

Guest WLAN and Internal WLAN using WLCs Configuration Example

Document ID: 70937

Introduction

Prerequisites

- Requirements
- Components Used
- Conventions

Network Setup

Configure

- Configure Dynamic Interfaces on the WLC for the Guest and Internal Users
- Create WLANs for the Guest and Internal Users
- Configure the Layer 2 Switch Port that Connects to the WLC as Trunk Port
- Configure the Router for the Two WLANs

Verify

Troubleshoot

- Troubleshooting Procedure
- Troubleshooting Commands

NetPro Discussion Forums – Featured Conversations

Related Information

Introduction

This document provides a configuration example for a guest wireless LAN (WLAN) and a secure internal WLAN that use WLAN controllers (WLCs) and lightweight access points (LAPs). In the configuration in this document, the guest WLAN uses web authentication to authenticate users and the secure internal WLAN uses Extensible Authentication Protocol (EAP) authentication.

Prerequisites

Requirements

Ensure that you meet these requirements before you attempt this configuration:

- Knowledge of how to configure the WLC with basic parameters
- Knowledge of how to set up a DHCP and Domain Name System (DNS) server

Components Used

The information in this document is based on these software and hardware versions:

- Cisco 2006 WLC that runs firmware release 4.0
- Cisco 1000 Series LAP
- Cisco 802.11a/b/g Wireless Client Adapter that runs firmware release 2.6
- Cisco 2811 router that runs Cisco IOS® version 12.4(2)XA
- Cisco 3500 XL Series Switch that runs Cisco IOS version 12.0(5)WC3b
- DNS server that runs on a Microsoft Windows 2000 server

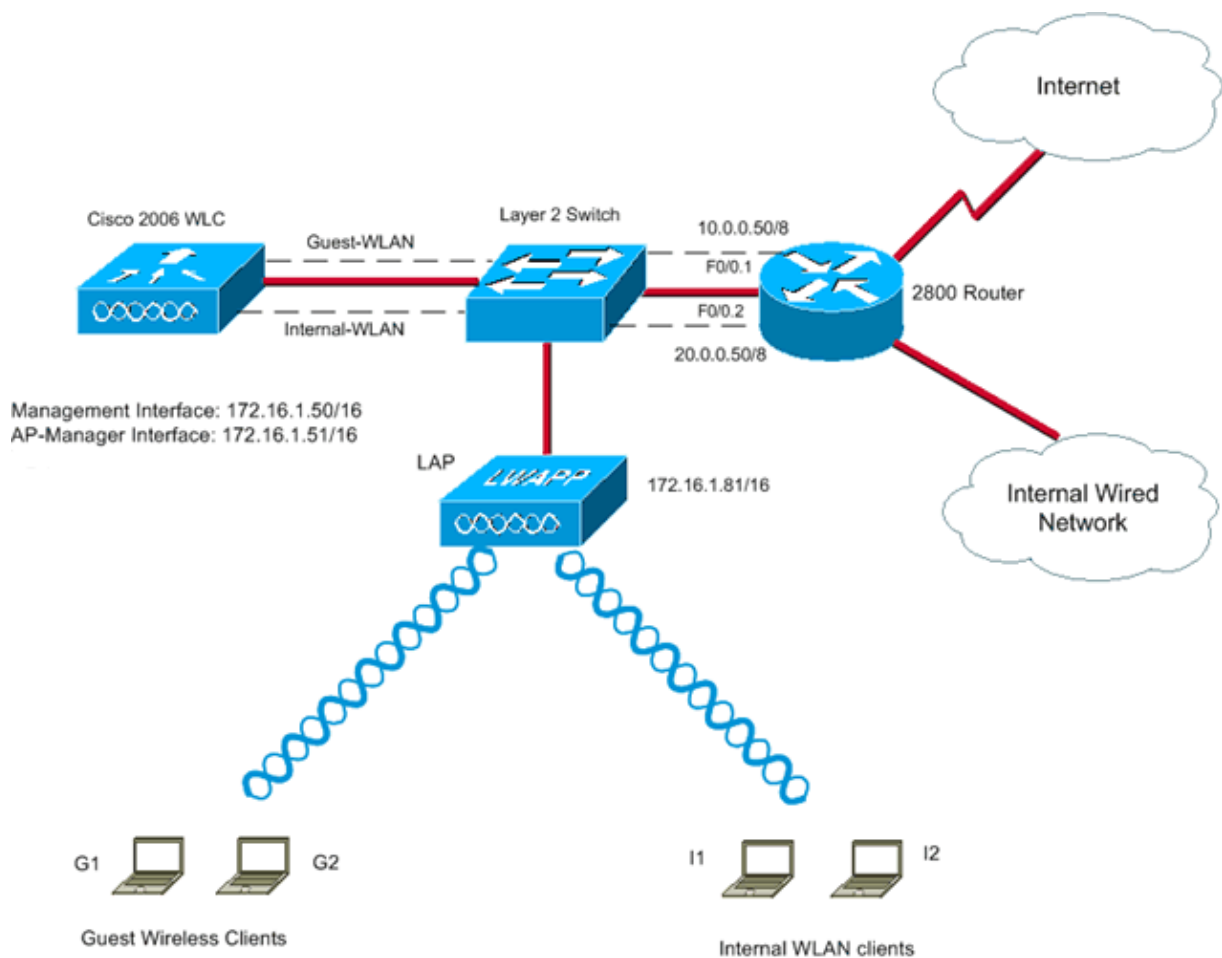
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Network Setup

The configuration example in this document uses the setup displayed in this diagram. The LAP is registered to the WLC. The WLC is connected to the Layer 2 switch. The router that connects the users to the WAN also connects to the Layer 2 switch. You need to create two WLANs, one for the guest users and the other for the internal LAN users. You also need a DHCP server to provide IP addresses for the guest and internal wireless clients. The guest users use web authentication in order to access the network. The internal users use EAP authentication. The 2811 router also acts as the DHCP server for the wireless clients.



Note: This document assumes that the WLC is configured with the basic parameters and the LAP is registered to the WLC. Refer to Lightweight AP (LAP) Registration to a Wireless LAN Controller (WLC) for information on how to configure the basic parameters on a WLC and how to register the LAP to WLC.

When configured as a DHCP server, some of the firewalls do not support DHCP requests from a relay agent. The WLC is a relay agent for the client. The firewall configured as a DHCP server ignores these requests. Clients must be directly connected to the firewall and cannot send requests through another relay agent or router. The firewall can work as a simple DHCP server for internal hosts that are directly connected to it. This

allows the firewall to maintain its table based on the MAC addresses that are directly connected and that it can see. This is why an attempt to assign addresses from a DHCP relay are not available and the packets are discarded. PIX Firewall has this limitation.

Configure

Complete these steps in order to configure the devices for this network setup:

1. Configure Dynamic Interfaces on the WLC for the Guest and Internal Users
2. Create WLANs for the Guest and Internal Users
3. Configure the Layer 2 Switch Port that Connects to the WLC as Trunk Port
4. Configure the Router for the Two VLANs

Configure Dynamic Interfaces on the WLC for the Guest and Internal Users

The first step is to create two dynamic interfaces on the WLC, one for the guest users and the other for internal users.

The example in this document uses these parameters and values for the dynamic interfaces:

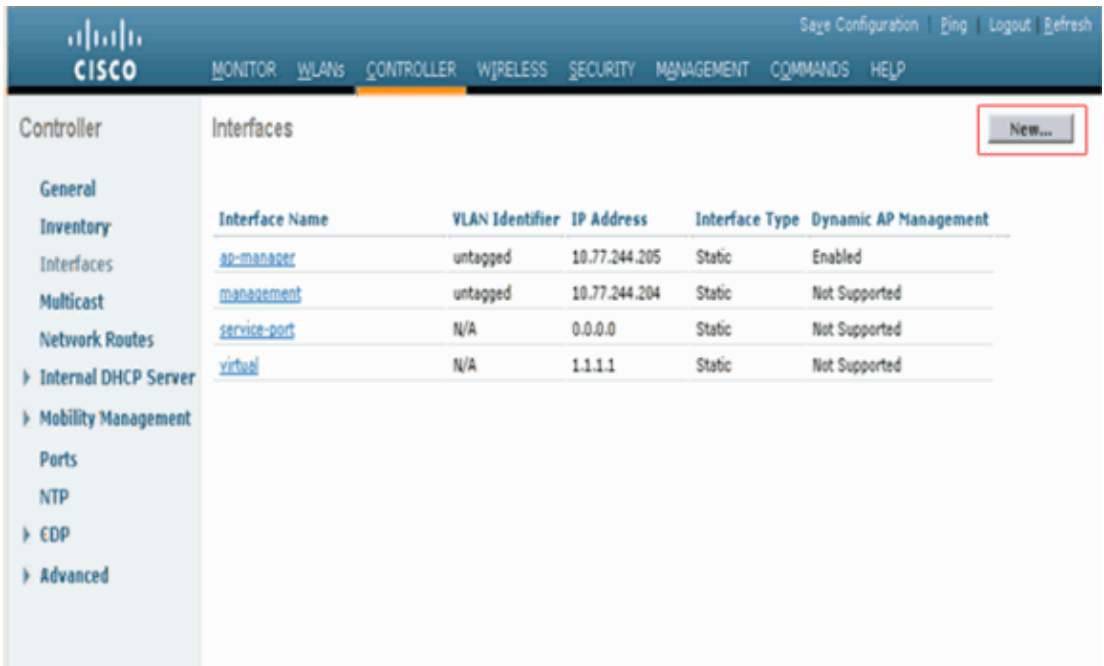
```
Guest-WLAN
VLAN Id : 10
IP address: 10.0.0.10
Netmask: 255.0.0.0
Gateway: 10.0.0.50
Physical port on WLC: 1
DHCP server: 172.16.1.60
```

```
Internal-WLAN
VLAN Id : 20
IP address: 20.0.0.10
Netmask: 255.0.0.0
Gateway: 20.0.0.50
Physical port on WLC: 1
DHCP server: 172.16.1.60
```

Complete these steps:

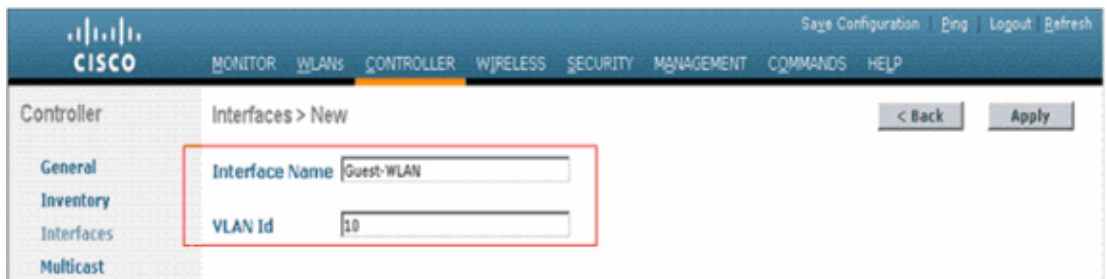
1. From the WLC GUI, choose **Controllers > Interfaces**.

The Interfaces window appears. This window lists the interfaces that are configured on the controller. This includes the default interfaces, which are the management interface, ap-manager interface, the virtual interface and the service port interface, and the user defined dynamic interfaces.



2. Click **New** in order to create a new dynamic interface.
3. In the Interfaces > New window, enter the Interface Name and the VLAN Id. Then, click **Apply**.

In this example, the dynamic interface is named Guest-WLAN and the VLAN Id is assigned 10.



4. In the Interfaces > Edit window, for the dynamic interface, enter the IP address, the subnet mask, and the default gateway. Assign it to a physical port on the WLC, and enter the IP address of the DHCP server. Then, click **Apply**.

This is the example:

Interfaces > Edit < Back Apply

General Information

Interface Name	Guest-WLAN
MAC Address	00:0b:85:48:53:c0

Configuration

Guest Lan	<input type="checkbox"/>
Quarantine	<input type="checkbox"/>

Physical Information

Port Number	<input type="text" value="2"/>
Backup Port	<input type="text" value="0"/>
Active Port	0
Enable Dynamic AP Management	<input type="checkbox"/>

Interface Address

VLAN Identifier	<input type="text" value="10"/>
IP Address	<input type="text" value="10.0.0.10"/>
Netmask	<input type="text" value="255.0.0.0"/>
Gateway	<input type="text" value="10.0.0.50"/>

DHCP Information

Primary DHCP Server	<input type="text" value="172.16.1.60"/>
---------------------	--

- The same procedure must be completed in order to create a dynamic interface for the Internal WLAN.
5. In the Interfaces > New window, enter **Internal-WLAN** for the dynamic interface for the internal users, and enter **20** for the VLAN Id. Then, click **Apply**.

CISCO Save Configuration Ping Logout Refresh

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP

Controller

- General
- Inventory
- Interfaces
- Multicast

Interfaces > New < Back Apply

Interface Name

VLAN Id

6. In the Interfaces > Edit window, for the dynamic interface, enter the IP address, the subnet mask, and the default gateway. Assign it to a physical port on the WLC, and enter the IP address of the DHCP server. Then, click **Apply**.

Interfaces > Edit < Back Apply

General Information

Interface Name: internal-wlan
 MAC Address: 00:0b:85:48:53:o4

Configuration

Guest Lan:
 Quarantine:

Physical Information

Port Number:
 Backup Port:
 Active Port: 2
 Enable Dynamic AP Management:

Interface Address

VLAN Identifier:
 IP Address:
 Netmask:
 Gateway:

DHCP Information

Primary DHCP Server:

Now that two dynamic interfaces are created, the Interfaces window summarizes the list of interfaces configured on the controller.

Controller	Interfaces New...					
	Interface Name	VLAN Identifier	IP Address	Interface Type	Dynamic AP Management	
General	ap-manager	untagged	10.77.244.207	Static	Enabled	
Inventory	guest-wlan	10	10.0.0.10	Dynamic	Disabled	<input type="checkbox"/>
Interfaces	internal-wlan	20	20.0.0.10	Dynamic	Disabled	<input type="checkbox"/>
Multicast	management	untagged	10.77.244.206	Static	Not Supported	
Network Routes	service-port	N/A	2.2.2.2	Static	Not Supported	
Internal DHCP Server	virtual	N/A	1.1.1.1	Static	Not Supported	
Mobility Management						

Create WLANs for the Guest and Internal Users

The next step is to create WLANs for the guest users and the internal users, and map the dynamic interface to the WLANs. Also, the security methods that are used to authenticate the guest and wireless users must be defined. Complete these steps:

1. Click **WLANs** from the controller GUI in order to create a WLAN.

The WLANs window appears. This window lists the WLANs configured on the controller.

2. Click **New** in order to configure a new WLAN.

In this example, the WLAN is named *Guest* and the WLAN ID is 2.

WLANs > New

Type: WLAN

Profile Name: Guest

WLAN SSID: Guest

3. Click **Apply** in top right corner.
4. The WLAN > Edit screen appears, which contains various tabs.

- a. Under the **General** tab for the guest WLAN, choose **guest-wlan** from the Interface Name field. This maps the dynamic interface **guest-wlan** that was previously created to the WLAN **Guest**.
- b. Make sure that the Status of the WLAN is enabled.

WLANs > Edit

General Security QoS Advanced

Profile Name: Guest

Type: WLAN

SSID: Guest

Status: Enabled

Security Policies: Web-Auth
(Modifications done under security tab will appear after applying the changes.)

Radio Policy: All

Interface: guest-wlan

Broadcast SSID: Enabled

- c. Click the **Security** tab. For this WLAN, Web Authentication a Layer 3 security mechanism is used to authenticate clients. Therefore, choose **None** under the *Layer 2* Security field. In the *Layer 3* Security field, check the **Web Policy** box and choose the **Authentication** option.

WLANs > Edit

General Security QoS Advanced

Layer 2 Layer 3 AAA Servers

Layer 3 Security: None

Web Policy

Authentication

Passthrough

Note: For more information on Web Authentication, refer to Wireless LAN Controller Web Authentication Configuration Example.

- d. Click **Apply**.
5. Create a WLAN for the internal users. In the WLANs > New window, enter **Internal** and choose **3** in order to create a WLAN for the internal users. Then, click **Apply**.

6. The WLANs > Edit window appears. Under the *General* Tab, choose **internal-wlan** from the Interface Name field.

This maps the dynamic interface **internal-wlan** that was previously created to the WLAN **Internal**. Make sure that the WLAN is enabled.

WLANs > Edit

General Security QoS Advanced

Profile Name Internal
Type WLAN
SSID Internal
Status Enabled
Security Policies [WPA2][Auth(802.1X)]
(Modifications done under security tab will appear after applying the changes.)
Radio Policy All
Interface internal-wlan
Broadcast SSID Enabled

Leave the Layer 2 Security option at the default value 802.1x because EAP authentication is used for the internal WLAN users.

WLANs > Edit

General Security QoS Advanced

Layer 2 Layer 3 AAA Servers

Layer 2 Security 802.1X
 MAC Filtering

802.1X Parameters

802.11 Data Encryption	Type	Key Size
<input checked="" type="radio"/>	WEP	104 bits

7. Click **Apply**.

The WLAN window appears and it shows the list of WLANs that are created.

WLANs

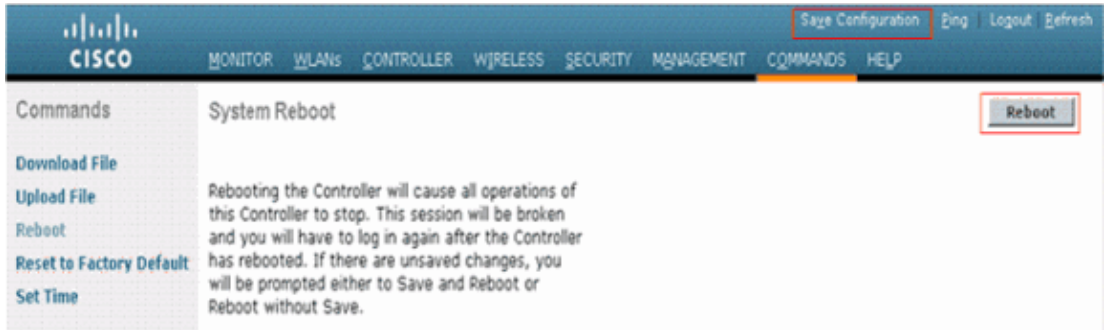
WLANs Entries 1 - 2 of 2

Current Filter: None [Change Filter] [Clear Filter] [Create New] [Go]

WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies
1	WLAN	Guest	Guest	Disabled	Web-Auth
2	WLAN	Internal	Internal	Enabled	[WPA2][Auth(802.1X)]

Note: Refer to EAP Authentication with WLAN Controllers (WLC) Configuration Example for more detailed information on how to configure an EAP-based WLAN with WLCs.

8. On the WLC GUI, click **Save Configuration**, then click **Commands** from the controller GUI. Next, choose the **Reboot** option to reboot the WLC in order to allow web authentication to take effect.



Note: Click **Save Configuration** in order to save the configuration across reboots.

Configure the Layer 2 Switch Port that Connects to the WLC as Trunk Port

You need to configure the switch port to support the multiple VLANs configured on the WLC because the WLC is connected to a Layer 2 switch. You must configure the switch port as an 802.1Q trunk port.

Each controller port connection is an 802.1Q trunk and should be configured as this on the neighbor switch. On Cisco switches, the native VLAN of an 802.1Q trunk, for example **VLAN 1**, is left untagged. Therefore, if you configure a controller's interface to use the native VLAN on a neighbor Cisco switch, make sure you configure the interface on the controller as untagged.

A zero value for the **VLAN** identifier (on the Controller > Interfaces window) means that the interface is untagged. In the example in this document, the AP-Manager and Management Interfaces are configured in the default untagged VLAN.

When a controller interface is set to a non-zero value, it should not be tagged to the native VLAN of the switch and the VLAN must be allowed on the switch. In this example, VLAN 60 is configured as the native VLAN on the switch port that connects to the controller.

This is the configuration for the switch port that connects to the WLC:

```
interface f0/12
Description Connected to the WLC
switchport trunk encapsulation dot1q
switchport trunk native vlan 60
switchport trunk allowed vlan 10,20,60
switchport mode trunk
no ip address
```

This is the configuration for the switch port that connects to the router as a trunk port:

```
interface f0/10
Description Connected to the Router
switchport trunk encapsulation dot1q
switchport trunk native vlan 60
switchport trunk allowed vlan 10,20,60
switchport mode trunk
no ip address
```

This is the configuration for the switch port that connects to the LAP. This port is configured as an access port:

```
interface f0/9
Description Connected to the LAP
Switchport access vlan 60
switchport mode access
no ip address
```

Configure the Router for the Two WLANs

In the example in this document, the 2811 router connects the guest users to the Internet and also connects the internal wired users to the internal wireless users. You also need to configure the router to provide DHCP services.

On the router, create sub-interfaces under the FastEthernet interface which connects to the trunk port on the switch for every VLAN. Assign the sub-interfaces to the corresponding VLANs, and configure an IP address from the respective subnets.

Note: Only relevant portions of the router configuration are given, and not the complete configuration.

This is the configuration required on the router to accomplish this.

These are the commands that must be issued in order to configure DHCP services on the router:

```
!
ip dhcp excluded-address 10.0.0.10

!--- IP excluded because this IP is assigned to the dynamic
!--- interface created on the WLC.

ip dhcp excluded-address 10.0.0.50

!--- IP excluded because this IP is assigned to the
!--- sub-interface on the router.

ip dhcp excluded-address 20.0.0.10

!--- IP excluded because this IP is assigned to the dynamic
!--- interface created on the WLC.

ip dhcp excluded-address 20.0.0.50

!--- IP excluded because this IP is assigned to the sub-interface on the router.

!
ip dhcp pool Guest

!--- Creates a DHCP pool for the guest users.

    network 10.0.0.0 255.0.0.0
    default-router 10.0.0.50
    dns-server 172.16.1.1

!--- Defines the DNS server.

!
ip dhcp pool Internal
    network 20.0.0.0 255.0.0.0
    default-router 20.0.0.50

!--- Creates a DHCP pool for the internal users.

!
```

These commands must be issued on the FastEthernet interface for the example setup:

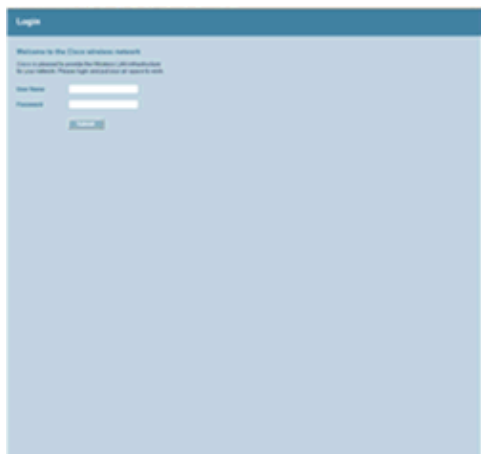
```
!  
interface FastEthernet0/0  
  description Connected to L2 Switch  
  ip address 172.16.1.60 255.255.0.0  
  duplex auto  
  speed auto  
  
!--- Interface connected to the Layer 2 switch.  
  
!  
interface FastEthernet0/0.1  
  description Guest VLAN  
  encapsulation dot1Q 10  
  ip address 10.0.0.50 255.0.0.0  
  
!--- Creates a sub-interface under FastEthernet0/0 for the guest VLAN.  
  
!  
interface FastEthernet0/0.2  
  description Internal VLAN  
  encapsulation dot1Q 20  
  ip address 20.0.0.50 255.0.0.0  
  
!--- Creates a sub-interface under FastEthernet0/0 for the internal VLAN.  
  
!
```

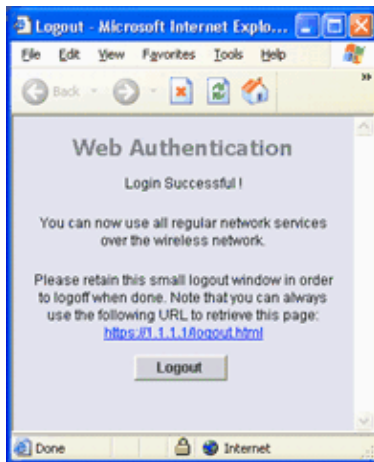
Verify

Use this section to confirm that your configuration works properly.

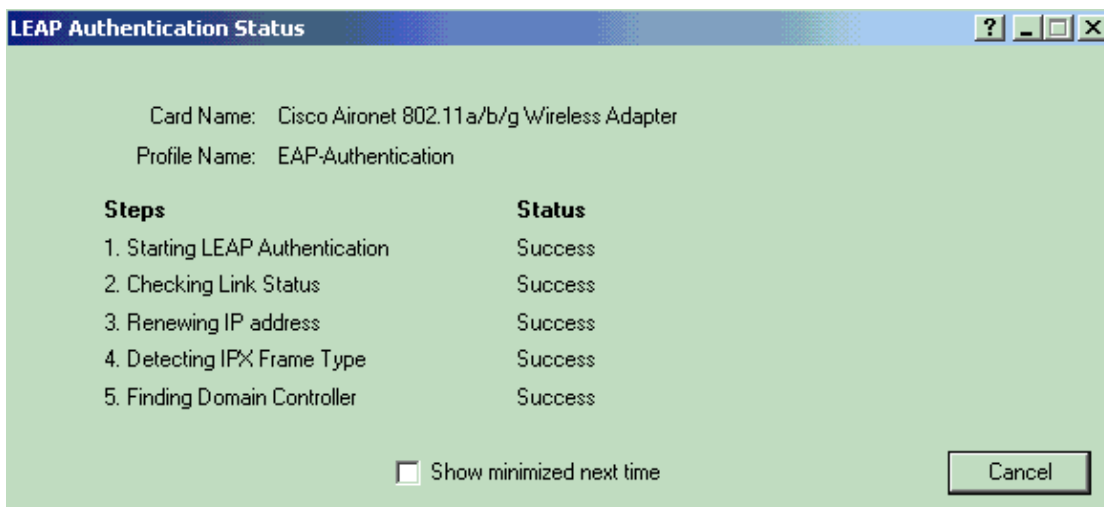
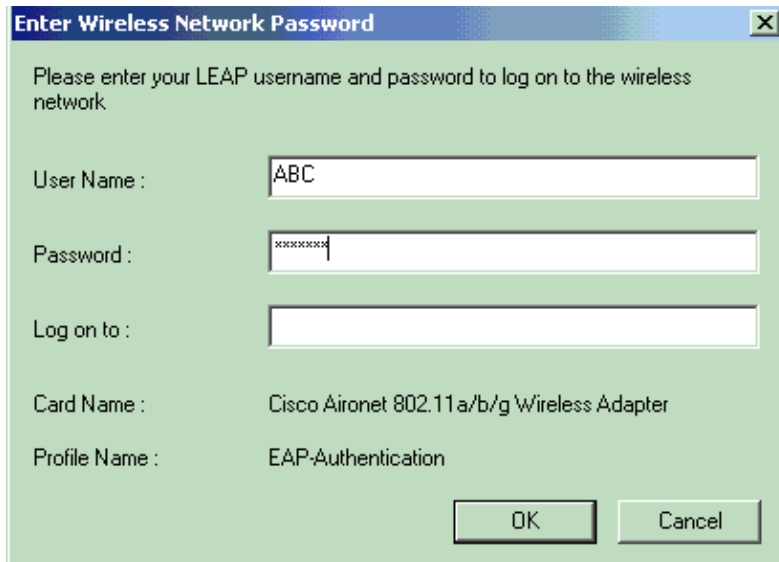
Connect two wireless clients, one guest user (with service set identifier [SSID] **Guest**) and one internal user (with SSID **Internal**), in order to verify the configuration works as expected.

Remember that the guest WLAN was configured for Web Authentication. When the guest wireless client comes up, enter any URL on the web browser. The default web authentication page pops up and prompts you to enter the username and password. Once the guest user enters a valid username/password, the WLC authenticates the guest user and allows access to the network (possibly the Internet). This example shows the web authentication window that the user receives and the output on a successful authentication:





The internal WLAN in this example is configured for 802.1x authentication. When the internal WLAN client comes up, the client uses EAP authentication. For more information on how to configure the client for EAP authentication, refer to the Using EAP Authentication section of Cisco Aironet 802.11a/b/g Wireless LAN Client Adapters (CB21AG and PI21AG) Installation and Configuration Guide. After successful authentication, the user can access the internal network. This example shows an internal wireless client that uses Lightweight Extensible Authentication Protocol (LEAP) authentication:



Troubleshoot

Troubleshooting Procedure

Use this section to troubleshoot your configuration.

If the configuration does not work as expected, complete these steps:

1. Ensure that all the VLANs configured on the WLC are allowed on the switch port connected to the WLC.
2. Ensure that switch port that connects to the WLC and to the router is configured as a trunk port.
3. Ensure that the VLAN Ids used are the same on the WLC and the router.
4. Check if the clients receive DHCP addresses from the DHCP server. If not, check if the DHCP server is configured correctly. For more information on troubleshooting client issues, refer to Troubleshooting Client Issues in the Cisco Unified Wireless Network.

One of the frequent issues that occurs with web authentication is when the redirect to the web authentication page does not work. The user does not see the web authentication window when the browser is opened. Instead, the user must manually enter **https://1.1.1.1/login.html** in order to get to the web authentication window. This has to do with the DNS lookup, which needs to work before the redirect to the web authentication page occurs. If the browser homepage on the wireless client points to a domain name, you need to perform nslookup successfully once the client associates in order for the redirect to work.

Also, for a WLC that runs a version earlier than 3.2.150.10, the way that web authentication works is when a user in that SSID attempts to access the Internet, the management interface of the controller does a DNS query to see if the URL is valid. If it is valid, the URL shows the authorization page with the Virtual Interfaces IP address. After the user successfully logs in, the original request is allowed to pass back to the client. This is because of Cisco bug ID CSCsc68105 (registered customers only) . For more information, refer to Troubleshooting Web Authentication Redirection on the WLC .

Troubleshooting Commands

Note: Refer to Important Information on Debug Commands before you use **debug** commands.

You can use these debug commands in order to troubleshoot the configuration:

- **debug mac addr <client-MAC-address xx:xx:xx:xx:xx:xx>** Configures MAC address debugging for the client.
- **debug aaa all enable** Configures debug of all AAA messages.
- **debug pem state enable** Configures debug of policy manager State Machine.
- **debug pem events enable** Configures debug of policy manager events.
- **debug dhcp message enable** Use this command in order to display debugging information about the DHCP client activities and to monitor the status of DHCP packets.
- **debug dhcp packet enable** Use this command in order to display DHCP packet level information.
- **debug pm ssh-appgw enable** Configures debug of application gateways.
- **debug pm ssh-tcp enable** Configures debug of policy manager tcp handling.

Here are sample outputs from some of these **debug** commands:

Note: Some lines of output have been wrapped to a second line due to spatial reasons.

```
(Cisco Controller) >debug dhcp message enable
Fri Mar  2 16:01:43 2007: 00:40:96:ac:e6:57 dhcp option len,
including the magic cookie = 64
```

```

Fri Mar 2 16:01:43 2007: 00:40:96:ac:e6:57 dhcp option: received DHCP REQUEST msg
Fri Mar 2 16:01:43 2007: 00:40:96:ac:e6:57 dhcp option: skipping option 61, len 7
Fri Mar 2 16:01:43 2007: 00:40:96:ac:e6:57 dhcp option: requested ip = 10.0.0.1
Fri Mar 2 16:01:43 2007: 00:40:96:ac:e6:57 dhcp option: skipping option 12, len 3
Fri Mar 2 16:01:43 2007: 00:40:96:ac:e6:57 dhcp option: skipping option 81, len 7
Fri Mar 2 16:01:43 2007: 00:40:96:ac:e6:57 dhcp option:
vendor class id = MSFT5.0 (len 8)
Fri Mar 2 16:01:43 2007: 00:40:96:ac:e6:57 dhcp option: skipping option 55, len 11
Fri Mar 2 16:01:43 2007: 00:40:96:ac:e6:57 dhcpParseOptions:
options end, len 64, actual 64
Fri Mar 2 16:01:43 2007: 00:40:96:ac:e6:57 Forwarding DHCP packet
(332 octets)from 00:40:96:ac:e6:57
-- packet received on direct-connect port requires forwarding to external DHCP server.
Next-hop is 10.0.0.50
Fri Mar 2 16:01:43 2007: 00:40:96:ac:e6:57 dhcp option len,
including the magic cookie = 64
Fri Mar 2 16:01:43 2007: 00:40:96:ac:e6:57 dhcp option: received DHCP ACK msg
Fri Mar 2 16:01:43 2007: 00:40:96:ac:e6:57 dhcp option: server id = 10.0.0.50
Fri Mar 2 16:01:43 2007: 00:40:96:ac:e6:57 dhcp option: lease time (seconds) =86400
Fri Mar 2 16:01:43 2007: 00:40:96:ac:e6:57 dhcp option: skipping option 58, len 4
Fri Mar 2 16:01:43 2007: 00:40:96:ac:e6:57 dhcp option: skipping option 59, len 4
Fri Mar 2 16:01:43 2007: 00:40:96:ac:e6:57 dhcp option: skipping option 81, len 6
Fri Mar 2 16:01:43 2007: 00:40:96:ac:e6:57 dhcp option: netmask = 255.0.0.0
Fri Mar 2 16:01:43 2007: 00:40:96:ac:e6:57 dhcp option: gateway = 10.0.0.50
Fri Mar 2 16:01:43 2007: 00:40:96:ac:e6:57 dhcpParseOptions:
options end, len 64, actual 64

```

(Cisco Controller) >debug dhcp packet enable

```

Fri Mar 2 16:06:35 2007: 00:40:96:ac:e6:57 dhcpProxy: Received packet:
Client 00:40:96:ac:e6:57 DHCP Op: BOOTREQUEST(1), IP len: 300, switchport: 1,
encap: 0xec03
Fri Mar 2 16:06:35 2007: 00:40:96:ac:e6:57 dhcpProxy: dhcp request,
client: 00:40:96:ac:e6:57: dhcp op: 1, port: 2, encap 0xec03, old mscb
port number: 2
Fri Mar 2 16:06:35 2007: 00:40:96:ac:e6:57 Determing relay for 00:40:96:ac:e6:57
dhcpServer: 10.0.0.50, dhcpNetmask: 255.0.0.0, dhcpGateway: 10.0.0.50,
dhcpRelay: 10.0.0.10 VLAN: 30
Fri Mar 2 16:06:35 2007: 00:40:96:ac:e6:57 Relay settings for 00:40:96:ac:e6:57
Local Address: 10.0.0.10, DHCP Server: 10.0.0.50, Gateway Addr: 10.0.0.50,
VLAN: 30, port: 2
Fri Mar 2 16:06:35 2007: 00:40:96:ac:e6:57 DHCP Message Type received:
DHCP REQUEST msg
Fri Mar 2 16:06:35 2007: 00:40:96:ac:e6:57 op: BOOTREQUEST, htype:
Ethernet,hlen: 6, hops: 1
Fri Mar 2 16:06:35 2007: 00:40:96:ac:e6:57 xid: 1674228912, secs: 0, flags: 0
Fri Mar 2 16:06:35 2007: 00:40:96:ac:e6:57 chaddr: 00:40:96:ac:e6:57
Fri Mar 2 16:06:35 2007: 00:40:96:ac:e6:57 ciaddr: 10.0.0.1, yiaddr: 0.0.0.0
Fri Mar 2 16:06:35 2007: 00:40:96:ac:e6:57 siaddr: 0.0.0.0, giaddr: 10.0.0.10
Fri Mar 2 16:06:35 2007: 00:40:96:ac:e6:57 DHCP request to 10.0.0.50,
len 350,switchport 2, vlan 30
Fri Mar 2 16:06:35 2007: 00:40:96:ac:e6:57 dhcpProxy: Received packet:
Client 00:40:96:ac:e6:57 DHCP Op: BOOTREPLY(2), IP len: 300, switchport: 2,
encap: 0xec00
Fri Mar 2 16:06:35 2007: DHCP Reply to AP client: 00:40:96:ac:e6:57, frame len412,
switchport 2
Fri Mar 2 16:06:35 2007: 00:40:96:ac:e6:57 DHCP Message Type received: DHCP ACK msg
Fri Mar 2 16:06:35 2007: 00:40:96:ac:e6:57 op: BOOTREPLY, htype:
Ethernet, hlen: 6, hops: 0
Fri Mar 2 16:06:35 2007: 00:40:96:ac:e6:57 xid: 1674228912, secs: 0, flags: 0
Fri Mar 2 16:06:35 2007: 00:40:96:ac:e6:57 chaddr: 00:40:96:ac:e6:57
Fri Mar 2 16:06:35 2007: 00:40:96:ac:e6:57 ciaddr: 10.0.0.1, yiaddr: 10.0.0.1
Fri Mar 2 16:06:35 2007: 00:40:96:ac:e6:57 siaddr: 0.0.0.0, giaddr: 0.0.0.0
Fri Mar 2 16:06:35 2007: 00:40:96:ac:e6:57 server id: 1.1.1.1
rcvd server id: 10.0.0.50

```

(Cisco Controller) >debug aaa all enable

```
Fri Mar 2 16:22:40 2007: User user1 authenticated
Fri Mar 2 16:22:40 2007: 00:40:96:ac:e6:57
Returning AAA Error 'Success' (0) for mobile 00:40:96:ac:e6:57
Fri Mar 2 16:22:40 2007: AuthorizationResponse: 0xbadff97c
Fri Mar 2 16:22:40 2007: structureSize.....70
Fri Mar 2 16:22:40 2007: resultCode.....0
Fri Mar 2 16:22:40 2007: protocolUsed.....0x00000008
Fri Mar 2 16:22:40 2007: proxyState.....00:40:96:AC:E6:57-00:00
Fri Mar 2 16:22:40 2007: Packet contains 2 AVPs:
Fri Mar 2 16:22:40 2007: AVP[01] Service-Type.....0x00000001 (1) (4 bytes)
Fri Mar 2 16:22:40 2007: AVP[02] Airespace /
WLAN-Identifier.....0x00000001 (1) (4 bytes)
Fri Mar 2 16:22:40 2007: 00:40:96:ac:e6:57 Applying new AAA override
for station 00:40:96:ac:e6:57
Fri Mar 2 16:22:40 2007: 00:40:96:ac:e6:57 Override values for station
00:40:96:ac:e6:57
        source: 48, valid bits: 0x1
        qosLevel: -1, dscp: 0xffffffff, dot1pTag: 0xffffffff, sessionTimeout: -1
        dataAvgC: -1, rTavgC: -1, dataBurstC: -1, rTimeBurstC: -1
        vlanIfName: '', aclName:
Fri Mar 2 16:22:40 2007: 00:40:96:ac:e6:57 Unable to apply override
policy for station 00:40:96:ac:e6:57
- VapAllowRadiusOverride is FALSE
Fri Mar 2 16:22:40 2007: AccountingMessage Accounting Start: 0xa62700c
Fri Mar 2 16:22:40 2007: Packet contains 13 AVPs:
Fri Mar 2 16:22:40 2007: AVP[01] User-Name.....user1 (5 bytes)
Fri Mar 2 16:22:40 2007: AVP[02] Nas-Port.....0x00000001 (1) (4 bytes)
Fri Mar 2 16:22:40 2007: AVP[03]
Nas-Ip-Address.....0x0a4df4d2 (172881106) (4 bytes)
Fri Mar 2 16:22:40 2007: AVP[04]
NAS-Identifier.....0x574c4331 (1464615729) (4 bytes)
Fri Mar 2 16:22:40 2007: AVP[05]
Airespace / WLAN-Identifier.....0x00000001 (1) (4 bytes)
Fri Mar 2 16:22:40 2007: AVP[06]
Acct-Session-Id.....45e84f50/00:40:96:ac:e6:57/9 (28 bytes)
Fri Mar 2 16:22:40 2007: AVP[07]
Acct-Authentic.....0x00000002 (2) (4 bytes)
Fri Mar 2 16:22:40 2007: AVP[08]
Tunnel-Type.....0x0000000d (13) (4 bytes)
Fri Mar 2 16:22:40 2007: AVP[09]
Tunnel-Medium-Type.....0x00000006 (6) (4 bytes)
Fri Mar 2 16:22:40 2007: AVP[10]
Tunnel-Group-Id.....0x3330 (13104) (2 bytes)
Fri Mar 2 16:22:40 2007: AVP[11]
Acct-Status-Type.....0x00000001 (1) (4 bytes)
Fri Mar 2 16:22:40 2007: AVP[12]
Calling-Station-Id.....10.0.0.1 (8 bytes)
Fri Mar 2 16:22:40 2007: AVP[13]
Called-Station-Id.....10.77.244.210 (13 bytes)
```

when web authentication is closed by user:

```
(Cisco Controller) >Fri Mar 2 16:25:47 2007: AccountingMessage
Accounting Stop: 0xa627c78
Fri Mar 2 16:25:47 2007: Packet contains 20 AVPs:
Fri Mar 2 16:25:47 2007:
AVP[01] User-Name.....user1 (5 bytes)
Fri Mar 2 16:25:47 2007:
AVP[02] Nas-Port.....0x00000001 (1) (4 bytes)
Fri Mar 2 16:25:47 2007:
AVP[03] Nas-Ip-Address.....0x0a4df4d2 (172881106) (4 bytes)
Fri Mar 2 16:25:47 2007:
AVP[04] NAS-Identifier.....0x574c4331 (1464615729) (4 bytes)
```

```

Fri Mar  2 16:25:47 2007:
AVP[05] Airespace / WLAN-Identifier.....0x00000001 (1) (4 bytes)
Fri Mar  2 16:25:47 2007:
AVP[06] Acct-Session-Id.....45e84f50/00:40:96:ac:e6:57/9 (28 bytes)
Fri Mar  2 16:25:47 2007:
AVP[07] Acct-Authentic.....0x00000002 (2) (4 bytes)
Fri Mar  2 16:25:47 2007:
AVP[08] Tunnel-Type.....0x0000000d (13) (4 bytes)
Fri Mar  2 16:25:47 2007:
AVP[09] Tunnel-Medium-Type.....0x00000006 (6) (4 bytes)
Fri Mar  2 16:25:47 2007:
AVP[10] Tunnel-Group-Id.....0x3330 (13104) (2 bytes)
Fri Mar  2 16:25:47 2007:
AVP[11] Acct-Status-Type.....0x00000002 (2) (4 bytes)
Fri Mar  2 16:25:47 2007:
AVP[12] Acct-Input-Octets.....0x0001820e (98830) (4 bytes)
Fri Mar  2 16:25:47 2007:
AVP[13] Acct-Output-Octets.....0x00005206 (20998) (4 bytes)
Fri Mar  2 16:25:47 2007:
AVP[14] Acct-Input-Packets.....0x000006ee (1774) (4 bytes)
Fri Mar  2 16:25:47 2007:
AVP[15] Acct-Output-Packets.....0x00000041 (65) (4 bytes)
Fri Mar  2 16:25:47 2007:
AVP[16] Acct-Terminate-Cause.....0x00000001 (1) (4 bytes)
Fri Mar  2 16:25:47 2007:
AVP[17] Acct-Session-Time.....0x000000bb (187) (4 bytes)
Fri Mar  2 16:25:47 2007:
AVP[18] Acct-Delay-Time.....0x00000000 (0) (4 bytes)
Fri Mar  2 16:25:47 2007:
AVP[19] Calling-Station-Id.....10.0.0.1 (8 bytes)
Fri Mar  2 16:25:47 2007:
AVP[20] Called-Station-Id.....10.77.244.210 (13 bytes)

```

(Cisco Controller) >debug pem state enable

```

Fri Mar  2 16:27:39 2007: 00:40:96:ac:e6:57 10.0.0.1
WEBAUTH_REQD (8) Change state to START (0)
Fri Mar  2 16:27:39 2007: 00:40:96:ac:e6:57 10.0.0.1
START (0) Change state to AUTHCHECK (2)
Fri Mar  2 16:27:39 2007: 00:40:96:ac:e6:57 10.0.0.1
AUTHCHECK (2) Change state to L2AUTHCOMPLETE (4)
Fri Mar  2 16:27:39 2007: 00:40:96:ac:e6:57 10.0.0.1
L2AUTHCOMPLETE (4) Change state to WEBAUTH_REQD (8)
Fri Mar  2 16:28:16 2007: 00:16:6f:6e:36:2b 0.0.0.0
START (0) Change state to AUTHCHECK (2)
Fri Mar  2 16:28:16 2007: 00:16:6f:6e:36:2b 0.0.0.0
AUTHCHECK (2) Change state to L2AUTHCOMPLETE (4)
Fri Mar  2 16:28:16 2007: 00:16:6f:6e:36:2b 0.0.0.0
L2AUTHCOMPLETE (4) Change state to DHCP_REQD (7)
Fri Mar  2 16:28:19 2007: 00:40:96:ac:e6:57 10.0.0.1
WEBAUTH_REQD (8) Change state to WEBAUTH_NOL3SEC (14)
Fri Mar  2 16:28:19 2007: 00:40:96:ac:e6:57 10.0.0.1
WEBAUTH_NOL3SEC (14) Change state to RUN (20)
Fri Mar  2 16:28:20 2007: 00:16:6f:6e:36:2b 0.0.0.0
START (0) Change state to AUTHCHECK (2)
Fri Mar  2 16:28:20 2007: 00:16:6f:6e:36:2b 0.0.0.0
AUTHCHECK (2) Change state to L2AUTHCOMPLETE (4)
Fri Mar  2 16:28:20 2007: 00:16:6f:6e:36:2b 0.0.0.0
L2AUTHCOMPLETE (4) Change state to DHCP_REQD (7)
Fri Mar  2 16:28:24 2007: 00:40:96:af:a3:40 0.0.0.0
START (0) Change state to AUTHCHECK (2)
Fri Mar  2 16:28:24 2007: 00:40:96:af:a3:40 0.0.0.0
AUTHCHECK (2) Change state to L2AUTHCOMPLETE (4)
Fri Mar  2 16:28:24 2007: 00:40:96:af:a3:40 0.0.0.0
L2AUTHCOMPLETE (4) Change state to DHCP_REQD (7)
Fri Mar  2 16:28:25 2007: 00:40:96:af:a3:40 40.0.0.1

```

```

DHCP_REQD (7) Change stateto RUN (20)
Fri Mar  2 16:28:30 2007: 00:16:6f:6e:36:2b 0.0.0.0
START (0) Change state to AUTHCHECK (2)
Fri Mar  2 16:28:30 2007: 00:16:6f:6e:36:2b 0.0.0.0
AUTHCHECK (2) Change state to L2AUTHCOMPLETE (4)
Fri Mar  2 16:28:30 2007: 00:16:6f:6e:36:2b 0.0.0.0
L2AUTHCOMPLETE (4) Change state to DHCP_REQD (7)
Fri Mar  2 16:28:34 2007: 00:16:6f:6e:36:2b 30.0.0.2
DHCP_REQD (7) Change stateto WEBAUTH_REQD (8)

```

(Cisco Controller) >debug pem events enable

```

Fri Mar  2 16:31:06 2007: 00:40:96:ac:e6:57 10.0.0.1 START (0) Initializing policy
Fri Mar  2 16:31:06 2007: 00:40:96:ac:e6:57 10.0.0.1 L2AUTHCOMPLETE (4)
Plumbed mobile LWAPP rule on AP 00:0b:85:5b:fb:d0
Fri Mar  2 16:31:06 2007: 00:40:96:ac:e6:57 10.0.0.1 WEBAUTH_REQD (8)
Adding TMP rule
Fri Mar  2 16:31:06 2007: 00:40:96:ac:e6:57 10.0.0.1 WEBAUTH_REQD (8)
Replacing Fast Path rule
  type = Temporary Entry
  on AP 00:0b:85:5b:fb:d0, slot 0, interface = 1
  ACL Id = 255, Jumbo Frames = NO, 802.1P = 0, DSCP = 0, TokenID = 1506
Fri Mar  2 16:31:06 2007: 00:40:96:ac:e6:57 10.0.0.1 WEBAUTH_REQD (8)
Successfully plumbed mobile rule (ACL ID 255)
Fri Mar  2 16:31:06 2007: 00:40:96:ac:e6:57 10.0.0.1 WEBAUTH_REQD (8)
Deleting mobile policy rule 27
Fri Mar  2 16:31:06 2007: 00:40:96:ac:e6:57 Adding Web RuleID 28 for
mobile 00:40:96:ac:e6:57
Fri Mar  2 16:31:06 2007: 00:40:96:ac:e6:57 10.0.0.1 WEBAUTH_REQD (8)
Adding TMP rule
Fri Mar  2 16:31:06 2007: 00:40:96:ac:e6:57 10.0.0.1 WEBAUTH_REQD (8)
ReplacingFast Path rule
  type = Temporary Entry
  on AP 00:0b:85:5b:fb:d0, slot 0, interface = 1
  ACL Id = 255, Jumbo Frames = NO, 802.1P = 0, DSCP = 0, TokenID = 1506
Fri Mar  2 16:31:06 2007: 00:40:96:ac:e6:57 10.0.0.1 WEBAUTH_REQD (8)
Successfully plumbed mobile rule (ACL ID 255)
Fri Mar  2 16:31:06 2007: 00:40:96:ac:e6:57 10.0.0.1 Removed NPU entry.
Fri Mar  2 16:31:06 2007: 00:40:96:ac:e6:57 10.0.0.1 Added NPU entry of type 8
Fri Mar  2 16:31:06 2007: 00:40:96:ac:e6:57 10.0.0.1 Added NPU entry of type 8

```

NetPro Discussion Forums – Featured Conversations

Networking Professionals Connection is a forum for networking professionals to share questions, suggestions, and information about networking solutions, products, and technologies. The featured links are some of the most recent conversations available in this technology.

NetPro Discussion Forums – Featured Conversations for Wireless
Wireless – Mobility: WLAN Radio Standards
Wireless – Mobility: Security and Network Management
Wireless – Mobility: Getting Started with Wireless
Wireless – Mobility: General

Related Information

- [Authentication on Wireless LAN Controllers Configuration Example](#)
- [External Web Authentication with Wireless LAN Controllers Configuration Example](#)
- [Cisco Wireless LAN Controller Configuration Guide, Release 4.0](#)

- **Wireless Product Support**
 - **Technical Support & Documentation – Cisco Systems**
-

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2008 – 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: May 04, 2009

Document ID: 70937
