使用 WLC 的访客 WLAN 和内部 WLAN 的配置示例

Contents

Introduction

本文档为使用 WLAN 控制器 (WLC) 和轻量接入点 (LAP) 的访客无线 LAN (WLAN) 和安全内部 WLAN 提供了一个配置示例。在本文档的配置中，访客 WLAN 使用 Web 身份验证来验证用户，安全内部 WLAN 使用可扩展身份验证协议 (EAP) 进行身份验证。

Prerequisites

Requirements

尝试进行此配置之前，请确保满足以下要求：

- 了解如何配置 WLC 上的基本参数
- 了解如何配置 DHCP 和域名系统 (DNS) 服务器

Components Used

本文档中的信息基于以下软件和硬件版本：

- 运行固件 4.0 版本的 Cisco 2006 WLC
- Cisco 1000系列LAP
- 运行固件版本 2.6 的 Cisco 802.11a/b/g 无线客户端适配器
- 运行 Cisco IOS® 版本 12.4(2)XA 的 Cisco 2811 路由器
- 运行 Cisco IOS 版本 12.0(5)WC3b 的 Cisco 3500 XL 系列交换机
- 在 Microsoft Windows 2000 服务器上运行的 DNS 服务器

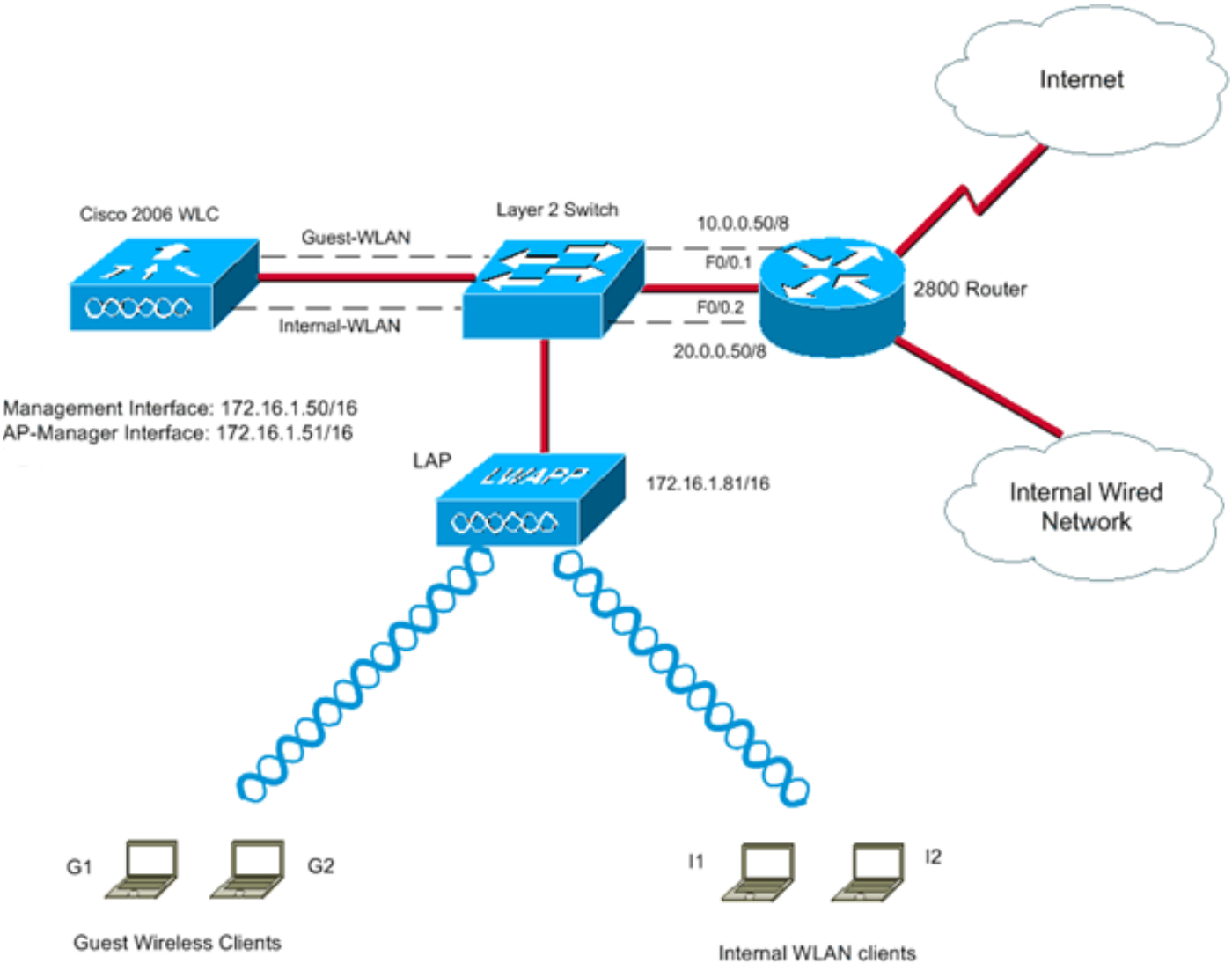
The information in this document was created from the devices in a specific lab environment.All of the devices used in this document started with a cleared (default) configuration.If your network is live, make sure that you understand the potential impact of any command.

Conventions

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

网络设置

本文档中的配置示例使用下图所示的设置。LAP 注册到 WLC。WLC 连接到第 2 层交换机。将用户连接到 WAN 的路由器还连接到第 2 层交换机。您需要创建两个 WLAN，一个用于访客用户，另一个用于内部 LAN 用户。您还需要一个 DHCP 服务器，为访客和内部无线客户端提供 IP 地址。访客用户使用 Web 身份验证接入网络。内部用户使用 EAP 身份验证。2811 路由器还充当无线客户端的 DHCP 服务器。



Note: 本文档假设配置了 WLC 的基本参数并且已在 WLC 中注册 LAP。有关如何在 WLC 上配置基本参数以及如何在 WLC 中注册 LAP 的信息，请参阅向无线 LAN 控制器 (WLC) 注册轻量接入点 (LAP)。

配置为 DHCP 服务器时，某些防火墙不支持来自中继代理的 DHCP 请求。WLC 是客户端的中继代理。配置为 DHCP 服务器的防火墙会忽略这些请求。客户端必须直接连接到防火墙，不能通过另一个中继代理或路由器发送请求。防火墙可以作为与之直接相连的内部主机的简单 DHCP 服务器。这允许防火墙基于直接连接并可查看的 MAC 地址对其表进行维护。正是由于这一原因，使得尝试从 DHCP 中继进行地址分配不可行并会丢弃数据包。PIX 防火墙具有此限制。

Configure

要为此网络设置配置设备，请完成以下步骤：

1. 为访客和内部用户在 WLC 上配置动态接口
2. 为访客和内部用户创建 WLAN
3. 配置作为中继端口连接 WLC 的第 2 层交换机端口
4. 为两个 WLAN 配置路由器

为访客和内部用户在 WLC 上配置动态接口

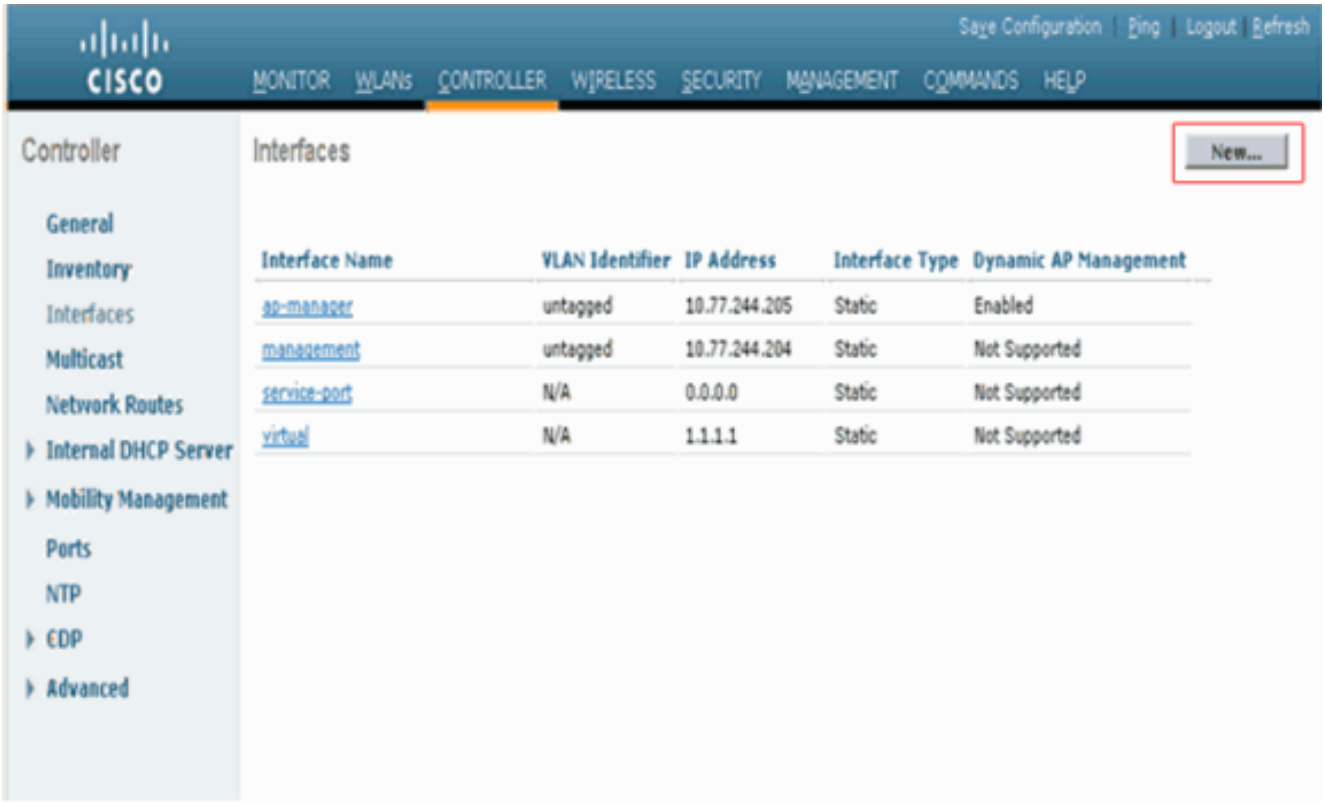
第一步是在 WLC 上创建两个动态接口，一个用于访客用户，另一个用于内部用户。

本文档中的示例为动态接口使用了以下参数和值：

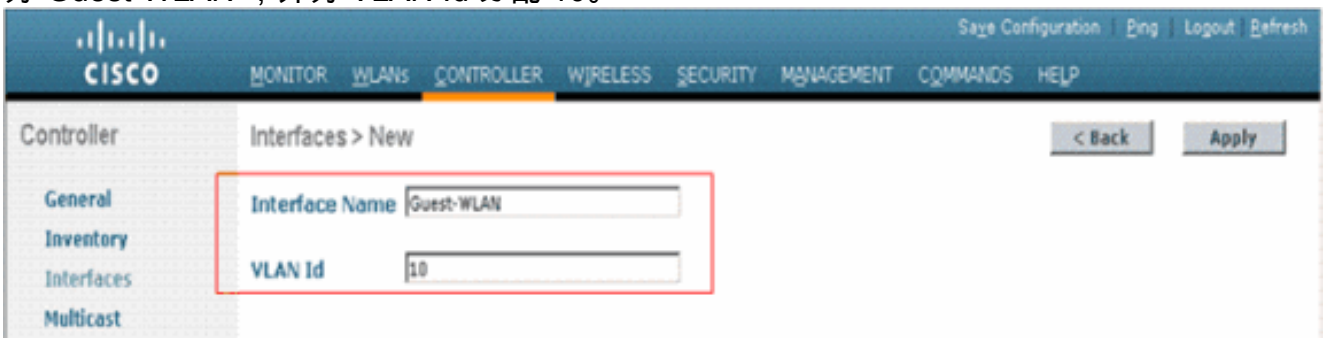
```
Guest-WLAN                                                    Internal-WLAN
VLAN Id : 10                              VLAN Id : 20
IP address: 10.0.0.10                            IP address: 20.0.0.10
Netmask: 255.0.0.0 Netmask: 255.0.0.0
Gateway: 10.0.0.50                           Gateway: 20.0.0.50
Physical port on WLC: 1                           Physical port on WLC: 1
DHCP server: 172.16.1.60                            DHCP server: 172.16.1.60
```

完成这些步骤：

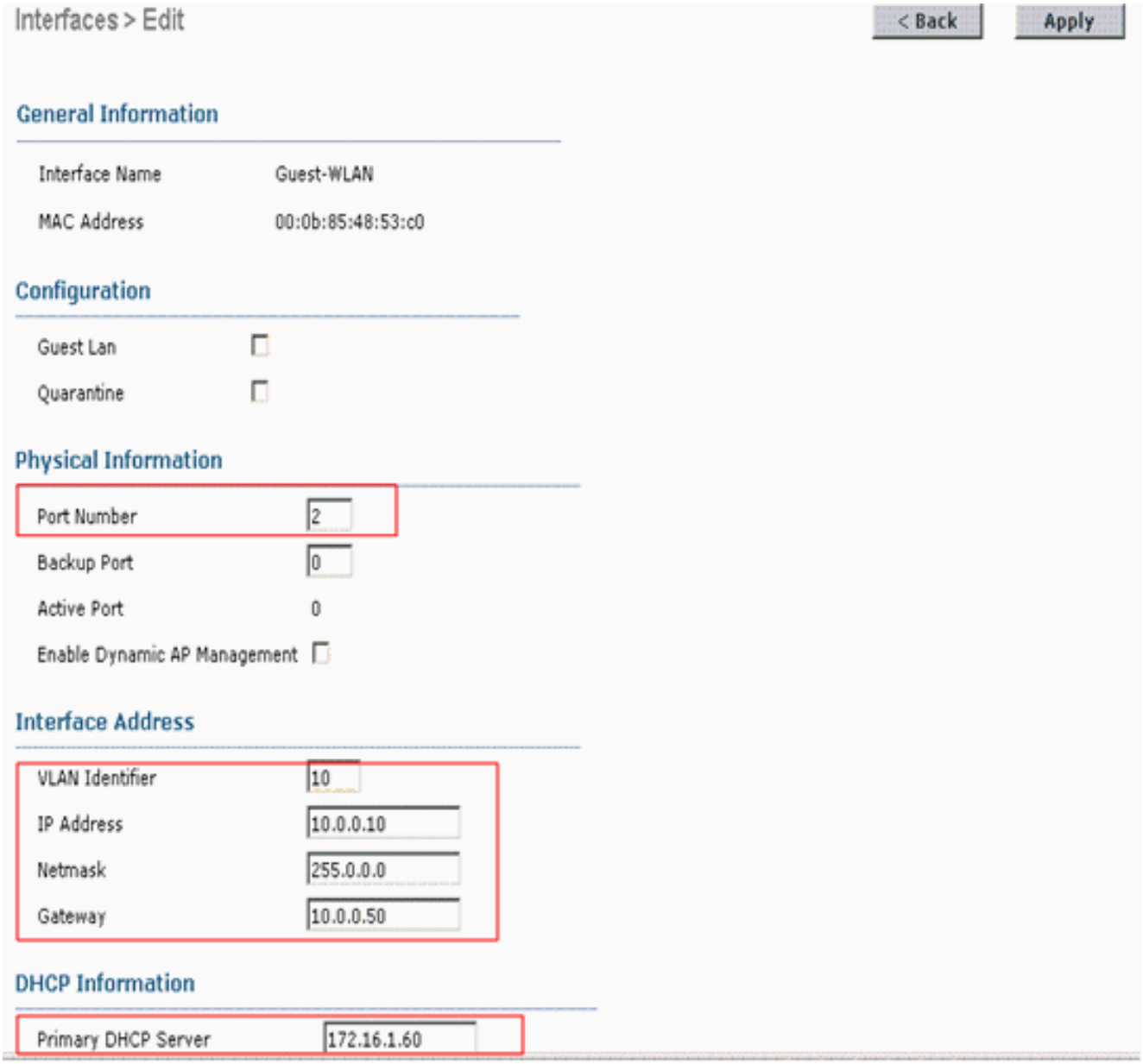
1. 从 WLC GUI 中，选择 **Controllers > Interfaces**。此时会显示“Interfaces”窗口。此窗口中会列出在控制器上配置的接口。这包括默认接口，包括管理接口、ap-manager 接口、虚拟接口和服务端口接口以及用户定义的动态接口。



2. 单击 **New** 创建新的动态接口。
3. 在接口>New窗口，请输入接口名称和VLAN Id。然后，单击 **Apply**。在本例中，动态接口命名为“Guest-WLAN”，并为 VLAN Id 分配 10。

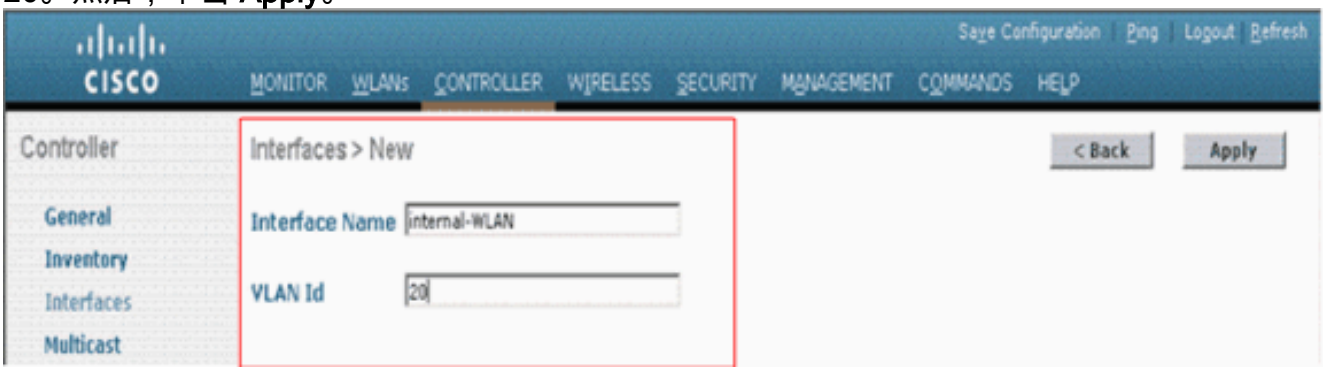


4. 对于动态接口，在 Interfaces > Edit 窗口中输入 IP 地址、子网掩码和默认网关。将它分配到 WLC 上的某个物理端口，再输入 DHCP 服务器的 IP 地址。然后，单击 **Apply**。如下面的示例所示
：

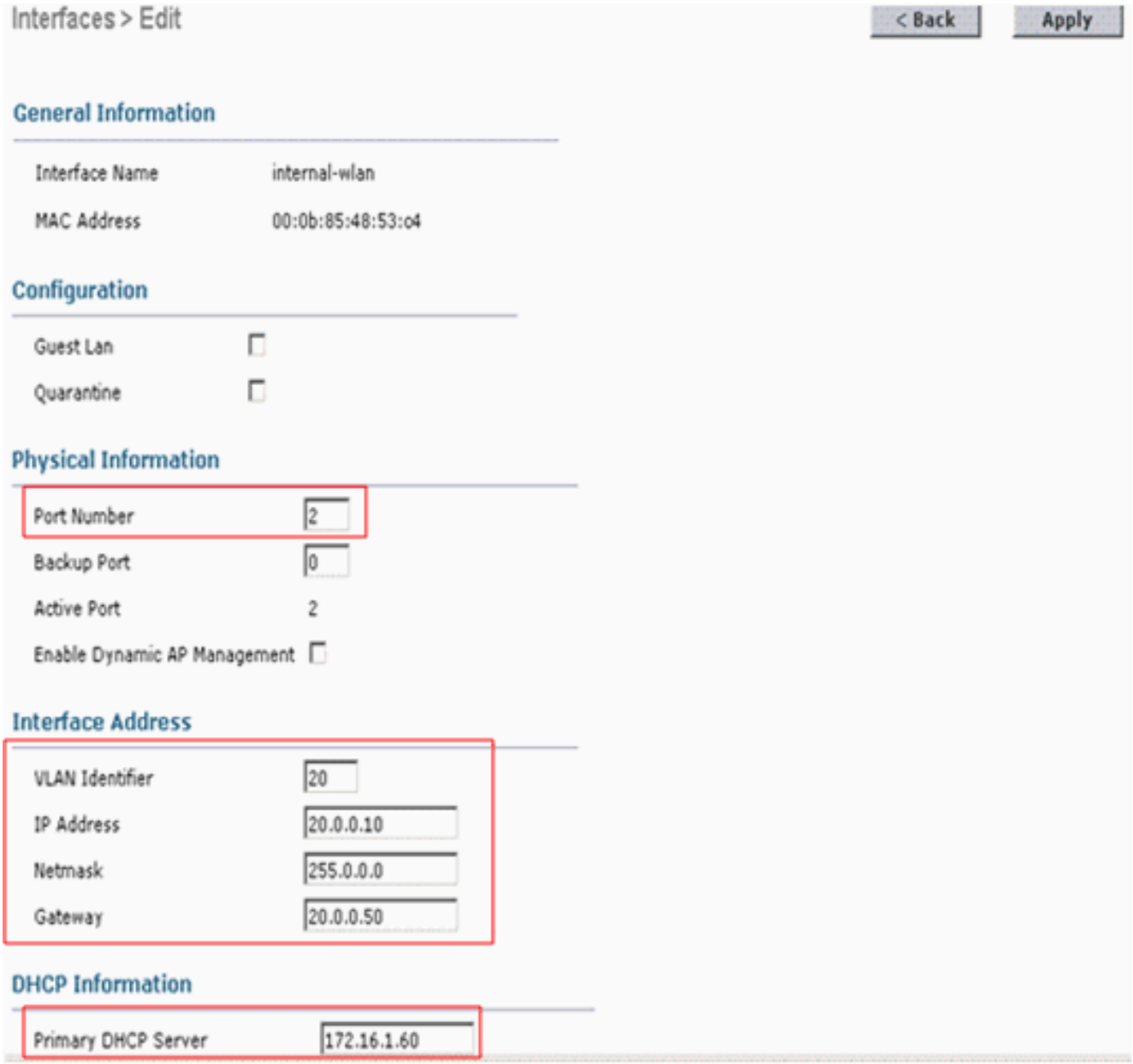


必须完成相同过程以便为内部 WLAN 创建动态接口。

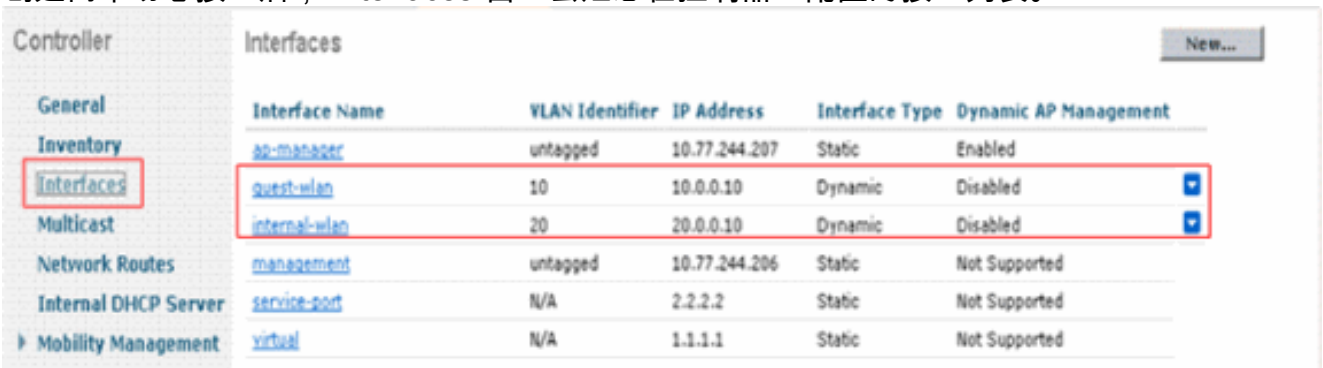
5. 在“Interfaces”>“New”窗口中，为内部用户的动态接口输入 **Internal-WLAN**，为“VLAN Id”输入 20。然后，单击 **Apply**。



6. 对于动态接口，在 Interfaces > Edit 窗口中输入 IP 地址、子网掩码和默认网关。将它分配到 WLC 上的某个物理端口，再输入 DHCP 服务器的 IP 地址。然后，单击 **Apply**。



创建两个动态接口后，“Interfaces”窗口会汇总在控制器上配置的接口列表。

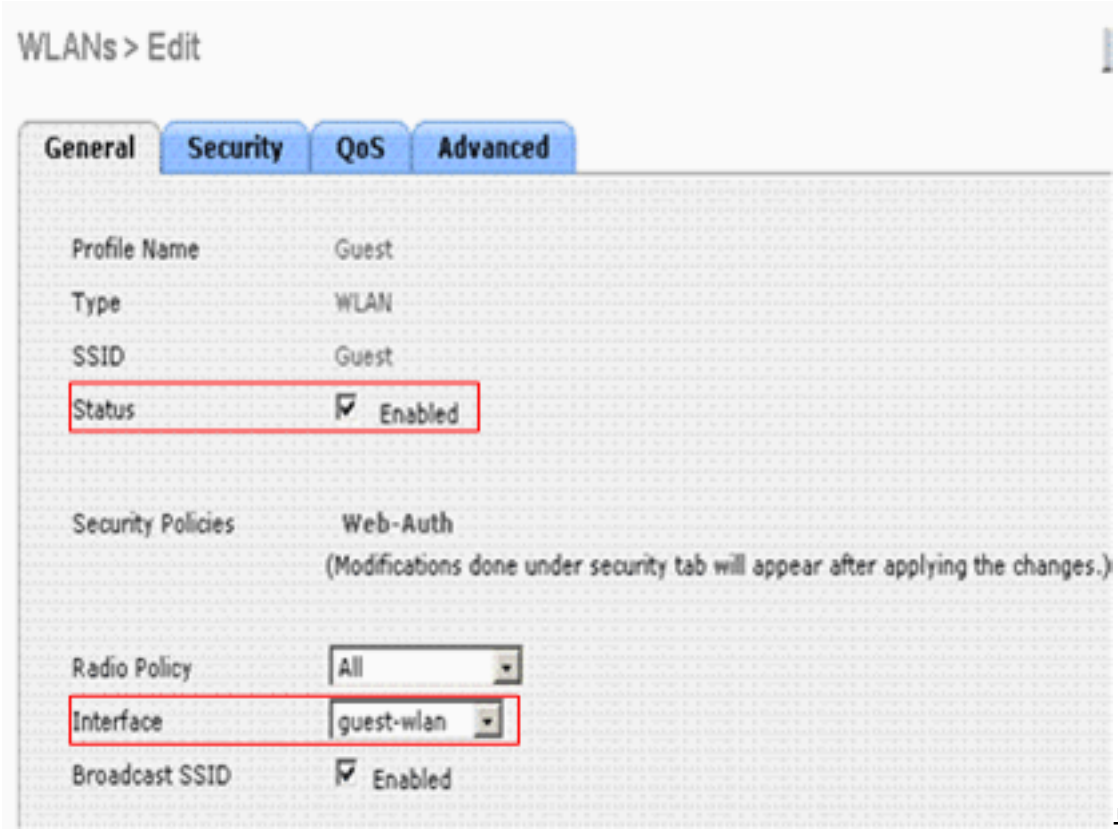


为访客和内部用户创建 WLAN

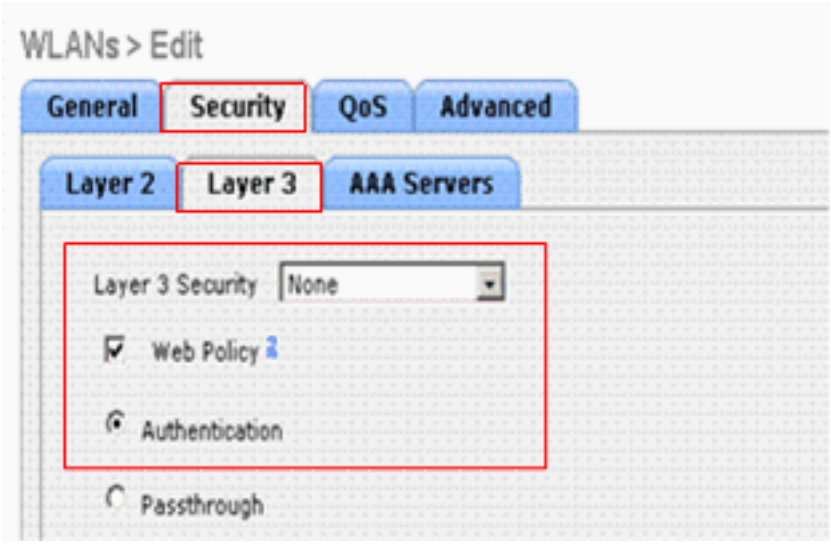
下一步是为访客用户和内部用户创建 WLAN，并将动态接口映射至 WLAN。另外还必须定义用于对来宾用户和无线用户进行身份验证的安全方法。完成这些步骤：

1. 要创建 WLAN，请从控制器 GUI 中单击 **WLANs**。随即显示 WLAN 窗口。该窗口列出了控制器中配置的 WLAN。
2. 要配置新的 WLAN，请单击 **New**。在本例中，WLAN 命名为 *Guest*，WLAN ID 是 2。

3. 单击右上角的 **Apply**。
4. 这时将显示“WLAN”>“Edit”屏幕，其中包含各种选项卡。在访客 WLAN 的 **General** 选项卡下，在“Interface Name”字段中选择“guest-wlan”。这将之前创建的动态接口 **guest-wlan** 映射至 WLAN Guest。确保 WLAN 的“Status”为“Enabled”。

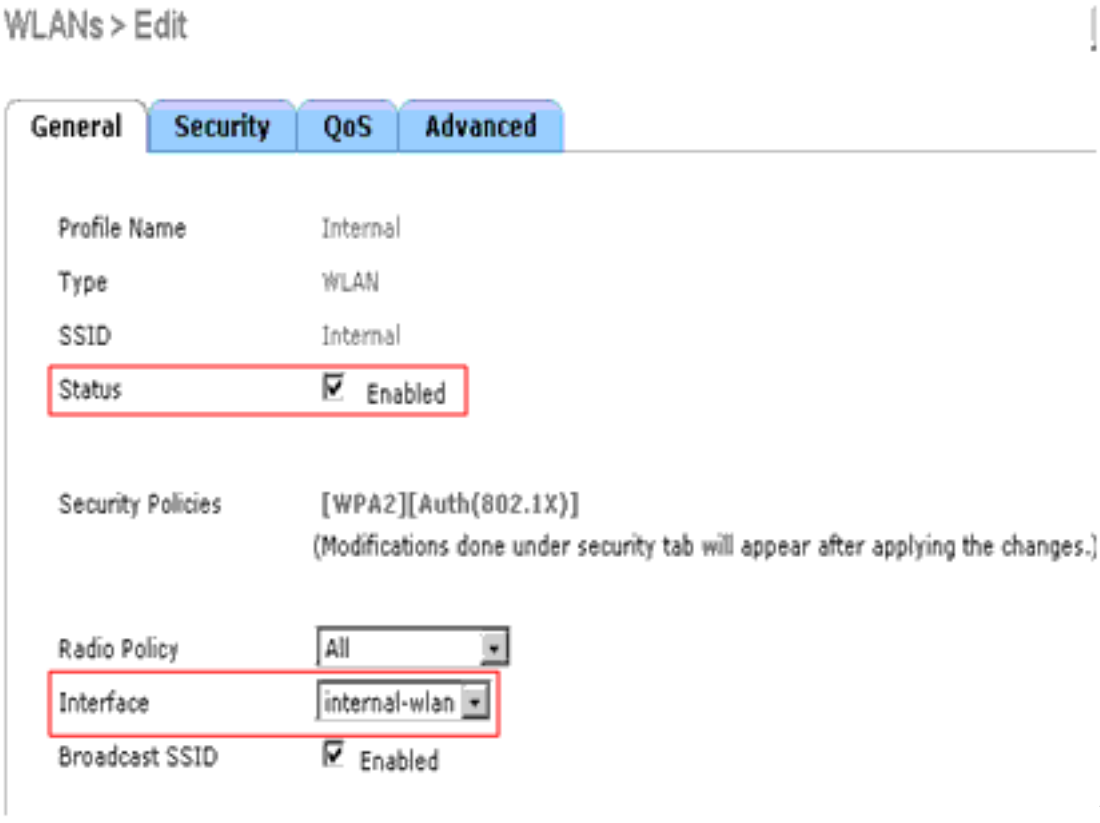


单击 **Security** 选项卡。对于此 WLAN，使用 Web 身份验证第 3 层安全机制对客户端进行身份验证。因此，在 *Layer 2 Security* 字段下选择 **None**。在 *Layer 3 Security* 字段中，选中 **Web Policy** 框并选择“Authentication”选项。

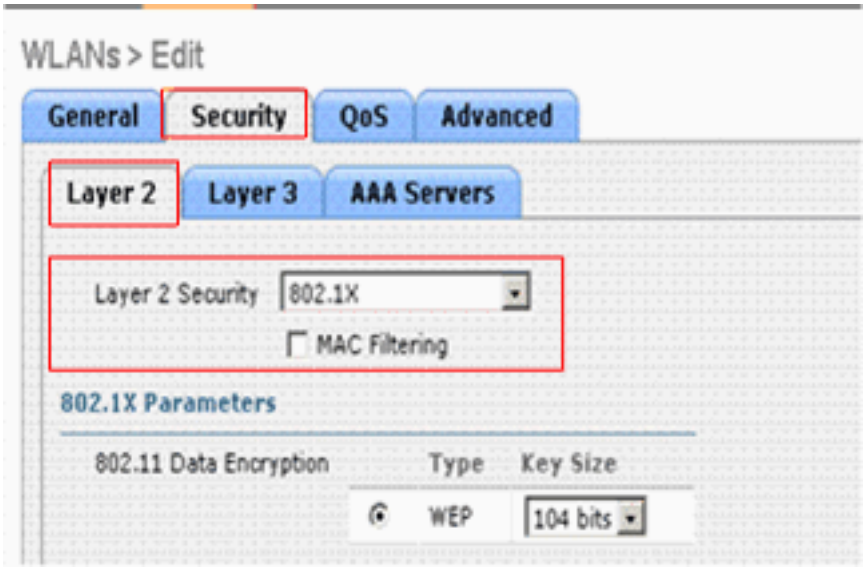


Note: 有关 Web 身份验证的详细信息，请参阅[无线 LAN 控制器 Web 身份验证配置示例](#)。单击 **Apply**。

5. 为内部用户创建 WLAN。在“WLANs”>“New”窗口中，输入 **Internal** 并选择 3 以便为内部用户创建 WLAN。然后，单击 **Apply**。
6. 这时将显示“WLANs”>“Edit”窗口。在 *General* 选项卡下，在“Interface Name”字段中选择 **internal-wlan**。这将之前创建的动态接口 **internal-wlan** 映射至 WLAN Internal。确保启用



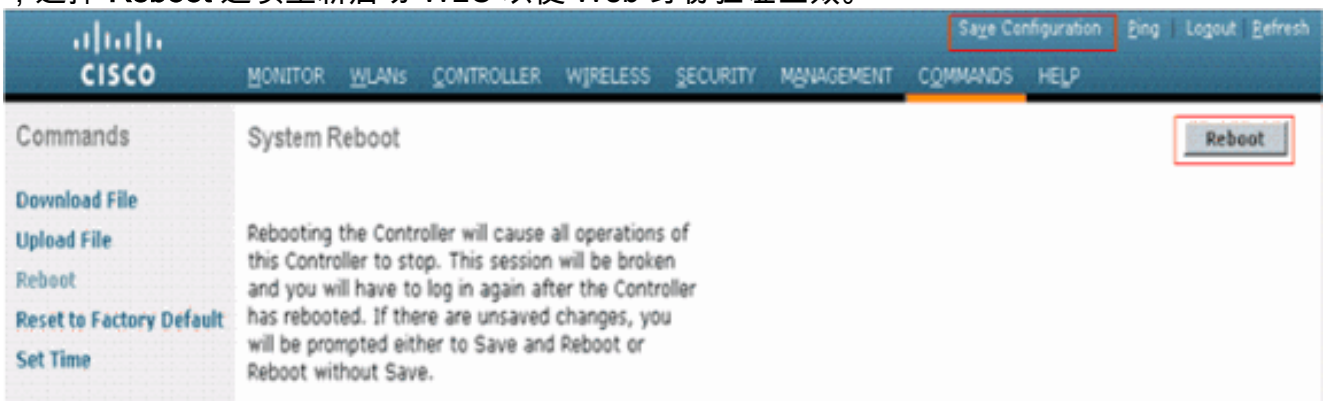
WLAN。保留“Layer 2 Security”选项的默认值 802.1x，因为内部 WLAN 用户使用 EAP 身份验证。



7. 单击 **Apply**。这时将显示 WLAN 窗口，其中显示了所创建的 WLAN 列表。

Note: 有关如何在 WLC 中配置基于 EAP 的 WLAN 的详细信息，请参阅 [WLAN 控制器 (WLC) 中 EAP 身份验证的配置示例](#)。

8. 在 WLC GUI 中，单击 **Save Configuration**，然后单击控制器 GUI 中的“Commands”。接下来，选择 **Reboot** 选项重新启动 WLC 以使 Web 身份验证生效。



Note: 单击 **Save Configuration** 以便在重新启动过程中保存配置。

配置作为中继端口连接 WLC 的第 2 层交换机端口

您需要配置交换机端口以支持在 WLC 上配置的多个 VLAN，因为 WLC 连接到第 2 层交换机。您必须将交换机端口配置为 802.1Q 中继端口。

每个控制器端口连接都是一个 802.1Q 中继，并应在相邻交换机上如此配置。在 Cisco 交换机上，802.1Q 中继的本地 VLAN（例如 **VLAN 1**）未进行标记。因此，如果将控制器的接口配置为使用相邻 Cisco 交换机上的本地 VLAN，请确保在控制器上将该接口配置为未标记。

VLAN identifier（在“Controller > Interfaces”窗口中）的零值表示该接口未标记。在本文档的示例中

，默认的无标记 VLAN 配置了“AP-Manager”和“Management”接口。

当控制器接口设置为非零值时，不应将其标记为交换机的本地 VLAN 并且在交换机上必须允许该 VLAN。在本例中，VLAN 60 配置为连接到控制器的交换机端口上的本地 VLAN。

以下是连接到 WLC 的交换机端口的配置：

```
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
```

以下是连接到路由器作为中继端口的交换机端口的配置：

```
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
```

以下是连接到 LAP 的交换机端口的配置。此端口配置为接入端口：

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

为两个 WLAN 配置路由器

在本文档的示例中，2811 路由器将访客用户连接到 Internet 并将内部有线用户连接到内部无线用户。您还需要配置路由器以提供 DHCP 服务。

在路由器上，为每个 VLAN 在连接到交换机上的中继端口的 FastEthernet 接口下创建子接口。将子接口分配给对应的 VLAN，并配置相应子网的 IP 地址。

Note: 这里只提供了路由器配置的相关部分，并未给出全部配置。

这是在路由器上完成此任务所需的配置。

必须发出以下命令以在路由器上配置 DHCP 服务：

```
!
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. !
```

对于示例设置，必须针对 FastEthernet 接口发出以下命令：

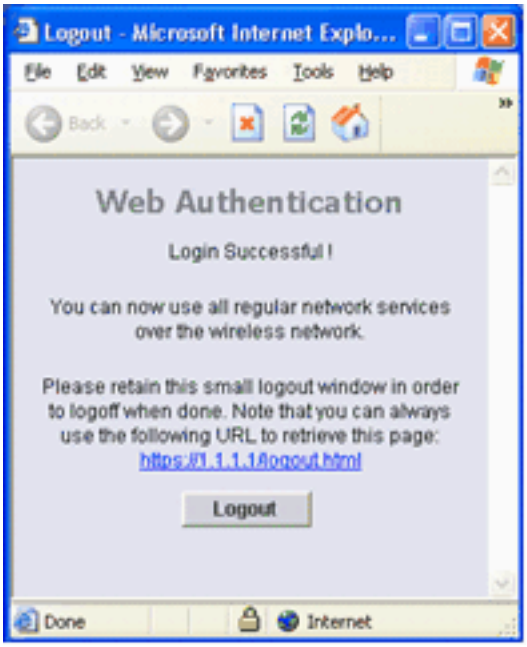
```
!
interface FastEthernet0/0
 description Connected to L2 Switch
 ip address 172.16.1.60 255.255.0.0
 duplex auto
 speed auto
!--- Interface connected to the Layer 2 switch. ! interface FastEthernet0/0.1 description Guest
VLAN encapsulation dot1Q 10 ip address 10.0.0.50 255.0.0.0 !--- Creates a sub-interface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

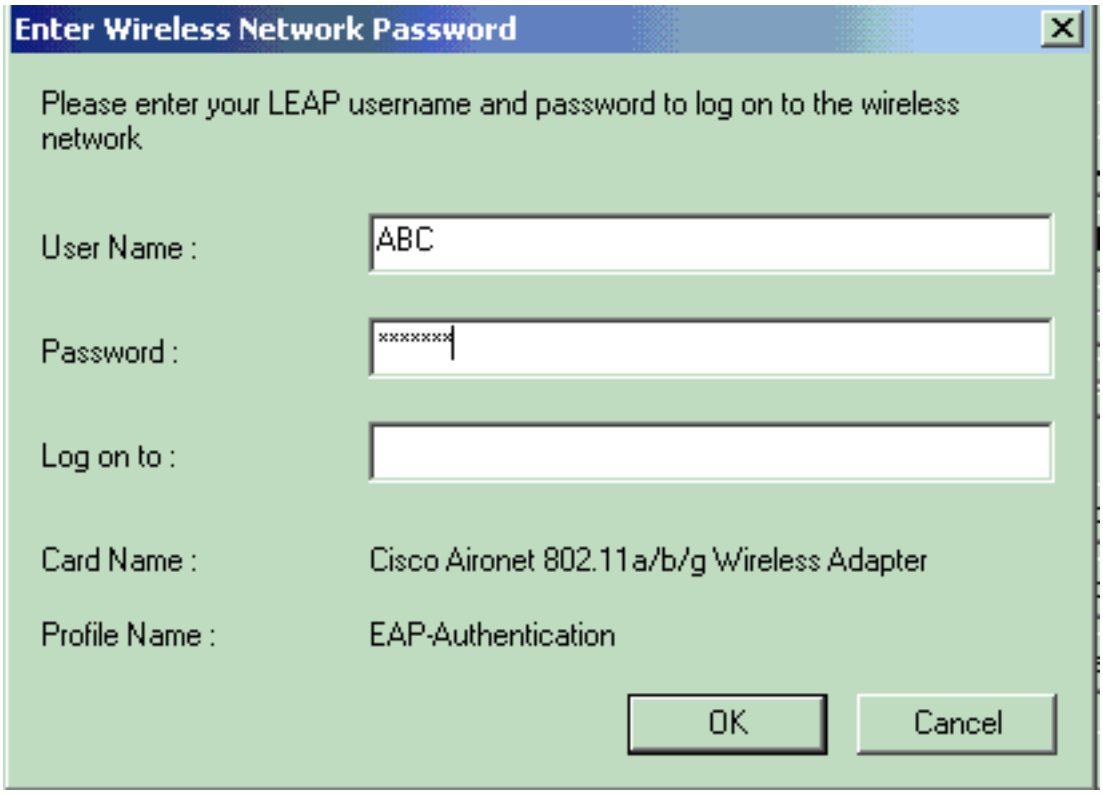
Use this section to confirm that your configuration works properly.

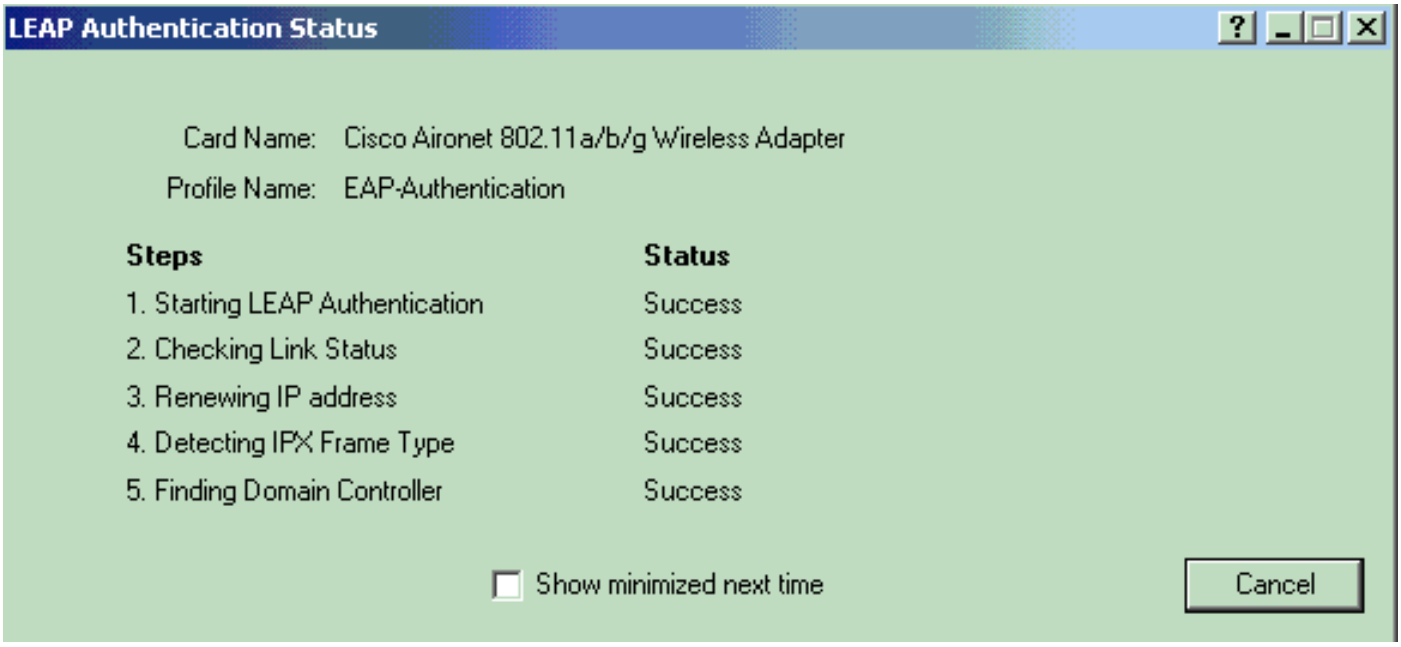
连接两个无线客户端，一个访客用户（服务集标识符 [SSID] 为 **Guest**）和一个内部用户（SSID 为 Internal），以验证配置是否能按预期方式正常工作。

请记住访客 WLAN 配置为 Web 身份验证。当访客无线客户端登录时，可在 Web 浏览器中输入任意 URL。这将弹出默认 Web 身份验证页面并提示您输入用户名和口令。当访客用户输入有效的用户名/口令之后，WLC 将对用户进行身份验证并允许其访问网络（或许是 Internet）。以下示例显示了用户看到的 Web 身份验证窗口以及成功通过身份验证后的结果：



本例中的内部 WLAN 配置为使用 802.1x 身份验证。当内部 WLAN 客户端登录时，客户端将使用 EAP 身份验证。有关如何配置客户端的 EAP 身份验证的详细信息，请参阅 Cisco Aironet 802.11a/b/g 无线局域网客户端适配器（CB21AG 和 PI21AG）安装和配置指南中的使用 EAP 身份验证部分。在成功进行身份验证后，用户便可以访问内部网络。以下示例显示了一个使用轻量可扩展身份验证协议 (LEAP) 进行身份验证的内部无线客户端：





Troubleshoot

故障检修程序

使用本部分可排除配置故障。

如果该配置未能按预期方式正常工作，请完成以下步骤：

1. 确保在连接到 WLC 的交换机端口上允许 WLC 上配置的所有 VLAN。
2. 确保将连接到 WLC 和路由器的交换机端口配置为中继端口。
3. 确保使用的 VLAN Id 与 WLC 和路由器上的相同。
4. 检查客户端是否收到来自 DHCP 服务器的 DHCP 地址。如果未收到，则检查是否正确配置了 DHCP 服务器。有关对客户端问题进行故障排除的详细信息，请参阅排除 Cisco 统一无线网络中的客户端问题。

其中一个使用 Web 身份验证的常见问题是在重定向到 Web 身份验证页面时无法正常工作。在打开浏览器时用户未看到 Web 身份验证窗口。相反，用户必须手动输入 **https://1.1.1.1/login.html** 以转到 Web 身份验证窗口。这与 DNS 查找有关，在重定向到 Web 身份验证页面之前必须先完成此任务。如果无线客户端上的浏览器主页指向一个域名，则一旦客户端建立关联，即需要成功执行 nslookup 以便进行重定向。

此外，对于运行早于 3.2.150.10 的版本的 WLC，Web 身份验证的工作方式是当该 SSID 中的用户试图访问 Internet 时，控制器的管理接口将执行 DNS 查询以查看该 URL 是否有效。如果有效，URL 将显示虚拟接口 IP 地址的身份验证页面。用户成功登录后，将允许原始请求返回客户端。这是由于 Cisco Bug ID CSCsc68105（仅限注册用户）。欲知更多信息，请参见排除在无线局域网控制器(WLC)的Web认证故障。

故障排除命令

Note: 使用 **debug** 命令之前，请参阅有关 Debug 命令的重要信息。

您可以使用以下调试命令排除配置故障：

- **debug mac addr <client-MAC-address xx:xx ：xx ：xx ：xx ：xx>** — 配置客户端的 MAC 地址

调试。

- **debug aaa all enable** - 配置所有 AAA 消息的调试。
- **debug pem state enable** — 配置策略管理器状态机的调试。
- **debug pem events enable** — 配置策略管理器事件的调试。
- **debug dhcp message enable** — 使用此命令以显示有关 DHCP 客户端活动的调试信息并监控 DHCP 数据包的状态。
- **debug dhcp packet enable** — 使用此命令以显示 DHCP 数据包级别信息。
- **debug pm ssh-appgw enable** — 配置应用程序网关的调试。
- **debug pm ssh-tcp enable** — 配置策略管理器 tcp 处理的调试。

下面是其中一些 **debug** 命令的输出范例：

Note: 由于空间有限，输出的一些行被拆分为两行显示。

```
(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 stateto 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
```

Related Information

- 无线访客访问FAQ
- 使用 Cisco WLAN 控制器的有线访客接入配置示例
- 无线局域网控制器上的身份验证配置示例
- 使用无线局域网控制器的外部 Web 身份验证配置示例
- Cisco 无线 LAN 控制器配置指南 4.0 版
- 无线产品支持
- Technical Support & Documentation - Cisco Systems