Wired Guest Access using Cisco WLAN Controllers Configuration Example

Contents

Introduction

This document describes how to configure guest access with the new Wired Guest Access feature support on the Cisco WLAN Controllers (WLCs) that use Cisco Unified Wireless Software Release 4.2.61.0 and later. A growing number of companies recognize the need to provide Internet access to its customers, partners, and consultants when they visit their facilities. IT managers can provide wired and wireless secured and controlled access to the Internet for guests on the same wireless LAN controller.

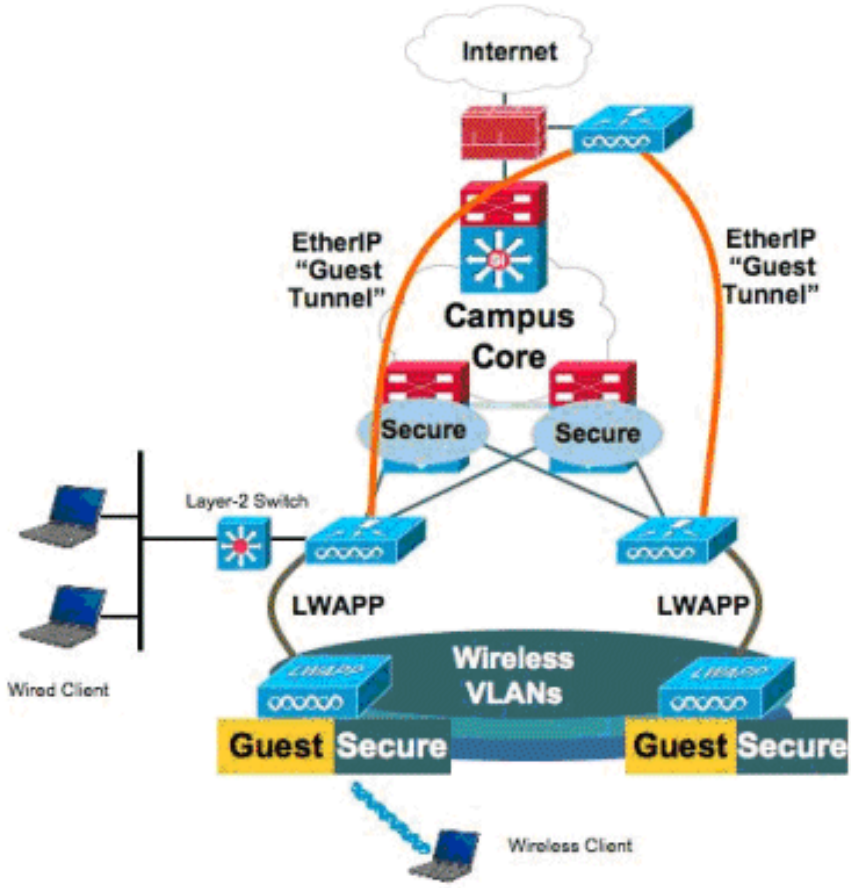
Guest users must be allowed to connect to designated Ethernet ports and access the guest network as configured by the administrator after they complete the configured authentication methods. Wireless guest users can easily connect to the WLAN Controllers with the current guest access features. In addition, Wireless Control System (WCS), along with basic configuration and management of WLAN Controllers, provides enhanced guest user services. For customers who have already deployed or plan to deploy WLAN Controllers and WCS in their network, they can leverage the same infrastructure for wired guest access. This provides a unified wireless and wired guest access experience to the end users.

Wired guest ports are provided in a designated location and plugged into an access switch. The configuration on the access switch puts these ports in one of the wired guest Layer 2 VLANs. Two separate solutions are available to the customers:

- A single WLAN controller (VLAN Translation mode) - the access switch trunks the wired guest traffic in the guest VLAN to the WLAN controller that provides the wired guest access solution. This controller carries out the VLAN translation from the ingress wired guest VLAN to the

egress VLAN.

- Two WLAN controllers (Auto Anchor mode) - the access switch trunks the wired guest traffic to a local WLAN controller (the controller nearest to the access switch). This local WLAN controller anchors the client onto a Demilitarized Zone (DMZ) Anchor WLAN controller that is configured for wired and wireless guest access. After a successful handoff of the client to the DMZ anchor controller, the DHCP IP address assignment, authentication of the client, and so on are handled in the DMZ WLC. After it completes the authentication, the client is allowed to send/receive
traffic.



Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The Wired Guest Access feature support on the Cisco WLAN controllers is supported by Cisco Unified Wireless Software Release 4.2.61.0 and later.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configure

In this section, you are presented with the information to configure the features described in this document.

Access Layer Switch Configuration

In order to provide the wired guest access, the designated ports in the Layer 2 access layer switch need to be configured on the guest VLAN by the administrator. The guest VLAN must be separate from any other VLANs that are configured on this switch. The guest VLAN traffic is trunked to the nearest WLAN local controller. The local controller tunnels the guest traffic across an Ethernet over IP (EoIP) tunnel to a DMZ Anchor controller. This solution requires at least two controllers.

Alternatively, the access switch trunks the guest VLAN to the single controller translates the guest VLAN to the egress interface of the WLAN controller.

```
cat6506# show vlan id 49

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
49   VLAN0049                         active    Gi2/1, Gi2/2, Gi2/4, Gi2/35
                                                Gi2/39, Fa4/24

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
49   enet  100049     1500  -      -      -        -    -        0      0

Remote SPAN VLAN
----------------
Disabled

Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------

cat6506#
interface FastEthernet4/24
 description Wired Guest Access
 switchport
 switchport access vlan 49
 no ip address
end
cat6506#
interface GigabitEthernet2/4
 description Trunk port to the WLC
 switchport
 switchport trunk native vlan 80
 switchport trunk allowed vlan 49,80,110
 switchport mode trunk
 no ip address
end
```

> **Note**: Use the Command Lookup Tool (registered customers only) to find more information on the commands used in this document.

Important Points for Wired Guest Deployment

- Currently, five Guest LANs for wired guest access are supported. In total, 16 WLANs for Wireless users and 5 WLANs for wired guest access can be configured on the Anchor WLC. No separate tunnels exist for WLANs. All the guest WLANs, which include the WLANs for wired guest access, use the same EoIP tunnels to the Anchor WLC.
- Administrators need to create dynamic interfaces in the WLAN controller, mark them as “Guest LAN,” and associate them to WLANs created as Guest LANs.
- Ensure that WLAN configurations, including authentication, are identical on both the Anchor and Remote controllers to pass the client traffic.
- WLCs should have compatible software versions. Ensure that they run the same major version.
- Web-authentication is the default security mechanism available on a wired guest LAN. The current options available are these: Open, Web Auth, and Web Passthrough.
- In case of failure of the EoIP tunnel between the remote and anchor WLC, the client database is cleaned up from the Anchor WLC. The client needs to reassociate and reauthenticate.
- No Layer 2 security is supported.
- Multicast/Broadcast traffic on the wired guest LANs is dropped.
- DHCP Proxy settings must be identical on both the Anchor and Remote controllers.

For the wired guest, there is an idle timeout that runs in the controller. If no packets are received within the configured period from the client, the client is removed from the controller. When a client sends an Address Resolution Protocol (ARP) request the next time, a new client entry is created and moved to the Web Auth/run state appropriately as per the security configuration.

Platform Support

Wired guest access is supported on these platforms:

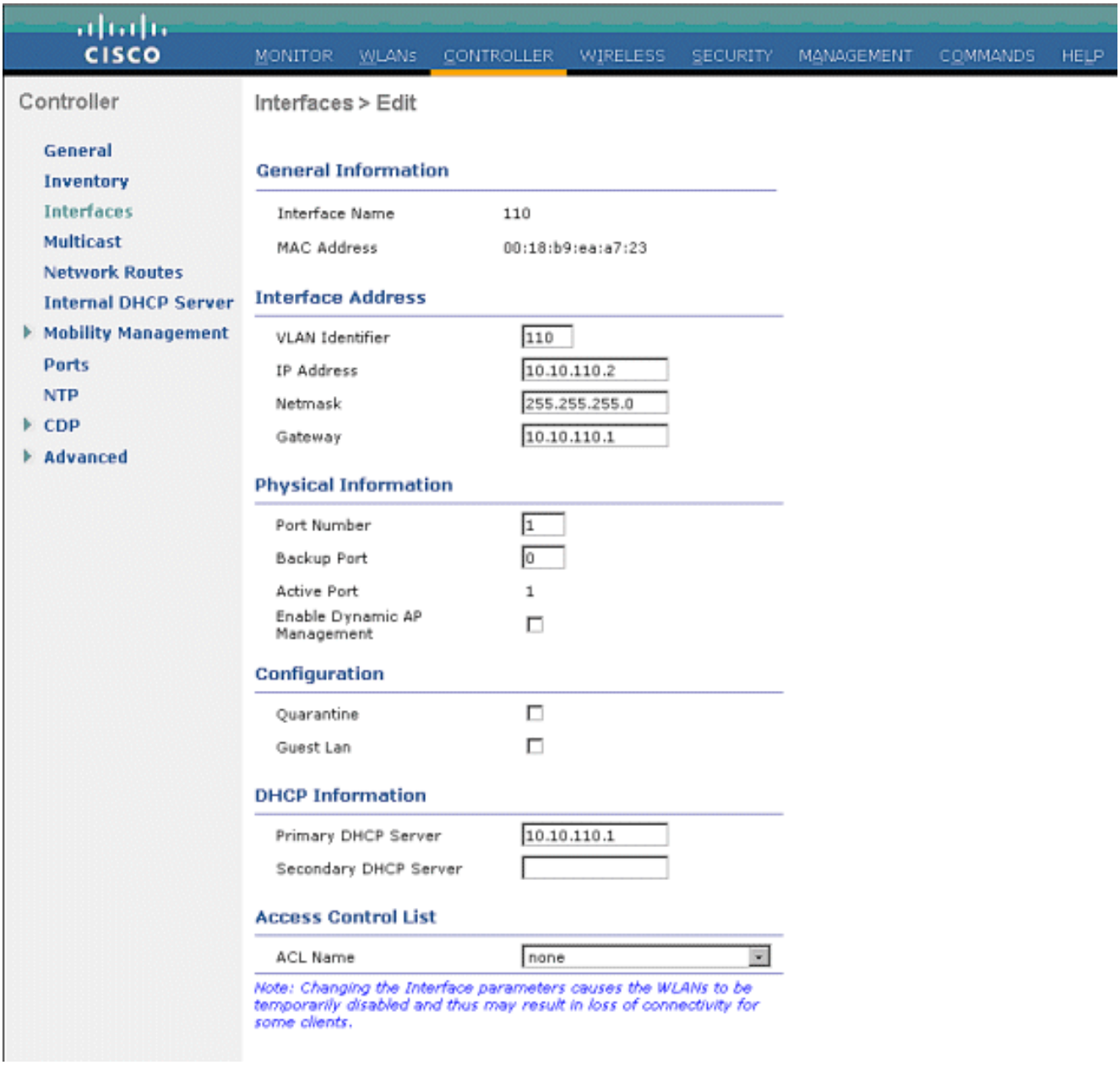
- Cisco WLC 4402, 4404, WiSM, 3750G, 5508, WiSM2, Virtual WLC

Wireless LAN Configuration

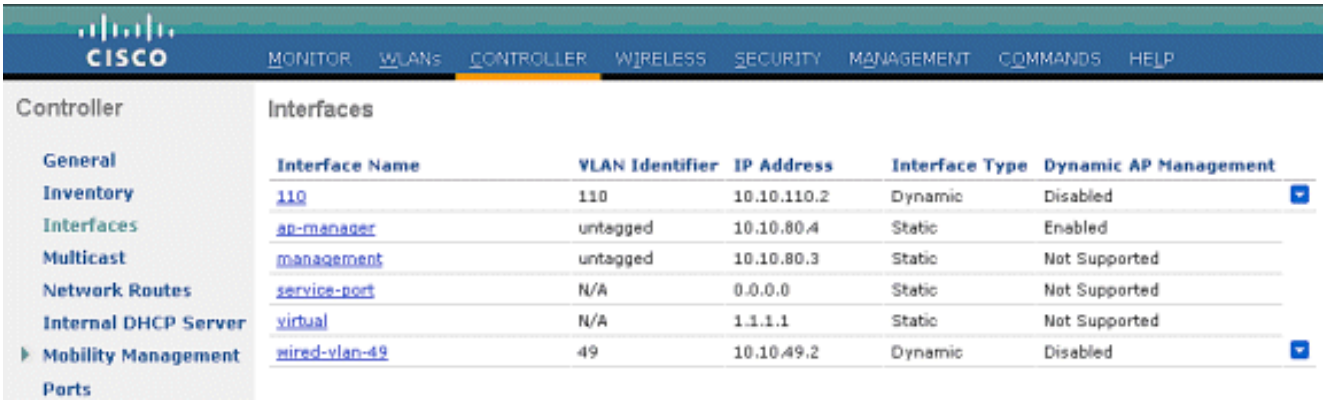
In this example, the basic configuration of the wireless LAN controller is assumed. The focus is on the additional configuration required to complete the wired guest access implementation.

1. Create a dynamic interface and mark it is as a “Guest LAN.” When you create this dynamic interface in the current release, you need to provide an IP address and default gateway, even though it does not exist since it is a Layer 2 VLAN; you need not provide any DHCP address. Wired guest clients are physically connected to this
   VLAN.

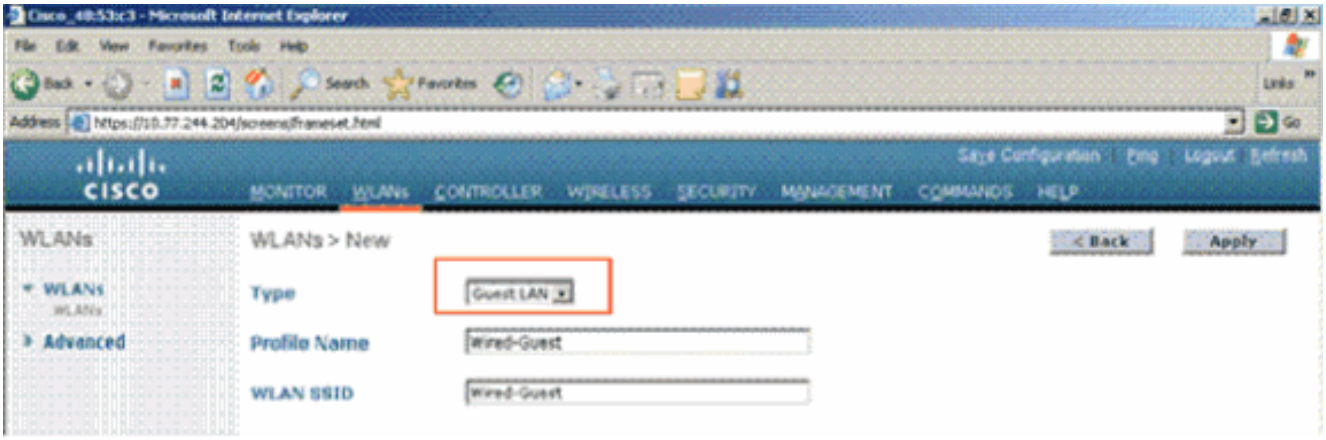
2. Create another dynamic interface where the wired guest clients receive an IP address.**Note**: You need to provide an IP address/ default gateway / DHCP server address in this interface.



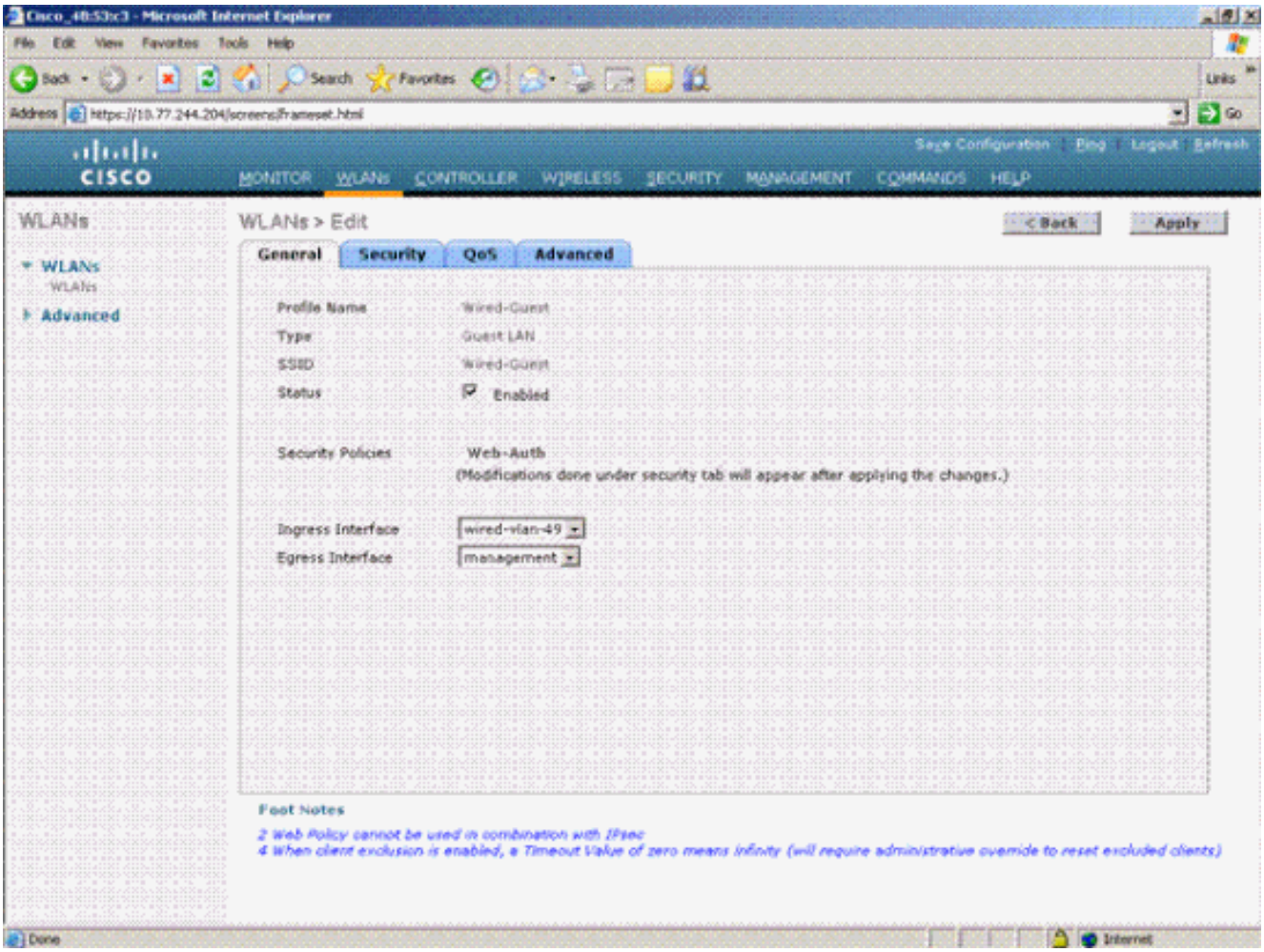
3. These are the dynamic interfaces:



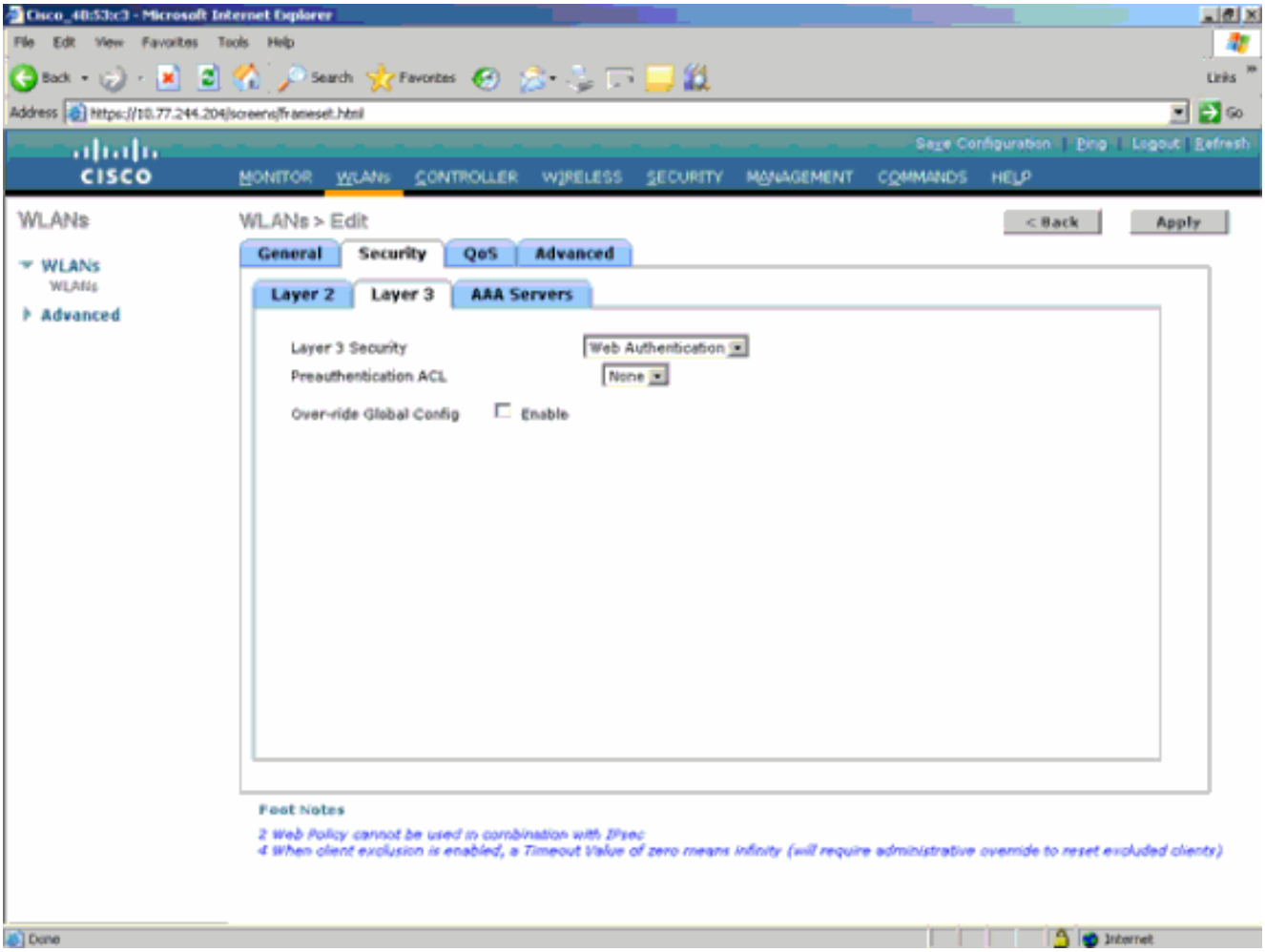
4. Add a new WLAN: Type=Guest LAN.



5. Enable the WLAN; map the ingress interface to the “Guest LAN” created in Step 1, and the egress interface can be a management interface or any other dynamic interface, although preferably a dynamic interface such as that created in Step 2.

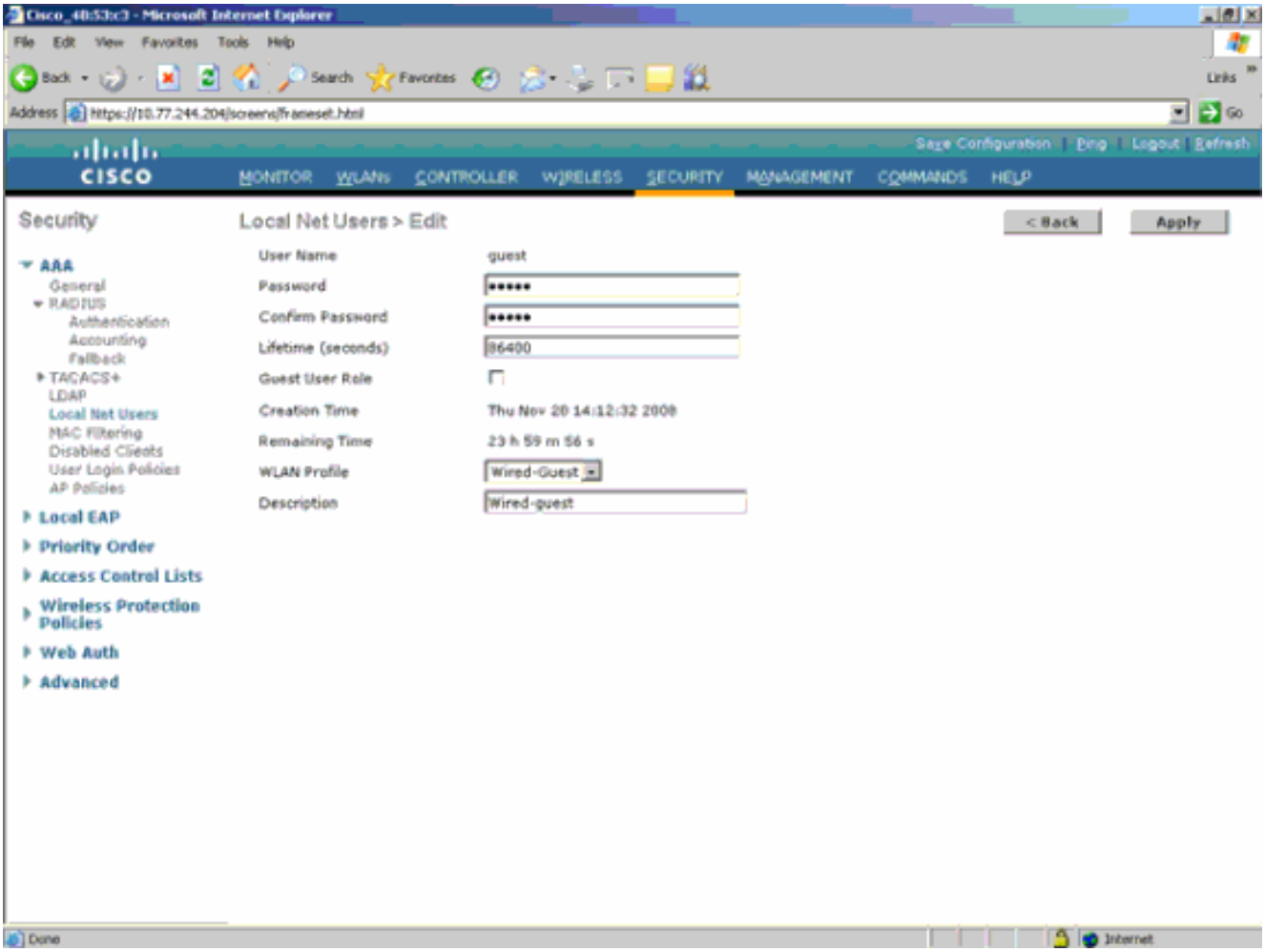


6. Web authentication is enabled by default as the security option configured on the Guest LAN. It can be changed to *None* or *Web Passthrough*.



7. This is the final configuration of the WLAN.

8. Add a guest user in the local database of the WLC.

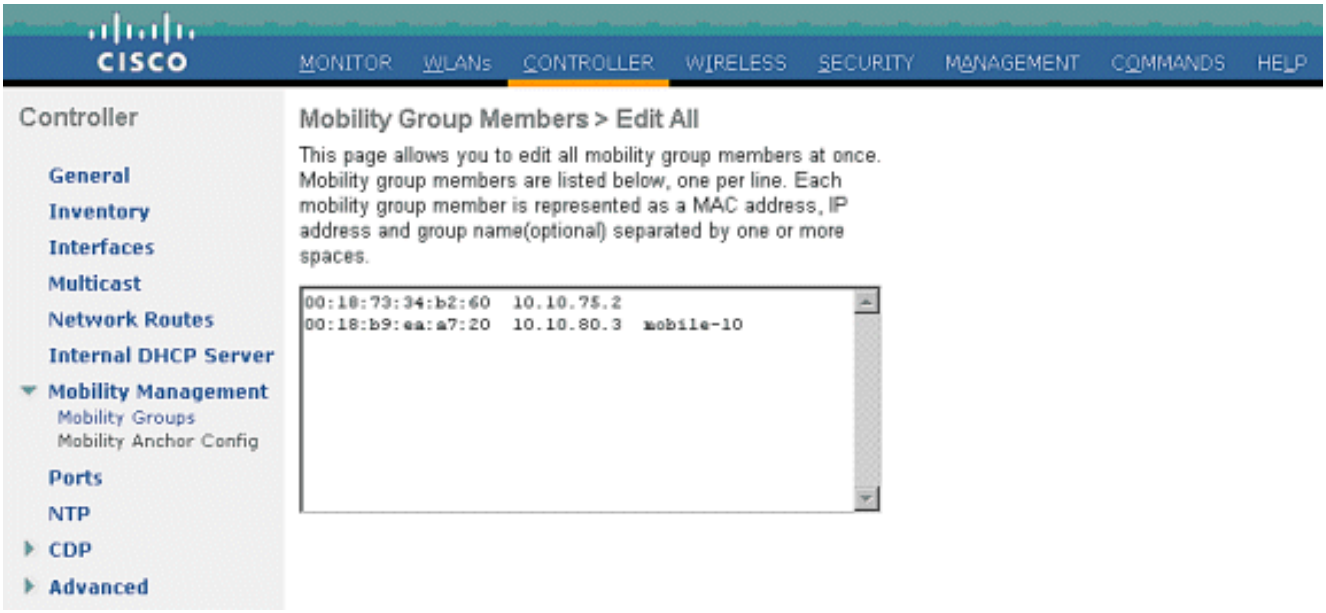


On the Foreign, you need to set the ingress as the configured “Guest LAN.” At the egress, you need to set it to some interface, possibly the management interface. However, once the EoIP tunnel is built, it sends the traffic automatically through the tunnel instead of the management address.

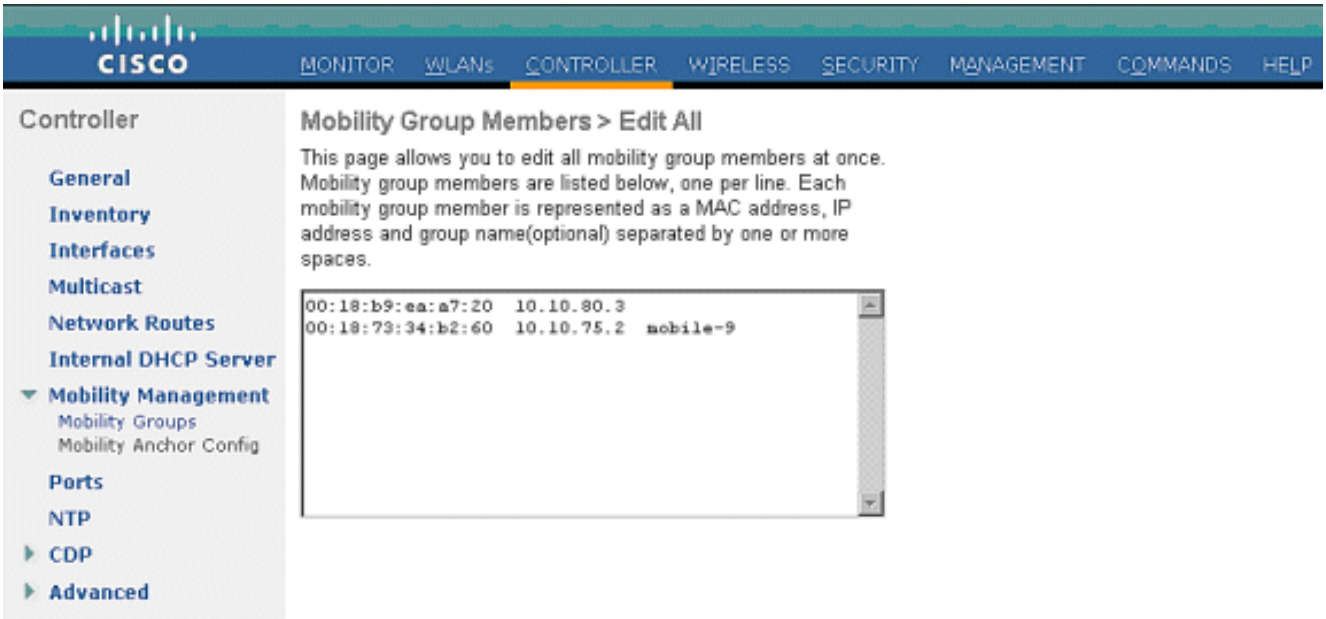
Wired Guest Access with Anchor WLAN Controller

In this example, the IP address of the remote wireless LAN controller is 10.10.80.3, and the IP address of the Anchor DMZ controller is 10.10.75.2. Both are part of two different mobility groups.

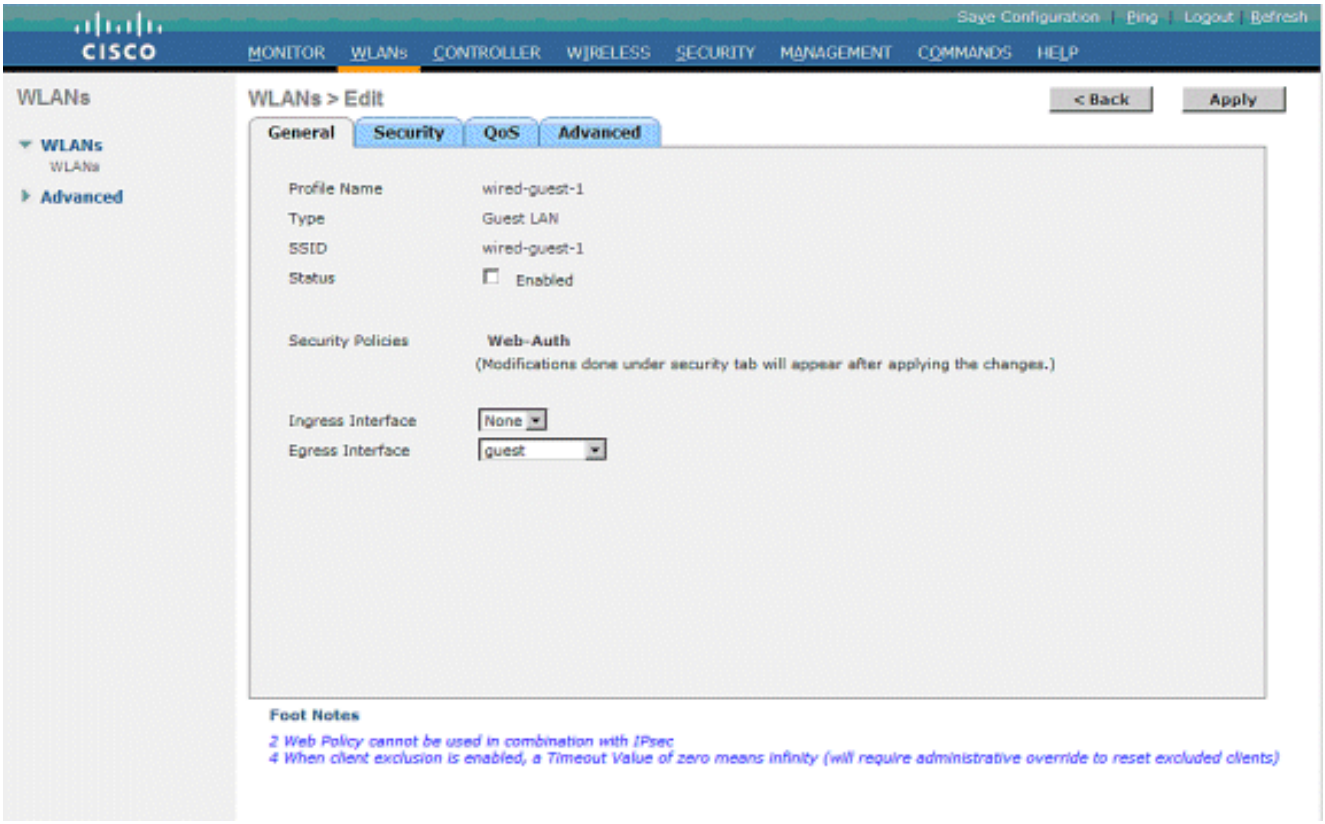
1. Configure the mobility group of the Anchor DMZ controller when you add the MAC address, IP address, and mobility group name of the remote controller.



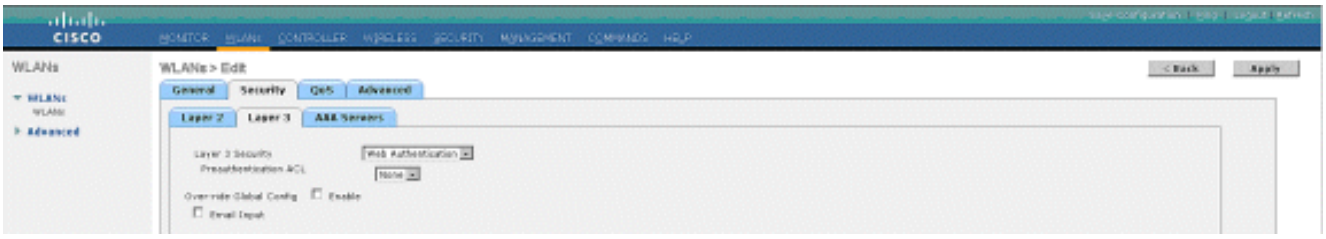
2. Similarly, configure the mobility group in the remote controller.



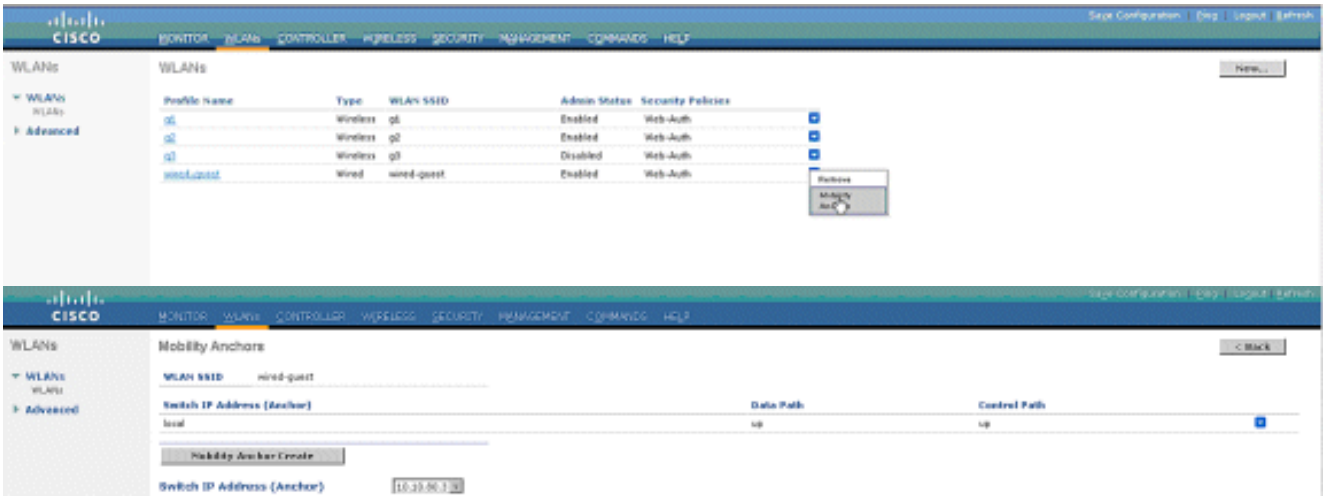
3. Create the wired WLAN with the exact name in the Anchor WLC. The ingress interface in this case is “none” because, logically, the ingress interface is the EoIP tunnel from the remote controller. The egress interface is a different interface, where the wired clients go to receive the IP address. In this example, a dynamic interface called *guest* is created. However, at this stage you cannot enable the WLAN because it displays an error message, which reads that an ingress interface cannot be *none*.



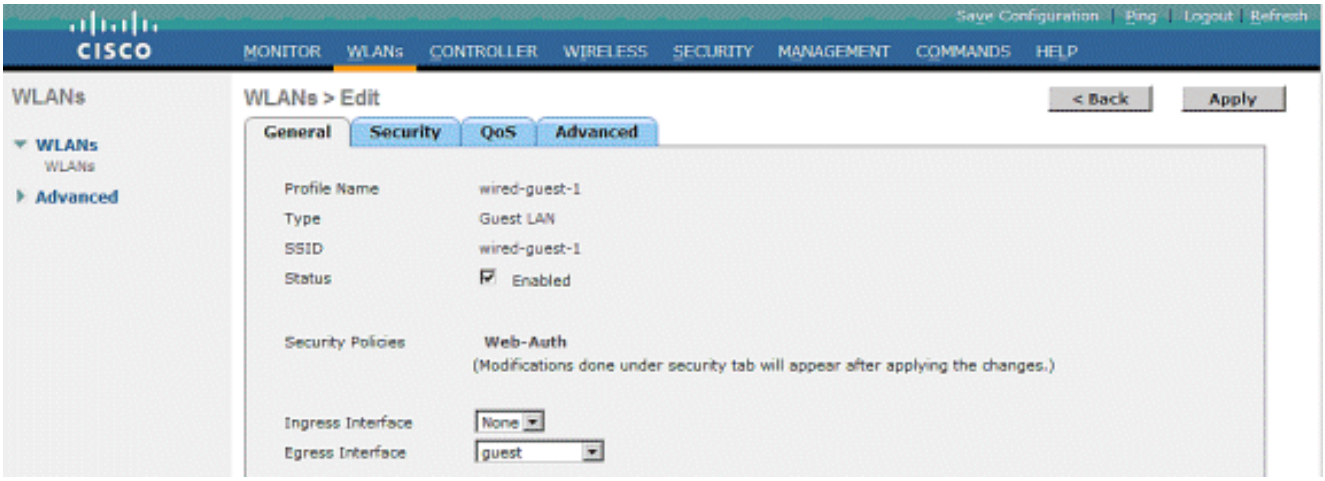
4. Configure Layer 3 security as *web authentication*, similar to the remote controller.



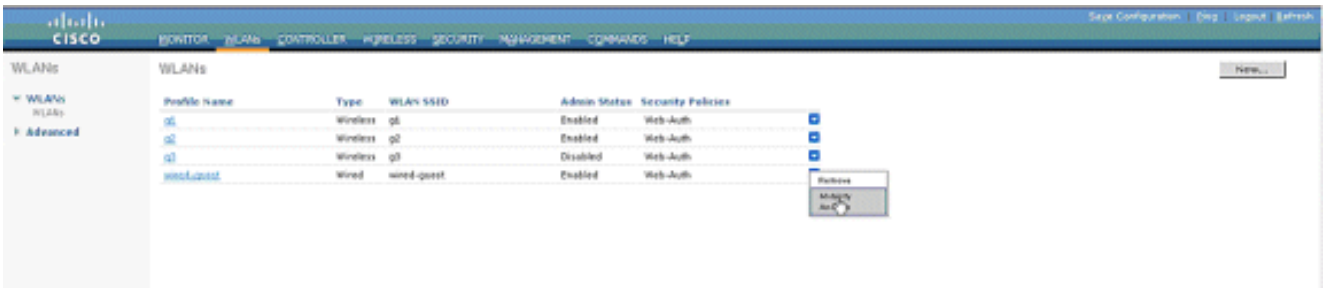
5. Create the mobility anchor on the anchor controller, and map it to itself.



6. Once the mobility anchor is created, go back and enable the wired WLAN.



7. Similarly, create the mobility anchor on the remote WLC for the wired guest WLAN.



Choose the IP address of the Anchor WLC and create the mobility anchor.

Check if the data and control path is up. If not, ensure these ports are open between the anchor and remote wireless LAN controller: UDP 16666 or IP 97.

8. Once a wired guest user is connected to the switch and has completed the web authentication, the Policy Manager State must be RUN, and the Mobility Role is Export Foreign.

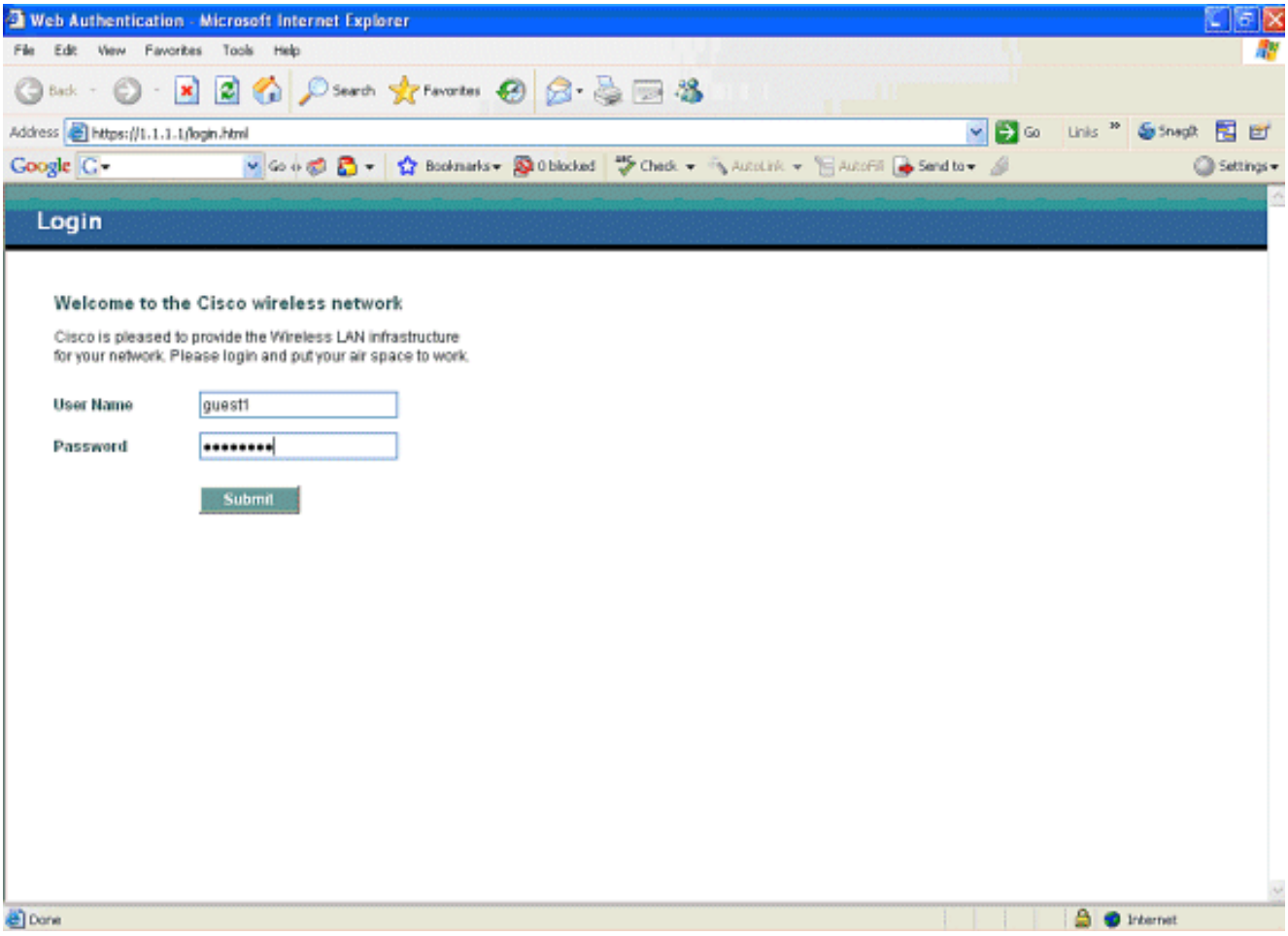
Similarly, check for the status in the Anchor WLC. The Policy Manager State must be RUN, and the Mobility Role is Export
Anchor.

Wired Guest Client Configuration

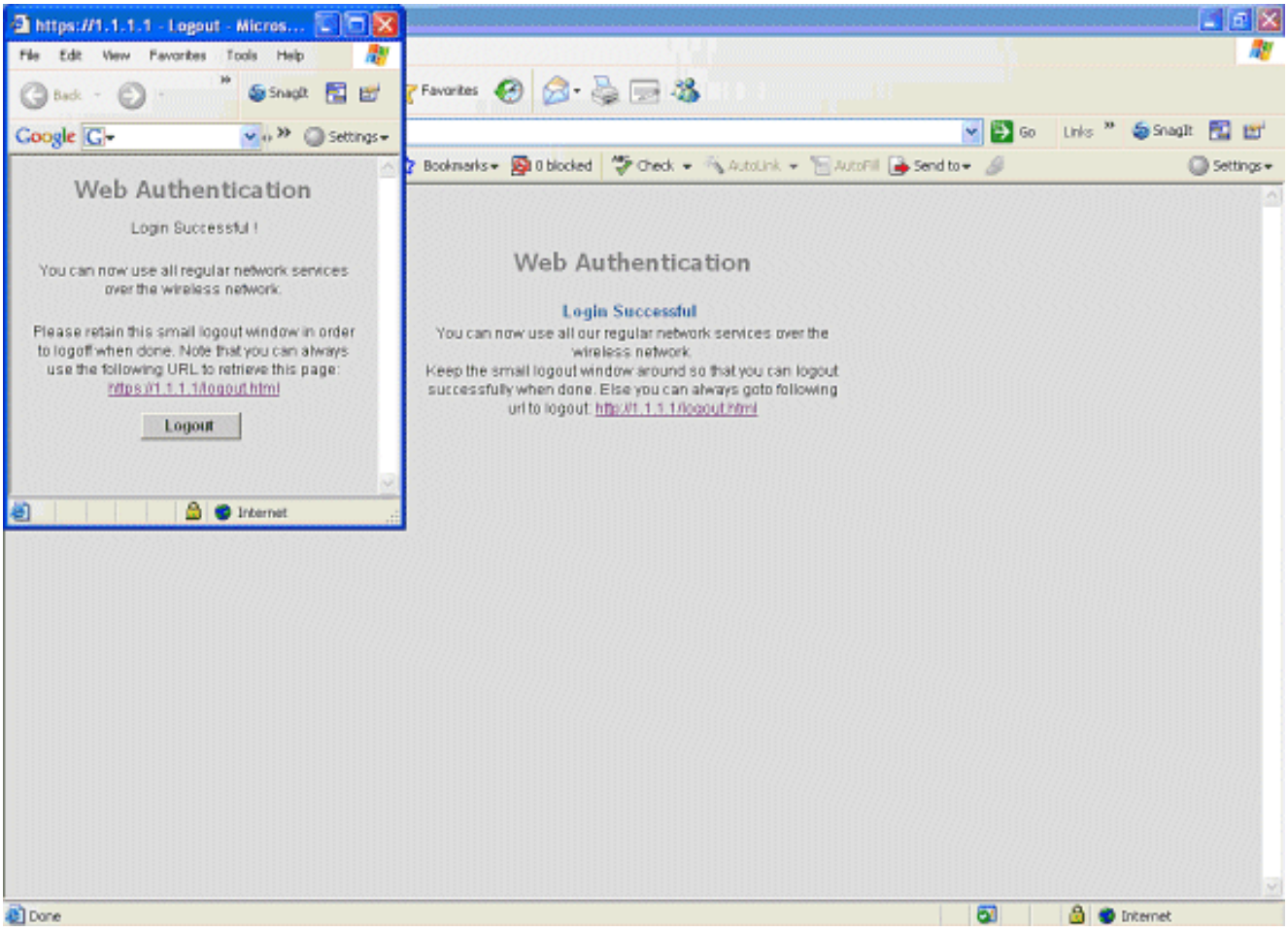
The wired guest client receives an IP address from the egress VLAN but cannot pass any traffic until it completes the web authentication process.

In order to log on as a guest user, follow these steps:

1. Open a browser window and enter the desired URL name (for example, www.cisco.com). The guest is redirected to the default webpage of the Wireless LAN controller if web authentication is enabled, and a DNS resolution can be completed for the URL that is entered. Otherwise, enter this URL: https://1.1.1.1/login.html, where the IP address 1.1.1.1 is the virtual IP address of the wireless LAN
controller.



2. Enter the username and password that are provided.
3. If the login is successful, a browser window notes that.



Debugs for Wired Guest Connection on Local WLC

This debug provides all the information related to the wired guest client.

debug client <mac-address>

```
 Cisco Controller) >show debug
MAC address ............................... 00:0d:60:5e:ca:62
Debug Flags Enabled:
  dhcp packet enabled.
  dot11 mobile enabled.
  dot11 state enabled
  dot1x events enabled.
  dot1x states enabled.
  pem events enabled.
  pem state enabled.

 (Cisco Controller) >Tue Sep 11 13:27:42 2007: 00:0d:60:5e:ca:62
   Adding mobile on Wired Guest 00:00:00:00:00:00(0)
Tue Sep 11 13:27:42 2007: 00:0d:60:5e:ca:62
   apfHandleWiredGuestMobileStation
  (apf_wired_guest.c:121) Changing state for mobile
   00:0d:60:5e:ca:62 on AP 00:00:00:
00:00:00 from Idle to Associated
Tue Sep 11 13:27:42 2007: 00:0d:60:5e:ca:62 0.0.0.0 START (0)
   Initializing policy
Tue Sep 11 13:27:42 2007: 00:0d:60:5e:ca:62 0.0.0.0 START (0)
   Change state to AUTHCHECK (2) last state AUTHCHECK (2)
Tue Sep 11 13:27:42 2007: 00:0d:60:5e:ca:62 0.0.0.0 AUTHCHECK (2)
   Change state to L2AUTHCOMPLETE (4) last state L2AUTHCOMPLETE (4)
Tue Sep 11 13:27:42 2007: 00:0d:60:5e:ca:62 0.0.0.0 L2AUTHCOMPLETE (4)
   Change state to DHCP_REQD (7) last state DHCP_REQD (7)
Tue Sep 11 13:27:42 2007: 00:0d:60:5e:ca:62
   apfPemAddUser2 (apf_policy.c:209) Changing state for mobile
   00:0d:60:5e:ca:62 on AP 00:00:00:00:00:00 from Associated to Associated
Tue Sep 11 13:27:42 2007: 00:0d:60:5e:ca:62 Session Timeout is 0 -
   not starting session timer for the mobile
Tue Sep 11 13:27:42 2007: 00:0d:60:5e:ca:62
   Stopping deletion of Mobile Station: (callerId: 48)
Tue Sep 11 13:27:42 2007: 00:0d:60:5e:ca:62
   Wired Guest packet from 10.10.80.252 on mobile
Tue Sep 11 13:27:43 2007: 00:0d:60:5e:ca:62
   Wired Guest packet from 10.10.80.252 on mobile
Tue Sep 11 13:27:43 2007: 00:0d:60:5e:ca:62
   Orphan Packet from 10.10.80.252
Tue Sep 11 13:27:43 2007: 00:0d:60:5e:ca:62
   Wired Guest packet from 169.254.20.157 on mobile
Tue Sep 11 13:27:44 2007: 00:0d:60:5e:ca:62
   Wired Guest packet from 169.254.20.157 on mobile
Tue Sep 11 13:27:44 2007: 00:0d:60:5e:ca:62 0.0.0.0
   DHCP_REQD (7) State Update from Mobility-Incomplete
   to Mobility-Complete, mobility role=Local
Tue Sep 11 13:27:44 2007: 00:0d:60:5e:ca:62 0.0.0.0
   DHCP_REQD (7) pemAdvanceState2 3934, Adding TMP rule
Tue Sep 11 13:27:44 2007: 00:0d:60:5e:ca:62 0.0.0.0
   DHCP_REQD (7) Adding Fast Path rule
type = Airespace AP - Learn IP address on AP 00:00:00:00:00:00,
   slot 0, interface = 1, QOS = 0 ACL Id = 255,
   Jumbo Frames = NO, 802.1P = 0, DSCP = 0, TokenID = 5006
Tue Sep 11 13:27:44 2007: 00:0d:60:5e:ca:62 0.0.0.0 DHCP_REQD
   (7) Successfully plumbed mobile rule (ACL ID 255)
```

```
Tue Sep 11 13:27:44 2007: 00:0d:60:5e:ca:62
   Installing Orphan Pkt IP address 169.254.20.157 for station
Tue Sep 11 13:27:44 2007: 00:0d:60:5e:ca:62
   Unsuccessfully installed IP address 169.254.20.157 for station
Tue Sep 11 13:27:44 2007: 00:0d:60:5e:ca:62
   0.0.0.0 Added NPU entry of type 9
Tue Sep 11 13:27:44 2007: 00:0d:60:5e:ca:62
   Sent an XID frame
Tue Sep 11 13:27:45 2007: 00:0d:60:5e:ca:62
   Wired Guest packet from 169.254.20.157 on mobile
Tue Sep 11 13:27:48 2007: 00:0d:60:5e:ca:62
   DHCP received op BOOTREQUEST (1) (len 310, port 1, encap 0xec00)
Tue Sep 11 13:27:48 2007: 00:0d:60:5e:ca:62
   DHCP selecting relay 1 - control block settings:
dhcpServer: 0.0.0.0, dhcpNetmask: 0.0.0.0,
dhcpGateway: 0.0.0.0, dhcpRelay: 0.0.0.0  VLAN: 0
Tue Sep 11 13:27:48 2007: 00:0d:60:5e:ca:62
   DHCP selected relay 1 - 10.10.110.1(local address 10.10.110.2,
   gateway 10.10.110.1, VLAN 110, port 1)
Tue Sep 11 13:27:48 2007: 00:0d:60:5e:ca:62
   DHCP transmitting DHCP DISCOVER (1)
Tue Sep 11 13:27:48 2007: 00:0d:60:5e:ca:62
   DHCP   op: BOOTREQUEST, htype: Ethernet, hlen: 6, hops: 1
Tue Sep 11 13:27:48 2007: 00:0d:60:5e:ca:62
   DHCP   xid: 0x87214d01 (2267106561),secs: 0, flags: 8000
Tue Sep 11 13:27:48 2007: 00:0d:60:5e:ca:62
   DHCP   chaddr: 00:0d:60:5e:ca:62
Tue Sep 11 13:27:48 2007: 00:0d:60:5e:ca:62
   DHCP   ciaddr: 0.0.0.0,  yiaddr: 0.0.0.0
Tue Sep 11 13:27:48 2007: 00:0d:60:5e:ca:62
   DHCP   siaddr: 0.0.0.0,  giaddr: 10.10.110.2
Tue Sep 11 13:27:48 2007: 00:0d:60:5e:ca:62
   DHCP   requested ip:10.10.80.252
Tue Sep 11 13:27:48 2007: 00:0d:60:5e:ca:62
   DHCP ARPing for 10.10.110.1 (SPA 10.10.110.2, vlanId 110)
Tue Sep 11 13:27:48 2007: 00:0d:60:5e:ca:62
   DHCP selecting relay 2 - control block settings:
dhcpServer: 0.0.0.0, dhcpNetmask: 0.0.0.0,
dhcpGateway: 0.0.0.0, dhcpRelay: 10.10.110.2
   VLAN: 110
Tue Sep 11 13:27:48 2007: 00:0d:60:5e:ca:62
   DHCP selected relay 2 - NONE
Tue Sep 11 13:27:51 2007: 00:0d:60:5e:ca:62
   DHCP received op BOOTREQUEST (1) (len 310, port 1, encap 0xec00)

Tue Sep 11 13:27:51 2007: 00:0d:60:5e:ca:62
   DHCP selecting relay 1 - control block settings:
dhcpServer: 0.0.0.0, dhcpNetmask: 0.0.0.0,
dhcpGateway: 0.0.0.0, dhcpRelay: 10.10.110.2  VLAN: 110
Tue Sep 11 13:27:51 2007: 00:0d:60:5e:ca:62
   DHCP selected relay 1 - 10.10.110.1(local address 10.10.110.2,
   gateway 10.10.110.1, VLAN 110, port 1)
Tue Sep 11 13:27:51 2007: 00:0d:60:5e:ca:62
   DHCP transmitting DHCP DISCOVER (1)
Tue Sep 11 13:27:51 2007: 00:0d:60:5e:ca:62
   DHCP   op: BOOTREQUEST, htype: Ethernet, hlen: 6, hops: 1
Tue Sep 11 13:27:51 2007: 00:0d:60:5e:ca:62
   DHCP   xid: 0x87214d01 (2267106561),secs: 36957, flags: 8000
Tue Sep 11 13:27:51 2007: 00:0d:60:5e:ca:62
   DHCP   chaddr: 00:0d:60:5e:ca:62
Tue Sep 11 13:27:51 2007: 00:0d:60:5e:ca:62
   DHCP   ciaddr: 0.0.0.0,  yiaddr: 0.0.0.0
Tue Sep 11 13:27:51 2007: 00:0d:60:5e:ca:62
   DHCP   siaddr: 0.0.0.0,  giaddr: 10.10.110.2
```

```
Tue Sep 11 13:27:51 2007: 00:0d:60:5e:ca:62
   DHCP   requested ip: 10.10.80.252
Tue Sep 11 13:27:51 2007: 00:0d:60:5e:ca:62
   DHCP sending REQUEST to 10.10.110.1 (len 350, port 1, vlan 110)
Tue Sep 11 13:27:51 2007: 00:0d:60:5e:ca:62
   DHCP selecting relay 2 - control block settings:
dhcpServer: 0.0.0.0, dhcpNetmask: 0.0.0.0,
dhcpGateway: 0.0.0.0, dhcpRelay: 10.10.110.2  VLAN: 110
Tue Sep 11 13:27:51 2007: 00:0d:60:5e:ca:62
   DHCP selected relay 2 - NONE
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   DHCP received op BOOTREPLY (2) (len 308, port 1, encap 0xec00)
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   DHCP setting server from OFFER
   (server 10.10.110.1, yiaddr 10.10.110.3)
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   DHCP sending REPLY to Wired Client (len 350, port 1)
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   DHCP transmitting DHCP OFFER (2)
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   DHCP   op: BOOTREPLY, htype: Ethernet, hlen: 6, hops: 0
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   DHCP   xid: 0x87214d01 (2267106561), secs: 0, flags: 8000
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   DHCP   chaddr: 00:0d:60:5e:ca:62
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   DHCP   ciaddr: 0.0.0.0,  yiaddr: 10.10.110.3
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   DHCP   siaddr: 0.0.0.0,  giaddr: 0.0.0.0
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   DHCP   server id: 1.1.1.1  rcvd server id: 10.10.110.1
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   DHCP received op BOOTREQUEST (1) (len 334, port 1, encap 0xec00)
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   DHCP selecting relay 1 - control block settings:
dhcpServer: 10.10.110.1, dhcpNetmask: 0.0.0.0,
dhcpGateway: 0.0.0.0, dhcpRelay: 10.10.110.2  VLAN: 110
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   DHCP selected relay 1 - 10.10.110.1(local address 10.10.110.2,
   gateway 10.10.110.1, VLAN 110, port 1)
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   DHCP transmitting DHCP REQUEST (3)
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   DHCP   op: BOOTREQUEST, htype: Ethernet, hlen: 6, hops: 1
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   DHCP   xid: 0x87214d01 (2267106561),secs: 36957, flags: 8000
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   DHCP   chaddr: 00:0d:60:5e:ca:62
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   DHCP   ciaddr: 0.0.0.0,  yiaddr: 0.0.0.0
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   DHCP   siaddr: 0.0.0.0,  giaddr: 10.10.110.2
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   DHCP   requested ip: 10.10.110.3
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   DHCP   server id: 10.10.110.1  rcvd server id: 1.1.1.1
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   DHCP sending REQUEST to 10.10.110.1(len 374, port 1, vlan 110)
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   DHCP selecting relay 2 - control block settings:
dhcpServer: 10.10.110.1, dhcpNetmask: 0.0.0.0,
dhcpGateway: 0.0.0.0, dhcpRelay: 10.10.110.2  VLAN: 110
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   DHCP selected relay 2 -NONE
```

```
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   DHCP received op BOOTREPLY (2) (len 308, port 1, encap 0xec00)
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   10.10.110.3 DHCP_REQD (7) Change state to WEBAUTH_REQD
   (8) last state WEBAUTH_REQD (8)
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   10.10.110.3 WEBAUTH_REQD (8) pemAdvanceState2
   4598, Adding TMP rule
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   10.10.110.3 WEBAUTH_REQD (8) Replacing Fast Path rule
  type = Airespace AP Client - ACL passthru
  on AP 00:00:00:00:00:00, slot 0, interface = 1, QOS = 0
  ACL Id = 255, Jumbo Frames = NO, 802.1P = 0, DSCP = 0, TokenID = 5006
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   10.10.110.3 WEBAUTH_REQD (8) Successfully
   plumbed mobile rule (ACL ID 255)
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   Plumbing web-auth redirect rule due to user logout
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   Adding Web RuleID 31 for mobile 00:0d:60:5e:ca:62
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   Assigning Address 10.10.110.3 to mobile
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   DHCP sending REPLY to Wired Client (len 350, port 1)
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   DHCP transmitting DHCP ACK (5)
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   DHCP   op: BOOTREPLY, htype: Ethernet, hlen: 6, hops: 0
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   DHCP   xid: 0x87214d01 (2267106561),secs: 0, flags: 8000
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   DHCP   chaddr: 00:0d:60:5e:ca:62

Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   DHCP   ciaddr: 0.0.0.0,  yiaddr: 10.10.110.3
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   DHCP   siaddr: 0.0.0.0,  giaddr: 0.0.0.0
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   DHCP   server id: 1.1.1.1  rcvd server id: 10.10.110.1
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   10.10.110.3 Added NPU entry of type 2
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62 Sent an XID frame
Tue Sep 11 13:28:12 2007: 00:0d:60:5e:ca:62
   Username entry (guest1) created for mobile
Tue Sep 11 13:28:12 2007: 00:0d:60:5e:ca:62
   Setting guest session timeout for mobile
   00:0d:60:5e:ca:62 to 79953 seconds
Tue Sep 11 13:28:12 2007: 00:0d:60:5e:ca:62
   Session Timeout is 79953 - starting session timer for the mobile
Tue Sep 11 13:28:12 2007: 00:0d:60:5e:ca:62
   10.10.110.3 WEBAUTH_REQD (8) Change state to
   WEBAUTH_NOL3SEC (14) last state WEBAUTH_NOL3SEC (14)
Tue Sep 11 13:28:12 2007: 00:0d:60:5e:ca:62
   10.10.110.3 WEBAUTH_NOL3SEC (14) Change state to RUN
   (20) last state RUN (20)
Tue Sep 11 13:28:12 2007: 00:0d:60:5e:ca:62 10.10.110.3 RUN
   (20) Reached PLUMBFA STPATH: from line 4518
Tue Sep 11 13:28:12 2007: 00:0d:60:5e:ca:62 10.10.110.3 RUN
   (20) Replacing FastPath rule
type = Airespace AP Client
on AP 00:00:00:00:00:00, slot 0, interface = 1, QOS = 0
ACL Id = 255, Jumbo Frames = NO, 802.1P = 0, DSCP = 0, TokenID = 5006
Tue Sep 11 13:28:12 2007: 00:0d:60:5e:ca:62 10.10.110.3 RUN
   (20) Successfully plumbed mobile rule (ACL ID 255)
```

```
Tue Sep 11 13:28:12 2007: 00:0d:60:5e:ca:62 10.10.110.3
   Added NPU entry of type 1
Tue Sep 11 13:28:12 2007: 00:0d:60:5e:ca:62 Sending a gratuitous
   ARP for 10.10.110.3, VLAN Id 110
```

Verify

There is currently no verification procedure available for this configuration.

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.

Related Information

- **Configuring Auto-Anchor Mobility**
- **Guest WLAN and Internal WLAN using WLCs Configuration Example**
- **External Web Authentication with Wireless LAN Controllers Configuration Example**
- **Cisco Wireless LAN Controller Configuration Guide, Release 4.2**
- **Wireless Product Support**
- **Technical Support & Documentation - Cisco Systems**