Ejemplo de Configuración de WLAN Guest y WLAN Interna mediante WLCs

Contenido

Introducción

Este documento proporciona un ejemplo de configuración de una LAN inalámbrica de invitado (WLAN) y una WLAN interna segura que utiliza Controladores de WLAN (WLC) y Lightweight Access Points (LAP). En la configuración de este documento, la WLAN de invitado utiliza la autenticación Web para autenticar a los usuarios y la WLAN interna segura utiliza la autenticación EAP (Extensible Authentication Protocol).

Prerequisites

Requisitos

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- Conocimiento de cómo configurar el WLC con los parámetros básicos
- Conocimiento de cómo poner un DHCP y un servidor del Domain Name System (DNS)

Componentes usados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco 2006 WLC que funciona con la versión 4.0 de los firmwares
- REVESTIMIENTO de las Cisco 1000 Series
- Adaptador de red inalámbrica de cliente de Cisco 802.11a/b/g que funciona con la versión 2.6 de los firmwares
- Cisco 2811 Router que funciona con la versión 12.4(2)XA de Cisco IOS®
- Conmutador de la serie de Cisco 3500 XL que funciona con la versión 12.0(5)WC3b del Cisco IOS
- Servidor DNS que se ejecuta en a Microsoft Windows 2000 Server

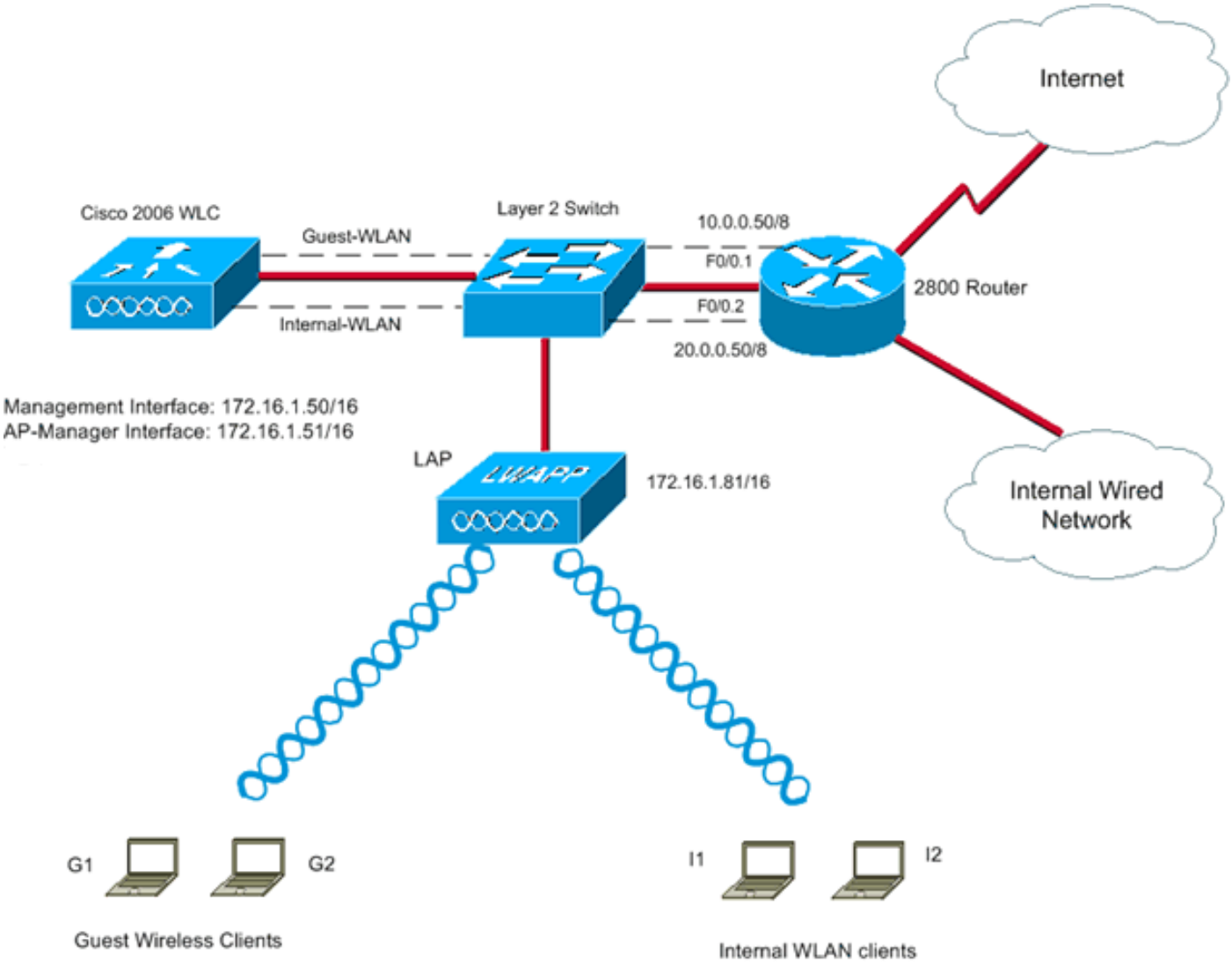
La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Configuración de la red

El ejemplo de la configuración en este documento utiliza la disposición visualizada en este diagrama. El REVESTIMIENTO se registra al WLC. El WLC está conectado con el 2 Switch de la capa. El router que conecta a los usuarios con WAN también conecta con el 2 Switch de la capa. Usted necesita crear dos redes inalámbricas (WLAN), una para los Usuarios invitados y la otra para los usuarios del LAN interno. Usted también necesita un servidor del DHCP proporcionar a los IP Addresses para el invitado y los clientes de red inalámbrica internos. Los Usuarios invitados utilizan la autenticación Web para tener acceso a la red. Los usuarios internos utilizan la autenticación EAP. El 2811 Router también actúa como el servidor del DHCP para los clientes de red inalámbrica.



Note: Este documento asume que el WLC está configurado con los parámetros básicos y el REVESTIMIENTO está registrado al WLC. Refiera al registro ligero AP (REVESTIMIENTO) a un regulador LAN de la Tecnología inalámbrica (WLC) para la información sobre cómo configurar los parámetros básicos en un WLC y cómo registrar el REVESTIMIENTO a WLC.

Cuando están configurada como servidor del DHCP, algunos de los Firewall no utilizan las solicitudes del DHCP de un Agente Relay. El WLC es Agente Relay para el cliente. El Firewall configurado como servidor del DHCP ignora estas solicitudes. Los clientes deben ser conectados directamente con el Firewall y no pueden enviar las solicitudes a través de otro Agente Relay o router. El Firewall puede trabajar como servidor simple del DHCP para los host internos que están conectados directamente con él. Esto permite que el Firewall mantenga su tabla basada en las direcciones MAC que están conectadas directamente y que puede ver. Esta es la razón por la cual una tentativa de asignar los direccionamientos de una retransmisión del DHCP no está disponible y se desechan los paquetes. El Firewall PIX tiene esta limitación.

Configurar

Complete estos pasos para configurar los dispositivos para esta configuración de la red:

1. Configure los interfaces dinámicos en el WLC para el invitado y los usuarios internos
2. Cree las redes inalámbricas (WLAN) para el invitado y los usuarios internos
3. Configure el puerto del 2 Switch de la capa que conecta con el WLC como puerto troncal

4. Configure al router para los dos VLA N

Configure los interfaces dinámicos en el WLC para el invitado y los usuarios internos

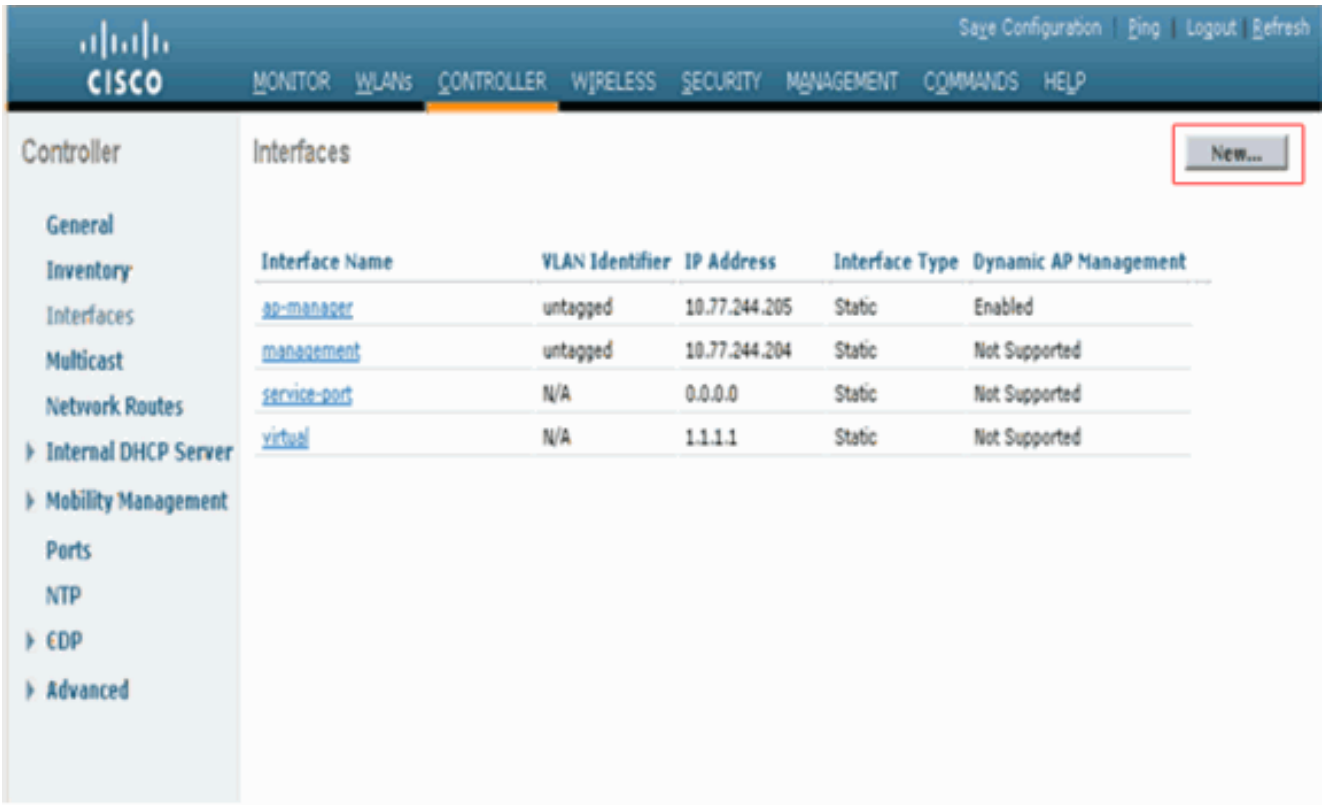
El primer paso es crear dos interfaces dinámicos en el WLC, uno para los Usuarios invitados y el otro para los usuarios internos.

El ejemplo en este documento utiliza estos parámetros y valores para los interfaces dinámicos:

```
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
```

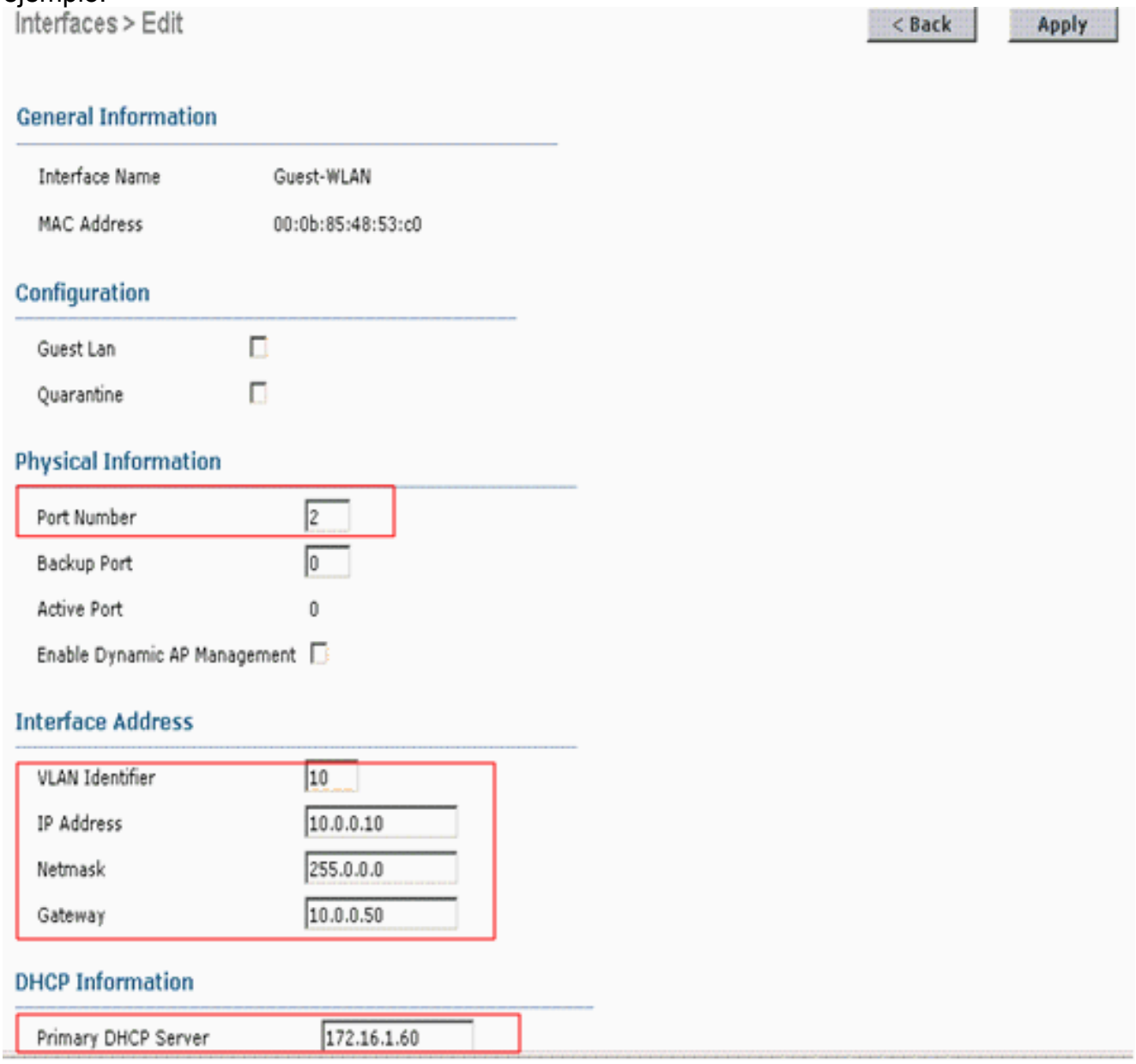
Complete estos pasos:

1. Del GUI WLC, elija los **reguladores > los interfaces**.La ventana de los interfaces aparece. Esta ventana enumera los interfaces que se configuran en el regulador. Esto incluye los interfaces del valor por defecto, que son la interfaz de administración, interfaz del ap-encargado, la interfaz virtual y la interfaz de puerto del servicio, y los interfaces dinámicos definidos por el
usario.



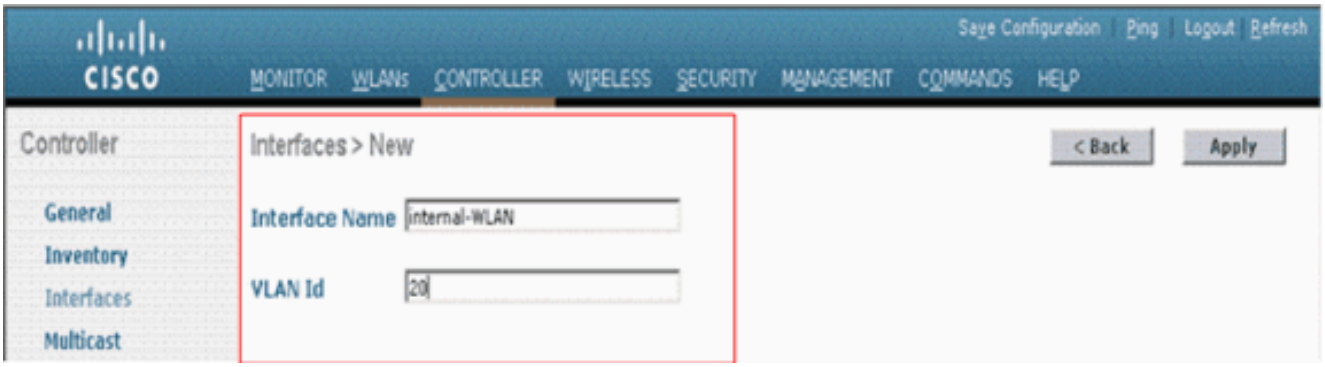
2. Haga clic **nuevo** para crear un nuevo interfaz dinámico.
3. En los interfaces > la nueva ventana, ingrese el nombre del interfaz y la identificación del VLA N. Entonces, el tecleo **se aplica**.En este ejemplo, el interfaz dinámico se nombra Invitado-RED INALÁMBRICA (WLAN) y la identificación del VLA N se asigna
10.

4. En los interfaces > corrija la ventana, para el interfaz dinámico, ingrese el IP address, la máscara de subred, y el gateway de valor por defecto. Asígnelo a un puerto físico en el WLC, y ingrese el IP address del servidor del DHCP. Entonces, el tecleo **se aplica**.Éste es el ejemplo:

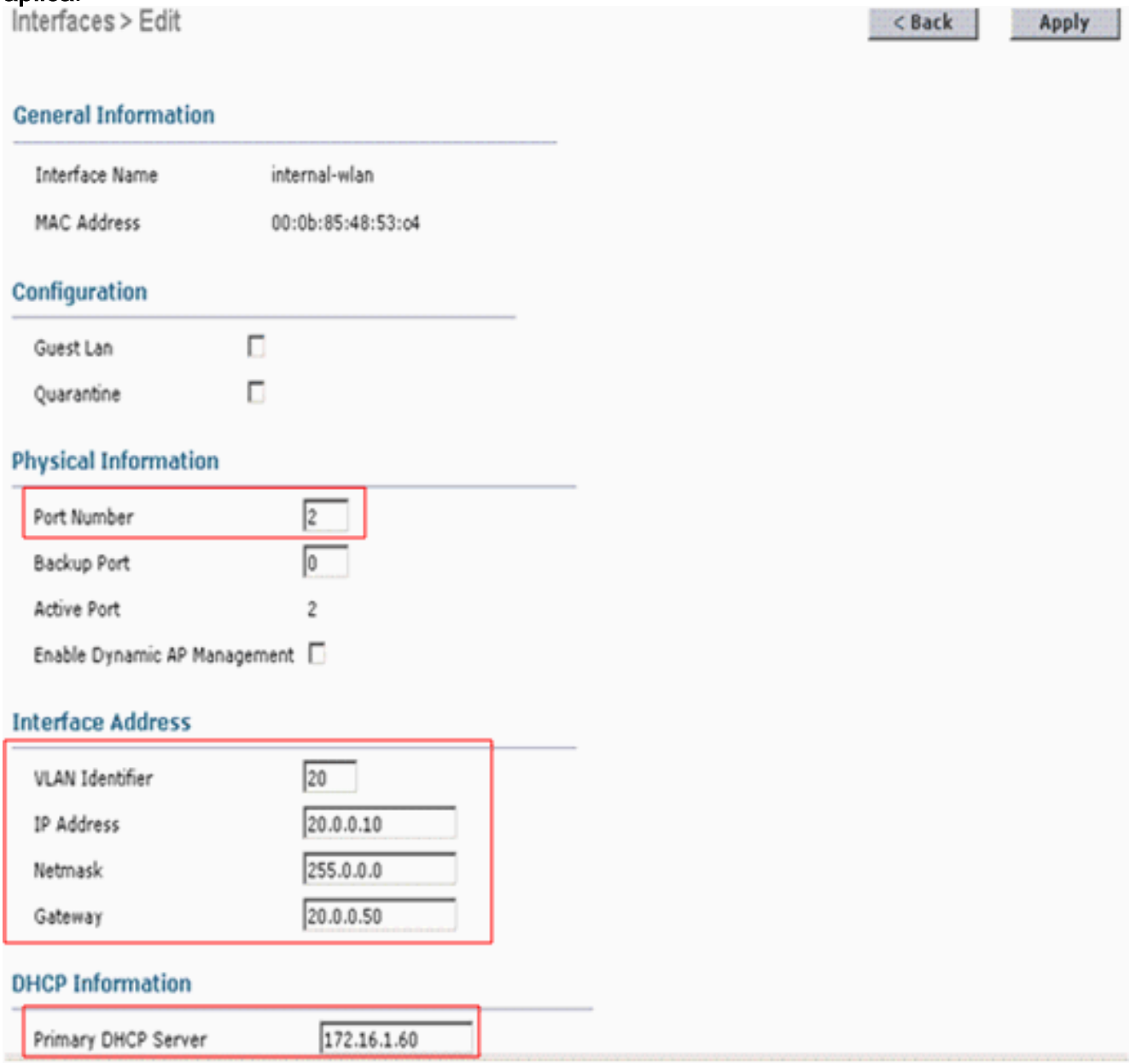


El mismo procedimiento se debe completar para crear un interfaz dinámico para la red inalámbrica (WLAN) interna.

5. En los interfaces > la nueva ventana, ingrese la Interno-**red inalámbrica (WLAN)** para el interfaz dinámico para los usuarios internos, y ingrese **20** para la identificación del VLA N. Entonces, el tecleo **se aplica**.



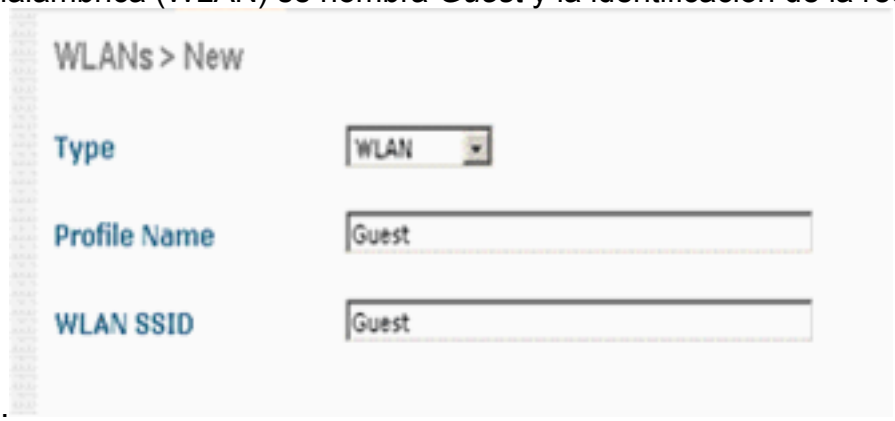
6. En los interfaces > corrija la ventana, para el interfaz dinámico, ingrese el IP address, la máscara de subred, y el gateway de valor por defecto. Asígnelo a un puerto físico en el WLC, y ingrese el IP address del servidor del DHCP. Entonces, el tecleo **se aplica**.



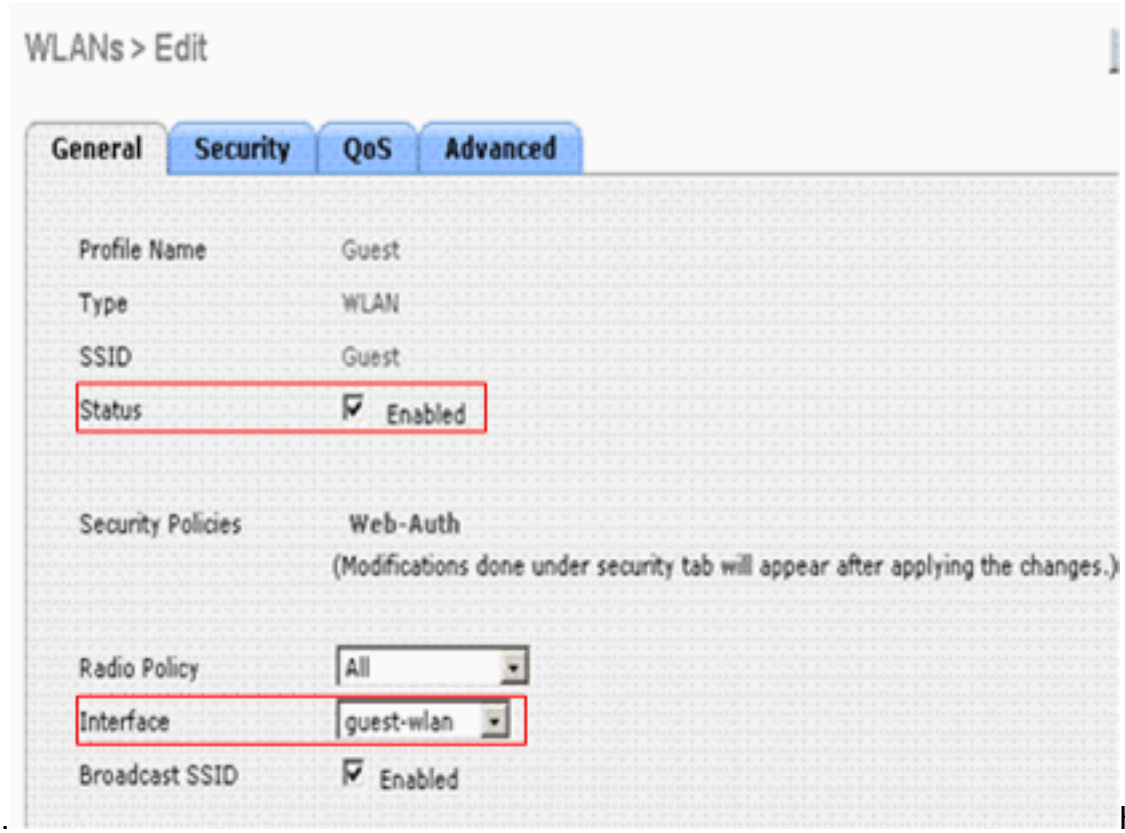
Ahora que se crean dos interfaces dinámicos, la ventana de los interfaces resume la lista de interfaces configurada en el
regulador.

Cree las redes inalámbricas (WLAN) para el invitado y los usuarios internos

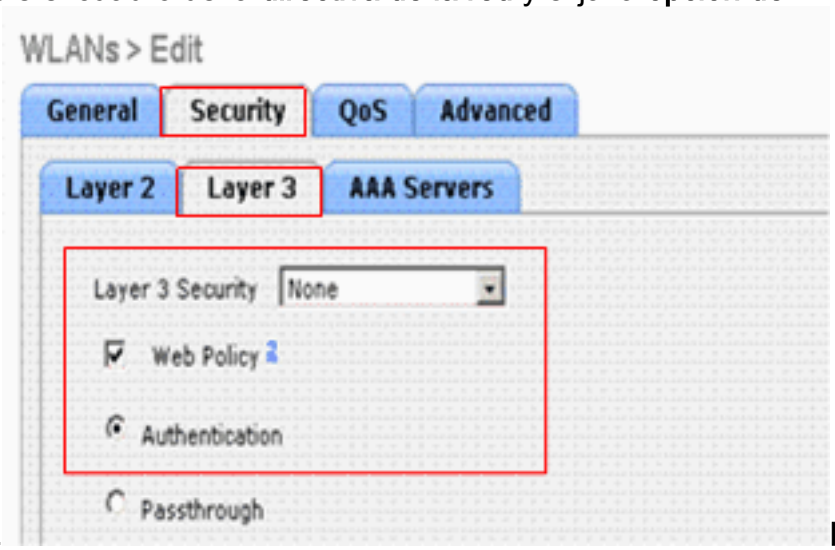
El siguiente paso es crear las redes inalámbricas (WLAN) para los Usuarios invitados y los usuarios internos, y asocia el interfaz dinámico a las redes inalámbricas (WLAN). También, los métodos de seguridad que se utilizan para autenticar el invitado y a los usuarios de red inalámbrica deben ser definidos. Complete estos pasos:

1. Haga clic las **redes inalámbricas (WLAN) del** GUI del regulador para crear una red inalámbrica (WLAN).La ventana de las redes inalámbricas (WLAN) aparece. Esta ventana enumera las redes inalámbricas (WLAN) configuradas en el regulador.
2. Tecleo **nuevo** para configurar una nueva red inalámbrica (WLAN).En este ejemplo, la red inalámbrica (WLAN) se nombra *Guest* y la identificación de la red inalámbrica (WLAN) es


2.
3. El tecleo **se aplica** en la esquina superior derecha.
4. La red inalámbrica (WLAN) > corrige la pantalla aparece, que contiene las diversas tabulaciones.Conforme a la **ficha general** para la red inalámbrica (WLAN) del invitado, elija invitado-**WLAN del** campo de nombre del interfaz. Esto asocia el interfaz dinámico invitado-**WLAN** que fue creado previamente al **invitado de la** red inalámbrica (WLAN).Asegúrese de que el estatus de la red inalámbrica (WLAN) esté

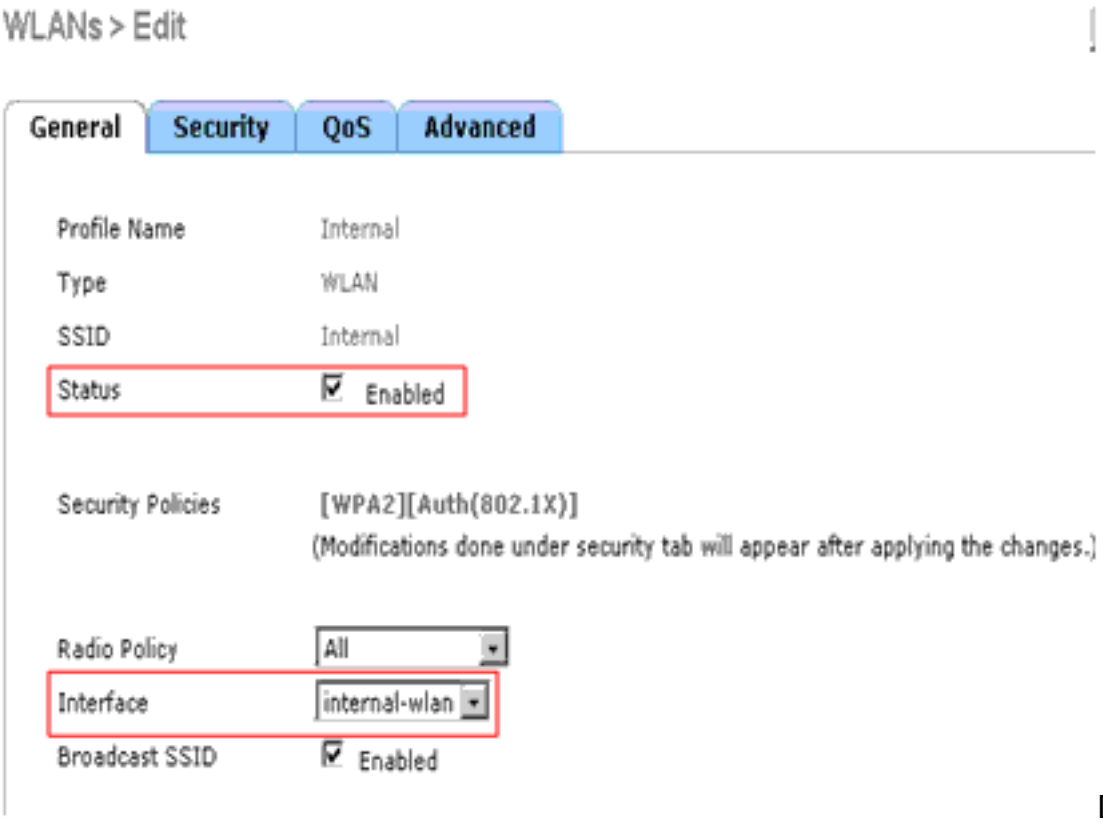


activado. Haga clic la **ficha de seguridad**. Para esta red inalámbrica (WLAN), la autenticación Web un mecanismo de seguridad de la capa 3 se utiliza para autenticar a los clientes. Por lo tanto, no elija **ninguno** bajo campo de Seguridad de la *capa 2*. En el campo de Seguridad de la *capa 3*, controle el cuadro de la **directiva de la red** y elija la **opción de**

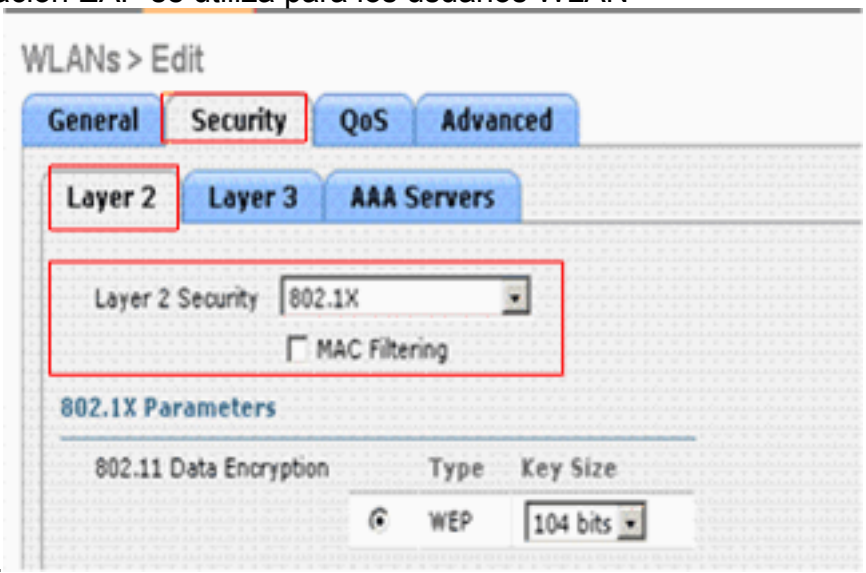


autenticación. **Note**: Para más información sobre la autenticación Web, refiera al ejemplo inalámbrico de la configuración de la autenticación Web del regulador LAN.Haga clic en Apply (Aplicar).

5. Cree una red inalámbrica (WLAN) para los usuarios internos. En el WLANs > la nueva ventana, ingrese **interno** y elija **3** para crear un WLAN para los usuarios internos. Entonces, el tecleo **se aplica**.
6. Las redes inalámbricas (WLAN) > corrigen la ventana aparecen. Conforme a la *ficha general*, elija interno-**WLAN del** campo de nombre del interfaz.Esto asocia el interfaz dinámico interno-**WLAN** que fue creado previamente a la red inalámbrica (WLAN) **interna**. Asegúrese de que la red inalámbrica (WLAN) esté



activada. Deje la opción de seguridad de la capa 2 en el 802.1x del valor predeterminado porque la autenticación EAP se utiliza para los usuarios WLAN



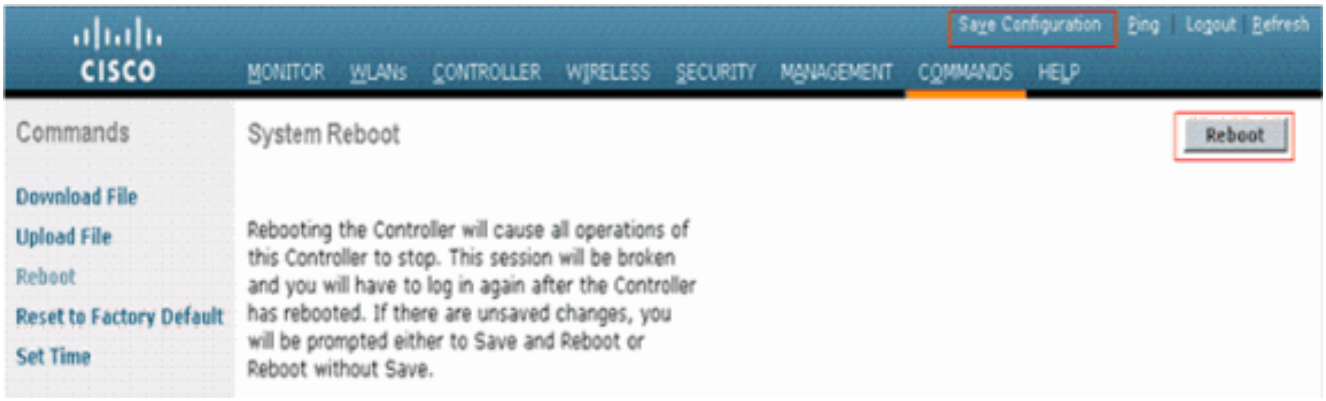
internos.

7. Haga clic en Apply (Aplicar).La ventana de la red inalámbrica (WLAN) aparece y muestra la lista de redes inalámbricas (WLAN) se creen que.

Note: Refiera a la [autenticación EAP con el ejemplo de la configuración de los reguladores]

de la red inalámbrica (WLAN) (WLC) para información más detallada sobre cómo configurar una red inalámbrica (WLAN) EAP-basada con WLCs.

8. En el GUI WLC, haga clic la **configuración de la salvaguardia**, después haga clic los **comandos del** GUI del regulador. Después, elija la opción de la **reinicialización** para reiniciar el WLC para permitir que la autenticación Web tome el efecto.



Note: **Configuración de la salvaguardia del** tecleo para salvar la configuración a través de las reinicializaciones.

Configure el puerto del 2 Switch de la capa que conecta con el WLC como puerto troncal

Usted necesita configurar el puerto del switch para utilizar los VLAN múltiples configurados en el WLC porque el WLC está conectado con un 2 Switch de la capa. Usted debe configurar el puerto del switch como puerto de tronco 802.1q.

Cada conexión del puerto del regulador es un tronco 802.1q y se debe configurar como esto en el switch de vecino. En el Switches de Cisco, el VLA N nativo de un tronco 802.1q, por ejemplo el **VLA N 1**, se deja untagged. Por lo tanto, si usted configura el interfaz de un regulador para utilizar el VLA N nativo en un conmutador vecino de Cisco, asegúrese de le para configurar el interfaz en el regulador como untagged.

Un valor cero para el identificador del **VLA N** (en el regulador > interconecta la ventana) significa que el interfaz es untagged. En el ejemplo en este documento, configuran al AP-encargado y las interfaces de administración en el VLAN sin Tags del valor por defecto.

Cuando un interfaz del regulador se fija a un valor sin cero, no debe ser marcado con etiqueta al VLA N nativo del conmutador y el VLA N se debe permitir en el conmutador. En este ejemplo, el VLA N 60 se configura como el VLA N nativo en el puerto del switch que conecta con el regulador.

Ésta es la configuración para el puerto del switch que conecta con el 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
```

Ésta es la configuración para el puerto del switch que conecta con el router como puerto troncal:

```
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
```

Ésta es la configuración para el puerto del switch que conecta con el REVESTIMIENTO. Este puerto se configura como puerto de acceso:

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

Configure al router para las dos redes inalámbricas (WLAN)

En el ejemplo en este documento, el 2811 Router conecta a los Usuarios invitados con Internet y también conecta a los usuarios atados con alambre internos con los usuarios de red inalámbrica internos. Usted también necesita configurar al router para proporcionar los servicios del DHCP.

En el router, cree los sub-interfaces bajo interfaz FastEthernet que conecta con el puerto troncal en el conmutador para cada VLA N. Asigne los sub-interfaces a los VLA N correspondientes, y configure una dirección IP de las subredes correspondientes.

Note: Solamente las porciones pertinentes de la configuración del router se dan, y no la configuración completa.

Ésta es la configuración requerida en el router para lograr esto.

Éstos son los comandos que se deben publicar para configurar los servicios del DHCP en el 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. !
```

Estos comandos se deben publicar en la interfaz FastEthernet por el ejemplo puesto:

```
!
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
```

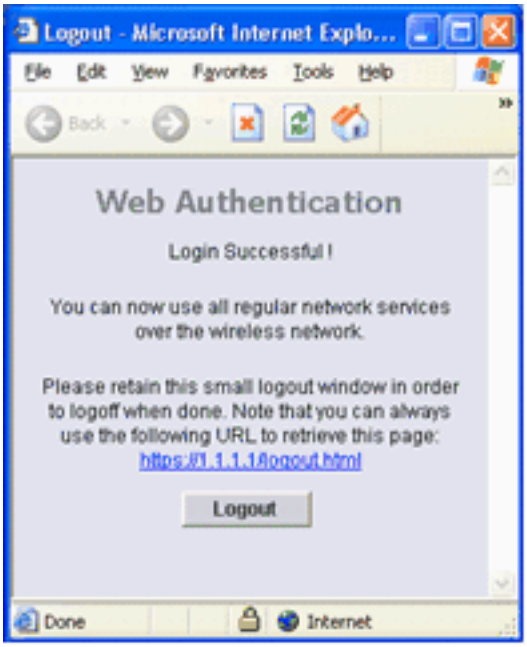
```
FastEthernet0/0 for the guest VLAN. ! interface FastEthernet0/0.2 description Internal VLAN
encapsulation dot1Q 20 ip address 20.0.0.50 255.0.0.0 !--- Creates a sub-interface under
FastEthernet0/0 for the internal VLAN. !
```

Verifique

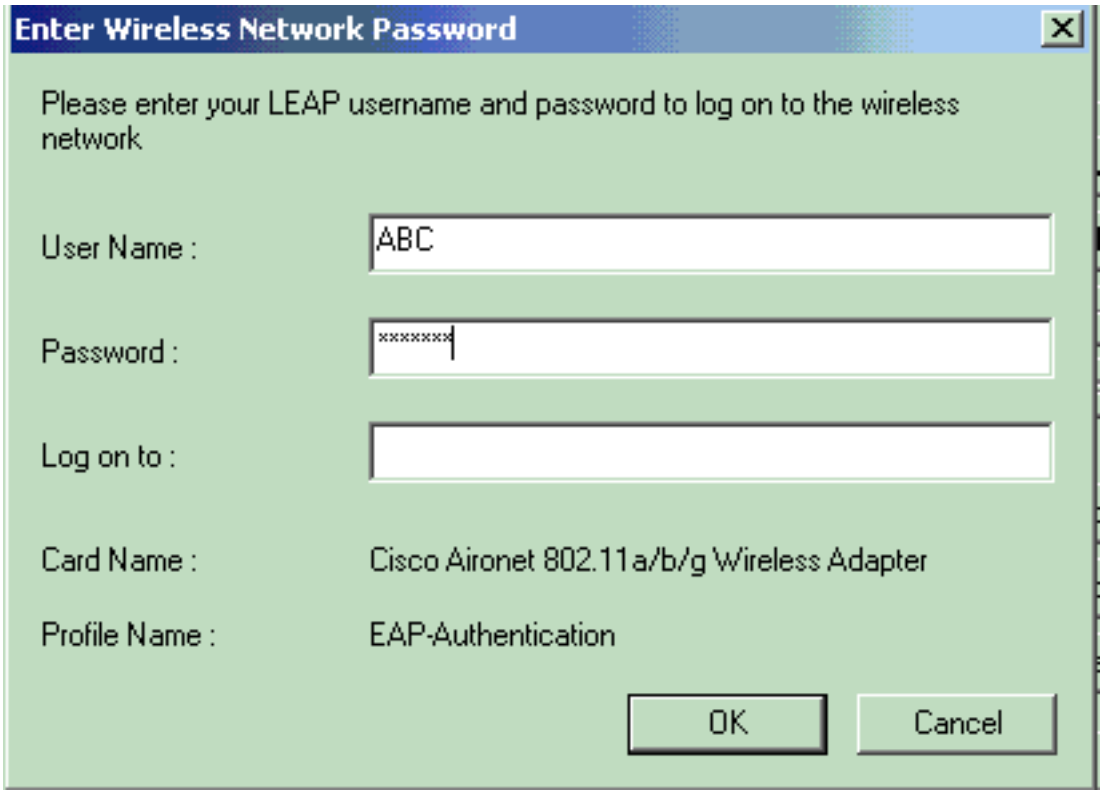
Use esta sección para confirmar que su configuración funciona correctamente.

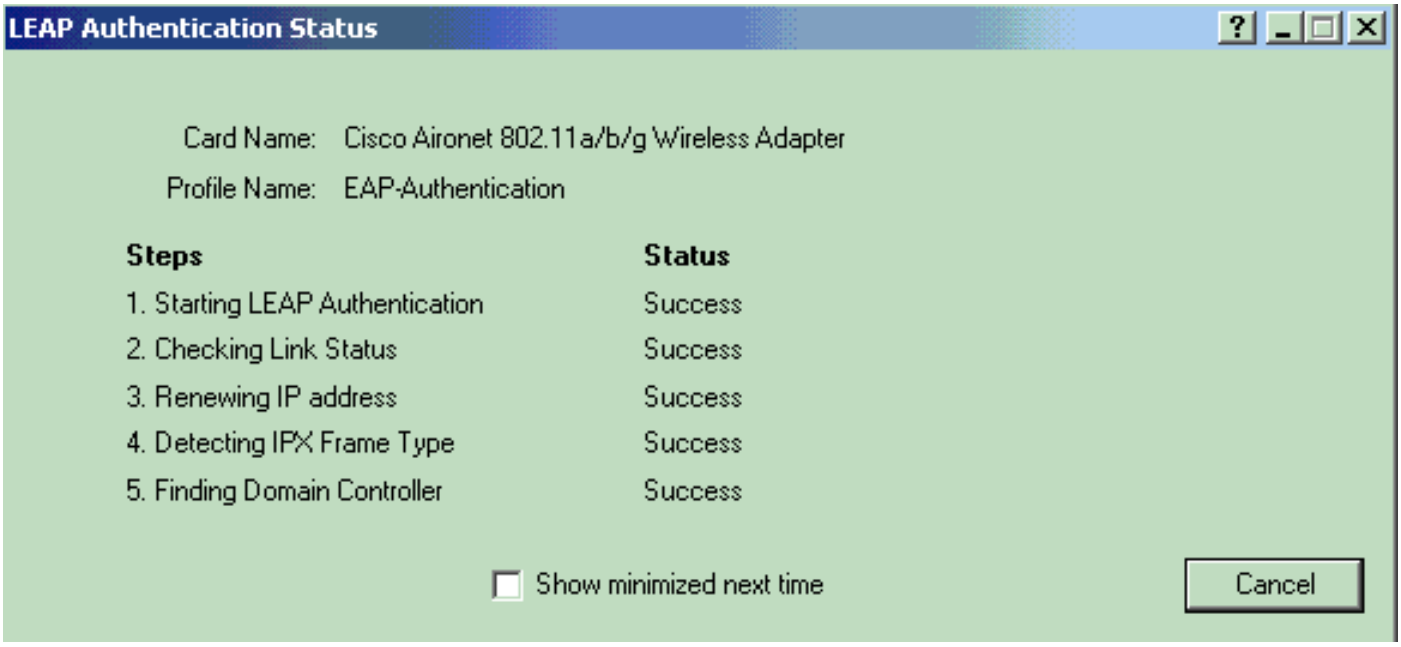
Conecte dos clientes de red inalámbrica, un Usuario invitado (con el **invitado del** [SSID] del identificador del conjunto de servicio) y a un usuario interno (con el SSID **interno**), para verificar los trabajos de la configuración como se esperaba.

Recuerde que la red inalámbrica (WLAN) del invitado fue configurada para la autenticación Web. Cuando sube el cliente de red inalámbrica del invitado, ingrese cualquier URL en el buscador Web. La página de la autenticación del Web predeterminada le surge e incita ingresar el nombre de usuario y contraseña. Una vez que el Usuario invitado ingresa un nombre de usuario válido/una contraseña, el WLC autentica al Usuario invitado y permite el acceso a la red (posiblemente el Internet). Este ejemplo muestra la ventana de la autenticación Web que el usuario recibe y la salida en una autenticación satisfactoria:



La red inalámbrica (WLAN) interna en este ejemplo se configura para la autenticación del 802.1x. Cuando sube el cliente interno de la red inalámbrica (WLAN), el cliente utiliza la autenticación EAP. Para más información sobre cómo configurar al cliente para la autenticación EAP, refiera a la sección de la autenticación EAP que usa de la guía de instalación y configuración inalámbrica de los adaptadores del cliente LAN de Cisco Aironet 802.11a/b/g (CB21AG y PI21AG). Después de la autenticación satisfactoria, el usuario puede tener acceso a la red interna. Este ejemplo muestra a un cliente de red inalámbrica interno que utilice la autenticación del protocolo lightweight extensible authentication (SALTO):





Troubleshooting

Resolver problemas el procedimiento

Use esta sección para resolver problemas de configuración.

Si la configuración no trabaja como se esperaba, complete estos pasos:

1. Asegúrese de que todos los VLA N configurados en el WLC estén permitidos en el puerto del switch conectado con el WLC.
2. Asegúrese que ese puerto del switch que conecta con el WLC y con el router se configura como puerto troncal.
3. Asegúrese de que los Ids del VLA N usados sean lo mismo en el WLC y el router.
4. Controle si los clientes reciben los direccionamientos del DHCP del servidor del DHCP. Si no, controle si el servidor del DHCP se configura correctamente. Para más información sobre resolver problemas del cliente, refiera a resolver problemas del cliente en la red inalámbrica unificada Cisco.

Uno de los problemas frecuentes que ocurre con la autenticación Web es cuando la reorientación a la página de la autenticación Web no trabaja. El usuario no ve la ventana de la autenticación Web cuando abren al navegador. En lugar, el usuario debe ingresar manualmente **https://1.1.1.1/login.html** para conseguir a la ventana de la autenticación Web. Esto tiene que hacer con la búsqueda de DNS, que ocurren las necesidades de trabajar antes de la reorientación a la página de la autenticación Web. Si el homepage del navegador en el cliente de red inalámbrica señala a un Domain Name, usted necesita realizar el nslookup con éxito una vez que el cliente se asocia para que la reorientación trabaje.

También, para un WLC que funcione con una versión anterior que 3.2.150.10, la manera que los trabajos de la autenticación Web son cuando un usuario en ese SSID intenta tener acceso a Internet, la interfaz de administración del regulador hace una interrogación DNS para considerar si el URL es válido. Si es válida, el URL muestra la página de la autorización con la dirección IP de las interfaces virtuales. Después de que el usuario inicia sesión con éxito, el cliente recupera la solicitud original. Esto está debido al ID de bug CSCsc68105 (clientes registrados de Cisco solamente). Para más información, refiera a la autenticación Web del troubleshooting en un

regulador LAN de la Tecnología inalámbrica (WLC).

Comandos para resolución de problemas

Note: Refiera a la información importante en los comandos Debug antes de que usted utilice los **comandos debug**.

Usted puede utilizar estos comandos debug para resolver problemas la configuración:

- **<client-MAC-direccionamiento xx addr del mac de la depuración: xx: xx: xx: xx: xx>** — Configura el depuración de la dirección MAC para el cliente.
- **la depuración aaa todo activa** — Configura la depuración de todos los mensajes AAA.
- **permiso del estado PEM de la depuración** — Configura la depuración de la máquina de estado del encargado de la directiva.
- **permiso de los eventos PEM de la depuración** — Configura la depuración de los eventos del encargado de la directiva.
- **permiso del mensaje DHCP de la depuración** — Utilice este comando para visualizar la información de debugging sobre las actividades del Cliente de DHCP y vigilar el estatus de los paquetes del DHCP.
- **ponga a punto el permiso del paquete DHCP** — Utilice este comando para visualizar la información del nivel del paquete del DHCP.
- **ponga a punto el permiso P.M. SSH-appgw** — Configura la depuración de los gatewayes de aplicación.
- **permiso de la depuración P.M. SSH-TCP** — Configura la depuración de la dirección tcp del encargado de la directiva.

Aquí están las salidas de muestra de algunos de estos **comandos debug**:

Note: Algunas líneas de salida se han envuelto a una segunda línea debido a las razones espaciales.

```
(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
```

Información Relacionada

- Preguntas Más Frecuentes sobre Acceso Guest Inalámbrico
- Acceso a Invitado Conectado con Ejemplo de configuración de Cisco WLAN Controllers
- Autenticación en el ejemplo inalámbrico de la configuración de los reguladores LAN
- Autenticación del Web externa con el ejemplo inalámbrico de la configuración de los reguladores LAN
- Guía de configuración del Controlador de LAN de la Red Inalámbrica Cisco, versión 4.0
- Soporte de Productos de Red Inalámbrica
- Soporte técnico y documentación - Cisco Systems