**.

Guest User Management Caveats

- Guest credentials can be added using either method above or both methods together.
- When using WCS, the lobby admin does not have visibility of user accounts that might have been created locally on the anchor controller. If a WCS lobby admin attempts to add a user name that is already in use, a pop-up window prompting the admin to choose a different user name is displayed.
- When adding user accounts locally on the controller, the admin sees 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.

External Radius Authentication

As described in Guest User Authentication, page 12-14, 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, then the lobby admin features described in Guest Management, page 12-36 cannot be used. It is assumed that some other guest management system will be used in conjunction with the external RADIUS server.

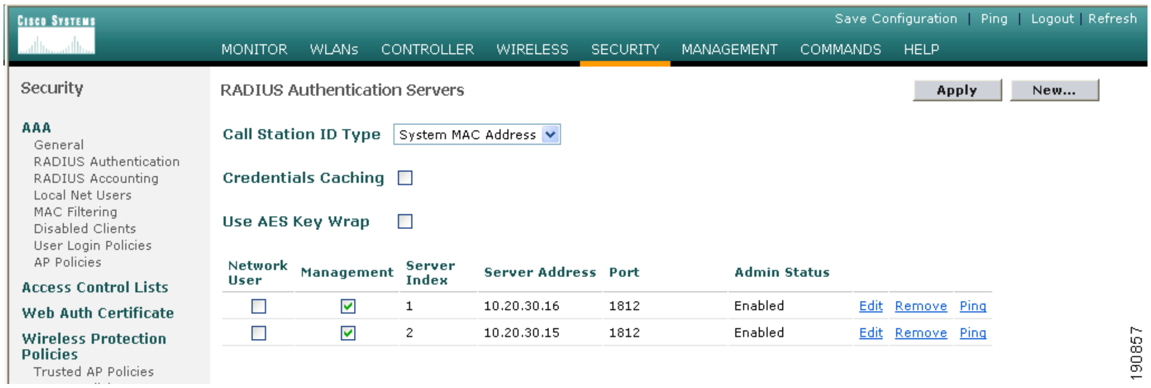
To configure a guest WLAN to use an external RADIUS server, perform the following configuration steps on the anchor controller.

Adding a RADIUS Server

Step 1 Click the **Security** tab.

A summary screen is displayed. (See Figure 12-50.)

Figure 12-50 Summary Screen



RADIUS Authentication Servers

Call Station ID Type: System MAC Address

Credentials Caching □

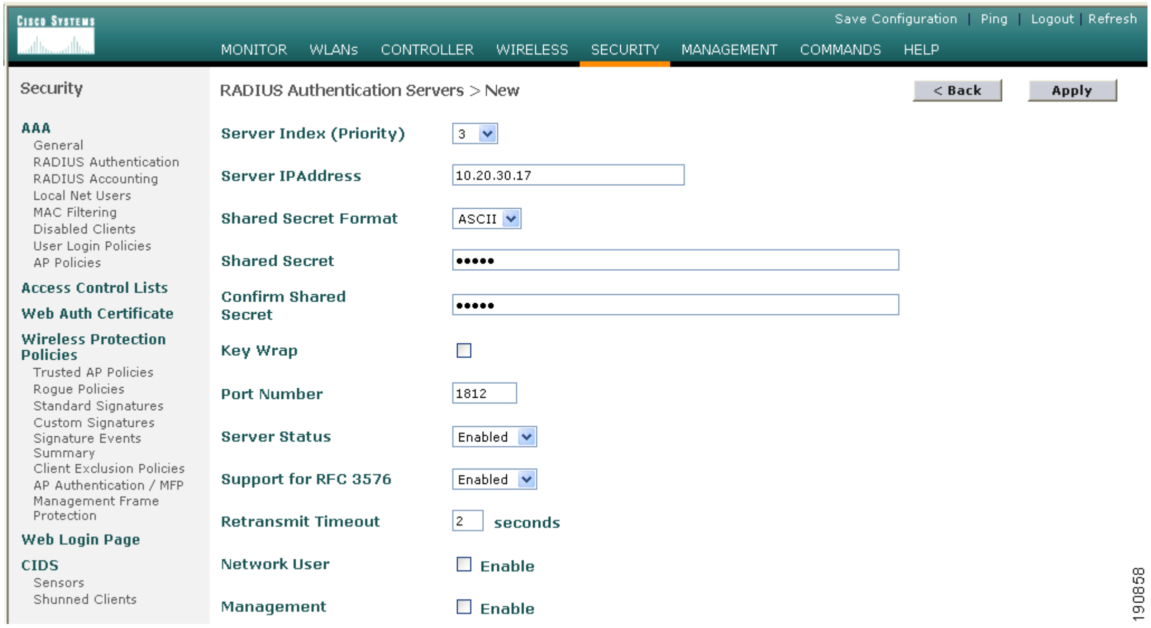
Use AES Key Wrap □

Network User	Management	Server Index	Server Address	Port	Admin Status			
□	☑	1	10.20.30.16	1812	Enabled	Edit	Remove	Ping
□	☑	2	10.20.30.15	1812	Enabled	Edit	Remove	Ping

Step 2 Click **New**.

The screen shown in Figure 12-51appears.

Figure 12-51 Defining RADIUS Server Settings



RADIUS Authentication Servers > New

Server Index (Priority)	3
Server IPAddress	10.20.30.17
Shared Secret Format	ASCII
Shared Secret	•••••
Confirm Shared Secret	•••••
Key Wrap	□
Port Number	1812
Server Status	Enabled
Support for RFC 3576	Enabled
Retransmit Timeout	2 seconds
Network User	□ Enable
Management	□ Enable

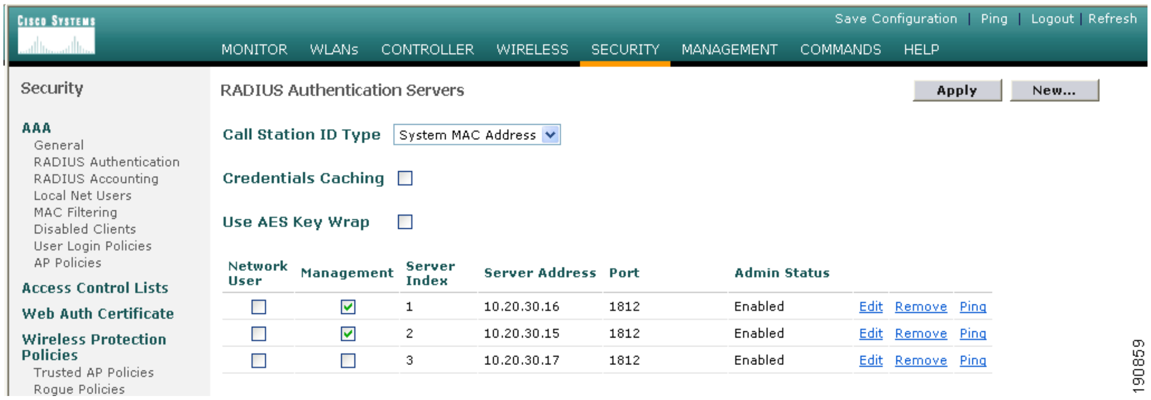
Step 3 To define RADIUS server settings, configure the IP address, Shared Secret, and Authentication Port Number as defined on the RADIUS server.

If the Network User check box is cleared, the RADIUS server is used only for user authentication when it is specifically selected under a given WLANs RADIUS setting. Otherwise, if the 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 shows the newly added server. (See Figure 12-52.)

Figure 12-52 Summary Screen



RADIUS Authentication Servers

Call Station ID Type: System MAC Address

Credentials Caching □

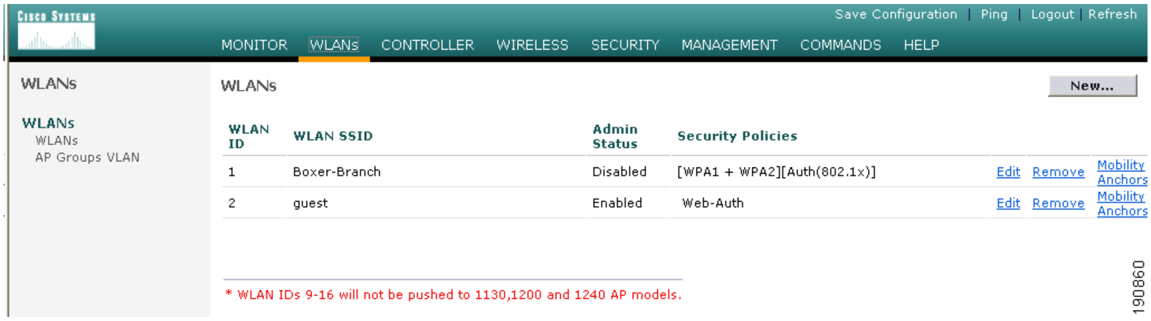
Use AES Key Wrap □

Network User	Management	Server Index	Server Address	Port	Admin Status			
□	☑	1	10.20.30.16	1812	Enabled	Edit	Remove	Ping
□	☑	2	10.20.30.15	1812	Enabled	Edit	Remove	Ping
□	□	3	10.20.30.17	1812	Enabled	Edit	Remove	Ping

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

Step 6 The screen shown in Figure 12-53 appears.

Figure 12-53 WLANs Tab



WLANs

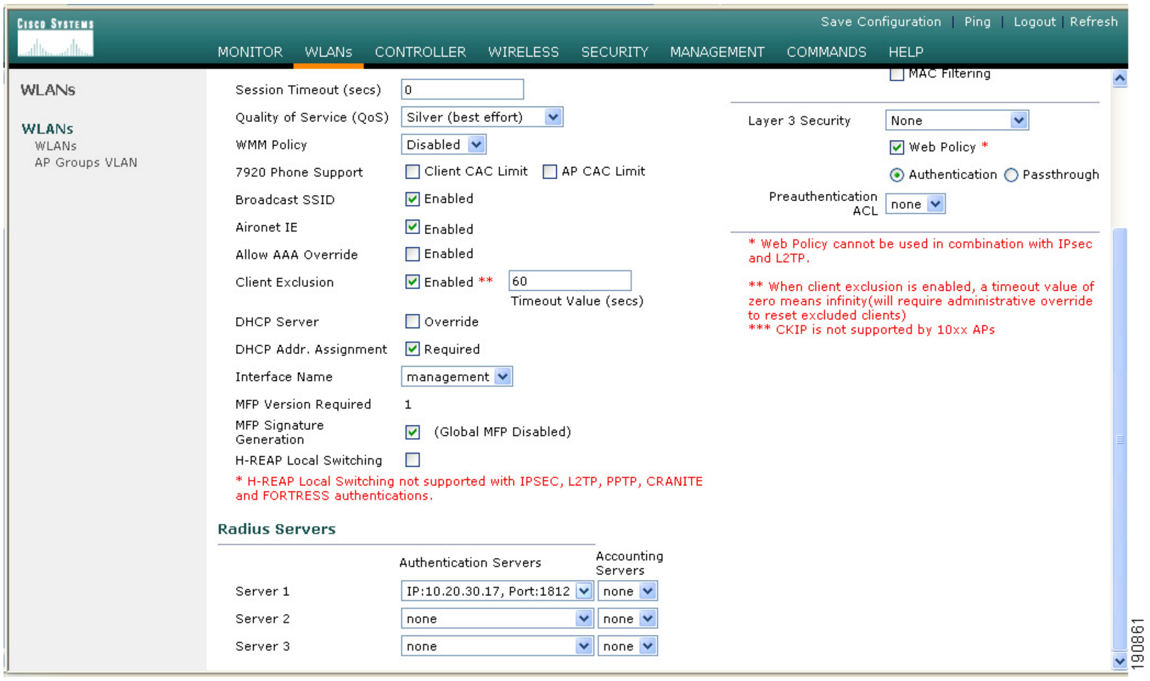
WLAN ID	WLAN SSID	Admin Status	Security Policies			
1	Boxer-Branch	Disabled	[WPA1 + WPA2][Auth(802.1x)]	Edit	Remove	Mobility Anchors
2	guest	Enabled	Web-Auth	Edit	Remove	Mobility Anchors

* WLAN IDs 9-16 will not be pushed to 1130,1200 and 1240 AP models.

Step 7 Find the guest WLAN and click **Edit**.

The guest WLAN configuration screen is displayed, as shown in Figure 12-54.

Figure 12-54 Guest WLAN Configuration Screen



Session Timeout (secs) 0
Quality of Service (QoS) Silver (best effort)
WMM Policy Disabled
7920 Phone Support □ Client CAC Limit □ AP CAC Limit
Broadcast SSID ☑ Enabled
Aironet IE ☑ Enabled
Allow AAA Override □ Enabled
Client Exclusion ☑ Enabled ** 60 Timeout Value (secs)
DHCP Server □ Override
DHCP Addr. Assignment ☑ Required
Interface Name management
MFP Version Required 1
MFP Signature Generation ☑ (Global MFP Disabled)
H-REAP Local Switching □
* H-REAP Local Switching not supported with IPSEC, L2TP, PPTP, CRANITE and FORTRESS authentications.

□ MAC Filtering
Layer 3 Security None
☑ Web Policy *
● Authentication ○ Passthrough
Preauthentication ACL none

* Web Policy cannot be used in combination with IPsec and L2TP.

** When client exclusion is enabled, a timeout value of zero means infinity(will require administrative override to reset excluded clients)
*** CKIP is not supported by 10xx APs

Radius Servers

	Authentication Servers	Accounting Servers
Server 1	IP:10.20.30.17, Port:1812	none
Server 2	none	none
Server 3	none	none

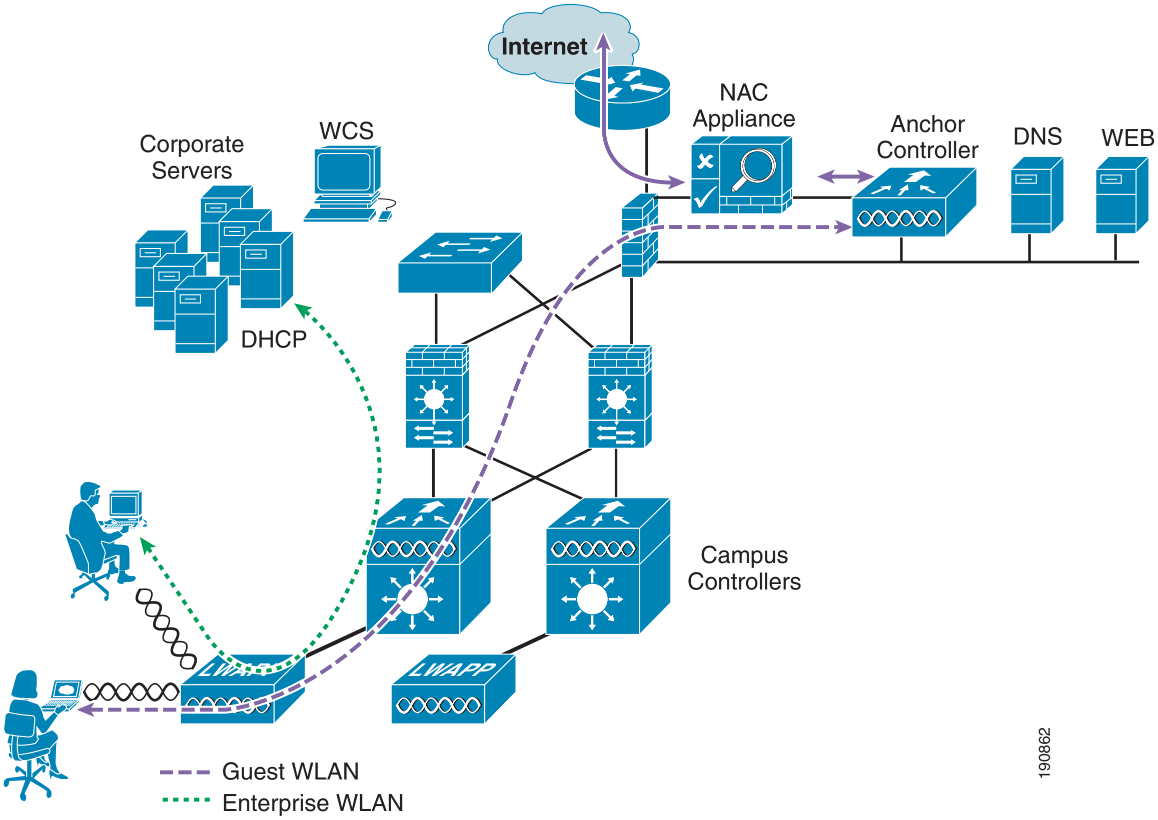
Step 8 Select the RADIUS server to be used for web authentication from the drop-down list.

External Access Control

The centralized guest access topology described in this chapter can be integrated with an external access control platform such as BBSM or Clean Access.

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 12-55).

Figure 12-55 Wireless Guest Access with External Access Control

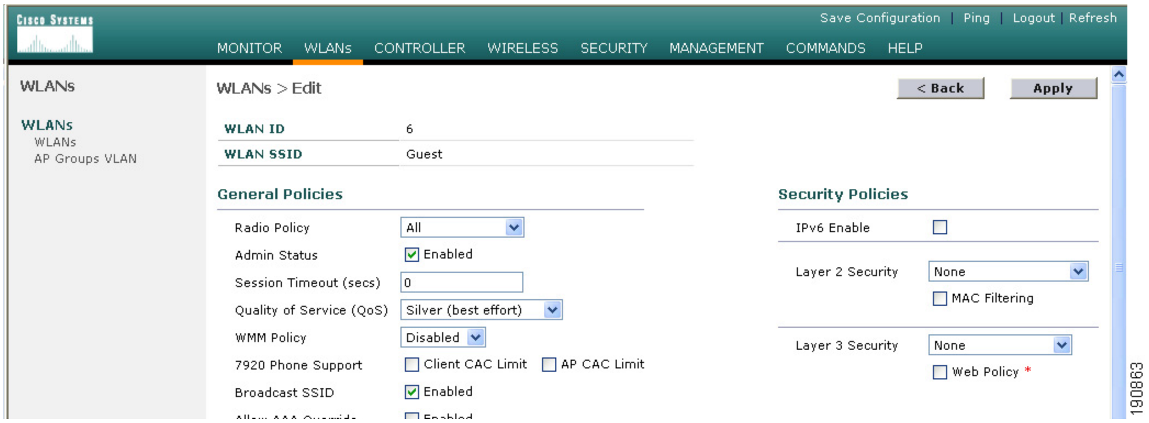


As shown in Figure 12-55, The wireless guest access topology remains the same except the guest VLAN interface on the anchor controller, instead of connecting to a firewall or border router, connects to an inside interface on an access control platform such as BBSM.

In this scenario, the BBSM platform is responsible for redirection, web authentication and subsequent access to the Internet. The campus and anchor controllers are only used to tunnel guest WLAN traffic across the enterprise into the DMZ where BBSM or some other platform is used to manage 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 web policy is disabled under the guest WLANs security policy (see Figure 12-56).

Figure 12-56 Guest WLAN Security Policy



WLAN ID	6
WLAN SSID	Guest

General Policies

Radio Policy	All
Admin Status	☑ Enabled
Session Timeout (secs)	0
Quality of Service (QoS)	Silver (best effort)
WMM Policy	Disabled
7920 Phone Support	☐ Client CAC Limit ☐ AP CAC Limit
Broadcast SSID	☑ Enabled
Allow AAA Override	☐ Enabled

Security Policies

IPv6 Enable	☐
Layer 2 Security	None ☐ MAC Filtering
Layer 3 Security	None ☐ Web Policy *

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

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

Its beyond the scope of this chapter to address BBSM or other external platform specific configuration. See the 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 upstream services)

Troubleshooting Guest Access

The following verifications and troubleshooting tasks assume:

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

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. 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 pings go through, but mpings do not, ensure that each WLCs mobility group name is the same and ensure that each WLCs IP, MAC, and mobility group name is entered in every WLC mobility list.

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

User Does Not Obtain an IP Address via DHCP

- Verify WLAN configuration settings are identical on the anchor and remote controllers
- Verify the guest WLAN is enabled on the anchor controller and all remote controllers that support the guest WLAN
- Check for a proper DHCP server address under the guest VLAN interface settings on the anchor controller
  - 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 controllers management IP address.
  - Verify that a DHCP scope has been configured and enabled on the controller
  - Verify that the DHCP scopes network mask is consistent with the mask on the guest VLAN interface.
  - Verify the DHCP scope does not overlap with any addresses assigned to 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 valid DNS servers are being assigned to the client via DHCP
- Ensure the DNS servers are reachable from the anchor controller
- Verify the URL being opened in the web browser is resolvable
- Verify the URL being opened in the web browser is connecting to http port 80

Note The internal web auth server does not redirect incoming requests on ports other than 80.

User Cannot Authenticate

- Verify user credentials are active on the anchor controller.
  - Guest credentials typically have a lifetime associated with them. If the credentials have expired, they do not appear under the 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 12-36 and Guest Credentials Management, page 12-13.
- 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 controller
- 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 summary

Number of Clients................................ 1
MAC Address        AP Name            Status         WLAN  Auth  Protocol  Port
-----------------  -----------------  -------------  ----  ----  --------  ----
00:40:96:a6:d5:3a  10.20.100.254      Associated     6     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 remote controller (originating controller).

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

```
(Cisco Controller) >show client detail 00:40:96:a6:d5:3a

Client MAC Address............................... 00:40:96:a6:d5:3a
Client Username ................................. guest1
AP MAC Address................................... 00:00:00:00:00:00
Client State..................................... Associated
Wireless LAN Id.................................. 6
BSSID............................................ 00:00:00:00:00:05
Channel.......................................... N/A
IP Address....................................... 10.20.31.101
Association Id................................... 0
Authentication Algorithm......................... Open System
Reason Code...................................... 0
Status Code...................................... 0
Session Timeout.................................. 0
Client CCX version............................... No CCX support
Re-Authentication Timeout........................ 81586
Remaining Re-Authentication Time................. 79010
Mirroring........................................ Disabled
```

```
QoS Level........................................ Silver
Diff Serv Code Point (DSCP)...................... disabled
802.1P Priority Tag.............................. disabled
WMM Support...................................... Disabled
Mobility State................................... Export Anchor
Mobility Foreign IP Address...................... 10.20.100.254  <Remote Controller
Mobility Move Count.............................. 1
Security Policy Completed........................ Yes
Policy Manager State............................. RUN
Policy Manager Rule Created...................... Yes
NPU Fast Fast Notified........................... Yes
Policy Type...................................... N/A
Encryption Cipher................................ None
EAP Type......................................... Unknown
Interface........................................ wlan-int
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]
```

The same information can be obtained through the web configuration and management interface of the controller under **Client Detail**. (See Figure 12-57.)

Figure 12-57 Monitor > Client Detail

Campus (Foreign) Controller

From the serial console port:

```
(Cisco Controller) >show client summary

Number of Clients................................ 1
MAC Address        AP Name            Status         WLAN  Auth  Protocol  Port
-----------------  -----------------  -------------  ----  ----  --------  ----
00:40:96:a6:d5:3a  Branch:24:a6:50    Associated     2     Yes   802.11g   1
```

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:

```
Cisco Controller) >show client detail 00:40:96:a6:d5:3a

Client MAC Address............................... 00:40:96:a6:d5:3a
Client Username ................................. N/A
AP MAC Address................................... 00:0b:85:24:a6:50
Client State..................................... Associated
Wireless LAN Id.................................. 2
BSSID............................................ 00:0b:85:24:a6:5e
Channel.......................................... 1
IP Address....................................... Unknown
Association Id................................... 4
Authentication Algorithm......................... Open System
```

```
Reason Code...................................... 0
Status Code...................................... 0
Session Timeout.................................. 0
Client CCX version............................... No CCX support
Re-Authentication Timeout........................ 0
Remaining Re-Authentication Time................. Timer is not running
QoS Level........................................ Silver
Diff Serv Code Point (DSCP)...................... disabled
802.1P Priority Tag.............................. disabled
WMM Support...................................... Disabled
Mobility State................................... Export Foreign
Mobility Anchor IP Address....................... 10.20.30.41<anchor controller>
Mobility Move Count.............................. 0
Security Policy Completed........................ Yes
Policy Manager State............................. RUN
Policy Manager Rule Created...................... Yes
Policy Type...................................... N/A
Encryption Cipher................................ None
EAP Type......................................... Unknown
Interface........................................ management <source of EoIP Tunnel>
VLAN............................................. 0
Client Capabilities:
      CF Pollable................................ Not implemented
      CF Poll Request............................ Not implemented
      Short Preamble............................. Implemented
      PBCC....................................... Not implemented
      Channel Agility............................ Not implemented
      Listen Interval............................ 0
Client Statistics:
      Number of Bytes Received................... 83288
      Number of Bytes Sent....................... 310361
      Number of Packets Received................. 670
      Number of Packets Sent..................... 430
      Number of Policy Errors.................... 0
      Radio Signal Strength Indicator............ -30 dBm
      Signal to Noise Ratio...................... 62 dB
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]
      Branch:24:a6:50(slot 1) ...................
antenna0: 451 seconds ago -26 dBm................ antenna1: 1522 seconds ago -68 dBm
```

The same information can be obtained through the controller web configuration and management interface under client detail (see Figure 12-57).

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
```