Asignación del VLAN dinámico con el servidor de RADIUS y el ejemplo de la configuración de controlador del Wireless LAN

Contenido

Introducción

Este documento presenta el concepto de asignación de VLAN dinámica. El documento explica cómo configurar el controlador de LAN inalámbrico (WLC) y un servidor RADIUS para asignar dinámicamente clientes de LAN inalámbrica (WLAN) a una VLAN específica.

prerrequisitos

Requisitos

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- Tenga conocimiento básico del WLC y de los Puntos de acceso ligeros (los revestimientos)
- Tenga conocimiento funcional del servidor de AAA

- Tenga conocimiento completo de las redes inalámbricas y de los problemas de seguridad de red inalámbrica
- Tenga conocimiento básico del protocolo ligero AP (el LWAPP)

Componentes Utilizados

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

- WLC de Cisco 4400 que funciona con la versión de firmware 5.2
- REVESTIMIENTO de las Cisco 1130 Series
- Adaptador de red inalámbrica de cliente de Cisco 802.11a/b/g que funciona con la versión de firmware 4.4
- Utilidad de escritorio del Cisco Aironet (ADU) esa versión 4.4 de los funcionamientos
- Access Control Server del CiscoSecure (ACS) esa versión 4.1 de los funcionamientos
- Cisco 2950 Series Switch

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.

Asignación del VLAN dinámico con el servidor de RADIUS

En la mayoría de los sistemas WLAN, cada red inalámbrica (WLAN) tiene una directiva estática que se aplique a todos los clientes asociados a un Service Set Identifier (SSID), o red inalámbrica (WLAN) en la terminología del controlador. Aunque sea potente, este método tenga limitaciones porque requiere a los clientes asociarse a diversos SSID para heredar diverso QoS y las políticas de seguridad.

Sin embargo, la solución de Cisco WLAN soporta el establecimiento de una red de la identidad. Esto permite la red haga publicidad de un solo SSID, pero permite que los usuarios específicos hereden diverso QoS o las políticas de seguridad basadas en el credencial de usuario.

La asignación del VLAN dinámico es una tal característica que coloca a un usuario de red inalámbrica en un VLA N específico basado en las credenciales suministradas por el usuario. Esta tarea de asignar a los usuarios a un VLA N específico es manejada por un servidor de autenticación de RADIUS, tal como CiscoSecure ACS. Esto se puede utilizar, por ejemplo, para permitir que el host inalámbrico permanezca en el mismo VLA N que mueve dentro de una red de oficinas centrales.

Por lo tanto, cuando un cliente intenta asociarse a un REVESTIMIENTO registrado a un regulador, el REVESTIMIENTO pasa las credenciales del usuario al servidor de RADIUS para la validación. Una vez que la autenticación es acertada, el servidor de RADIUS pasa ciertos atributos de la Fuerza de tareas de ingeniería en Internet (IETF) (IETF) al usuario. Estos atributos de RADIUS deciden al VLAN ID que se debe asignar al cliente de red inalámbrica. El SSID (red

inalámbrica (WLAN), en términos de WLC) del cliente no importa porque asignan el usuario siempre a este VLAN ID predeterminado.

Los atributos del usuario de RADIUS usados para la asignación VLAN ID son:

- IETF 64 (tipo de túnel) — Fije esto al VLA N.
- IETF 65 (tipo medio del túnel) — fije esto a 802
- IETF 81 (ID de grupo privado del túnel) — fije esto al VLAN ID.

El VLAN ID es 12-bits, y toma un valor entre 1 y 4094, inclusivo. Porque el Túnel-Soldado-Grupo-ID está de tipo string, según lo definido en el RFC2868 para el uso con el IEEE 802.1X, el valor del número entero VLAN ID se codifica como cadena. Cuando se envían estos atributos del túnel, es necesario completar el campo de la etiqueta.

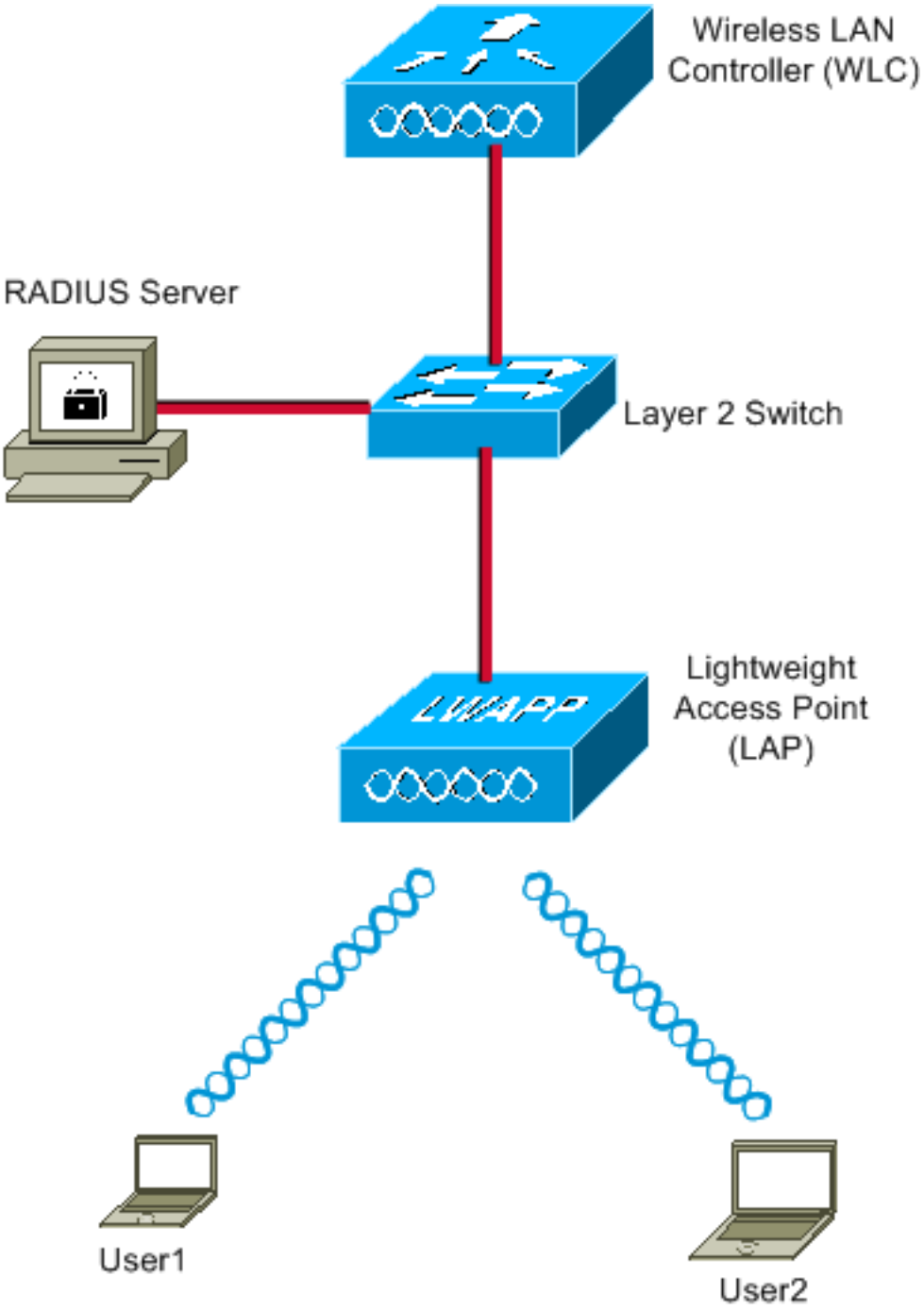
Como se apunta en el RFC2868 , sección 3.1: **El campo de la etiqueta es un octeto de largo y se piensa proporcionar los medios de agrupar los atributos en el mismo paquete que refieren al mismo túnel.** Los valores válidos para este campo son 0x01 con 0x1F, inclusivo. Si el campo de la etiqueta es inusitado, debe ser cero (0x00). Refiera al RFC 2868 para más información sobre todos los atributos de RADIUS.

Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

Diagrama de la red

En este documento, se utiliza esta configuración de red:



Éstos son los detalles de la configuración de los componentes usados en este diagrama:

- La dirección IP del servidor ACS (RADIUS) es 172.16.1.1.
- El direccionamiento de la interfaz de administración del WLC es 172.16.1.30.
- El direccionamiento de la interfaz del AP manager del WLC es 172.16.1.31.
- El direccionamiento 172.16.1.1 del servidor DHCP se utiliza para asignar los IP Addresses al LWAPP. **Utilizan al servidor DHCP interno en el regulador para asignar la dirección IP a los clientes de red inalámbrica.**
- El VLAN10 y VLAN11 se utilizan en esta configuración. El user1 se configura para ser colocado en el VLAN10 y el user2 se configura para ser colocado en VLAN11 por el servidor de RADIUS.**Nota:** Este documento muestra solamente toda la configuración relacionada con la información al user1. Complete el mismo procedimiento explicado en este documento para el user2.
- Este documento utiliza el 802.1x con el SALTO como el mecanismo de seguridad.**Nota:** Cisco recomienda que usted utiliza los métodos de autentificación avanzados, tales como EAP-

FAST y autenticación EAP-TLS, para asegurar la red inalámbrica (WLAN). Este documento utiliza el SALTO solamente para la simplicidad.

Configuración

Antes de la configuración, este documento asume que el REVESTIMIENTO está registrado ya con el WLC. Refiera al ejemplo de la configuración básica del regulador y del Lightweight Access Point del Wireless LAN para más información. Refiera al registro ligero AP (REVESTIMIENTO) a un regulador del Wireless LAN (WLC) para la información sobre el procedimiento de inscripción implicado.

Pasos de configuración

Esta configuración se separa en tres categorías:

1. Configuración del servidor de RADIUS
2. Configure el Switch para los VLAN múltiples
3. Configuración del WLC
4. Configuración de utilidad del cliente de red inalámbrica

Configuración del servidor de RADIUS

La configuración requiere estos pasos:

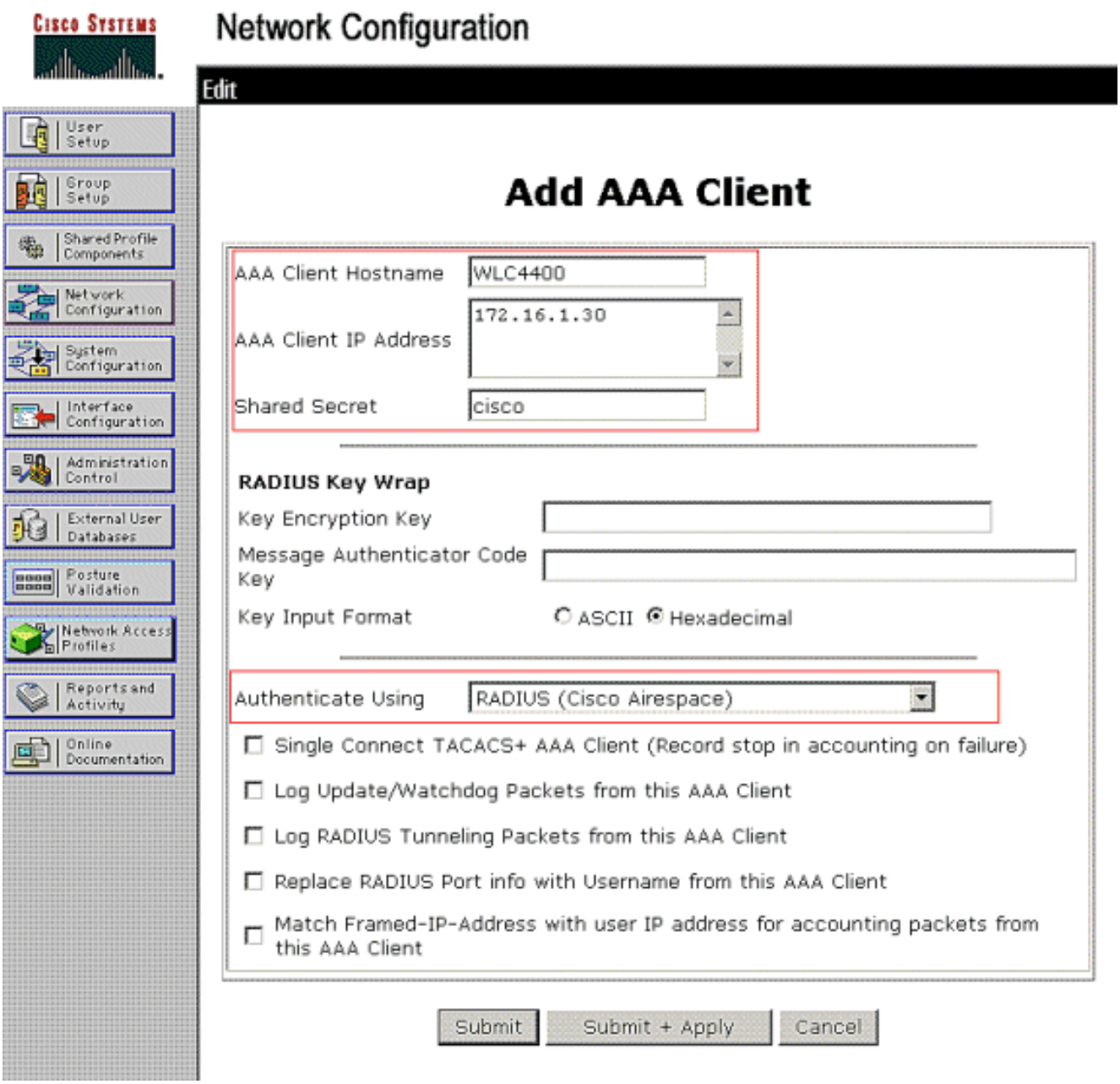
- Configure el WLC como cliente AAA en el servidor de RADIUS
- Configure los usuarios y los atributos RADIUS (IETF) usados para la asignación del VLAN dinámico en el servidor de RADIUS

Configure al cliente AAA para el WLC en el servidor de RADIUS

Este procedimiento explica cómo agregar el WLC como cliente AAA en el servidor de RADIUS de modo que el WLC pueda pasar los credenciales de usuario al servidor de RADIUS.

Complete estos pasos:

1. Del ACS GUI, haga clic la **configuración de red**.
2. Haga clic la sección de la **entrada del agregar** bajo campo de los clientes AAA.
3. Ingrese el IP Address y la clave del cliente AAA.La dirección IP debe ser la dirección IP de la interfaz de administración del WLC.Aseegurese que la clave que usted ingresa es lo mismo que la que está configurada en el WLC bajo la ventana de seguridad. Ésta es la clave secreta usada para la comunicación entre el cliente AAA (WLC) y el servidor de RADIUS.
4. Elija **RADIUS (Airespace de Cisco) de la** autenticidad usando el campo para el tipo de autenticación.

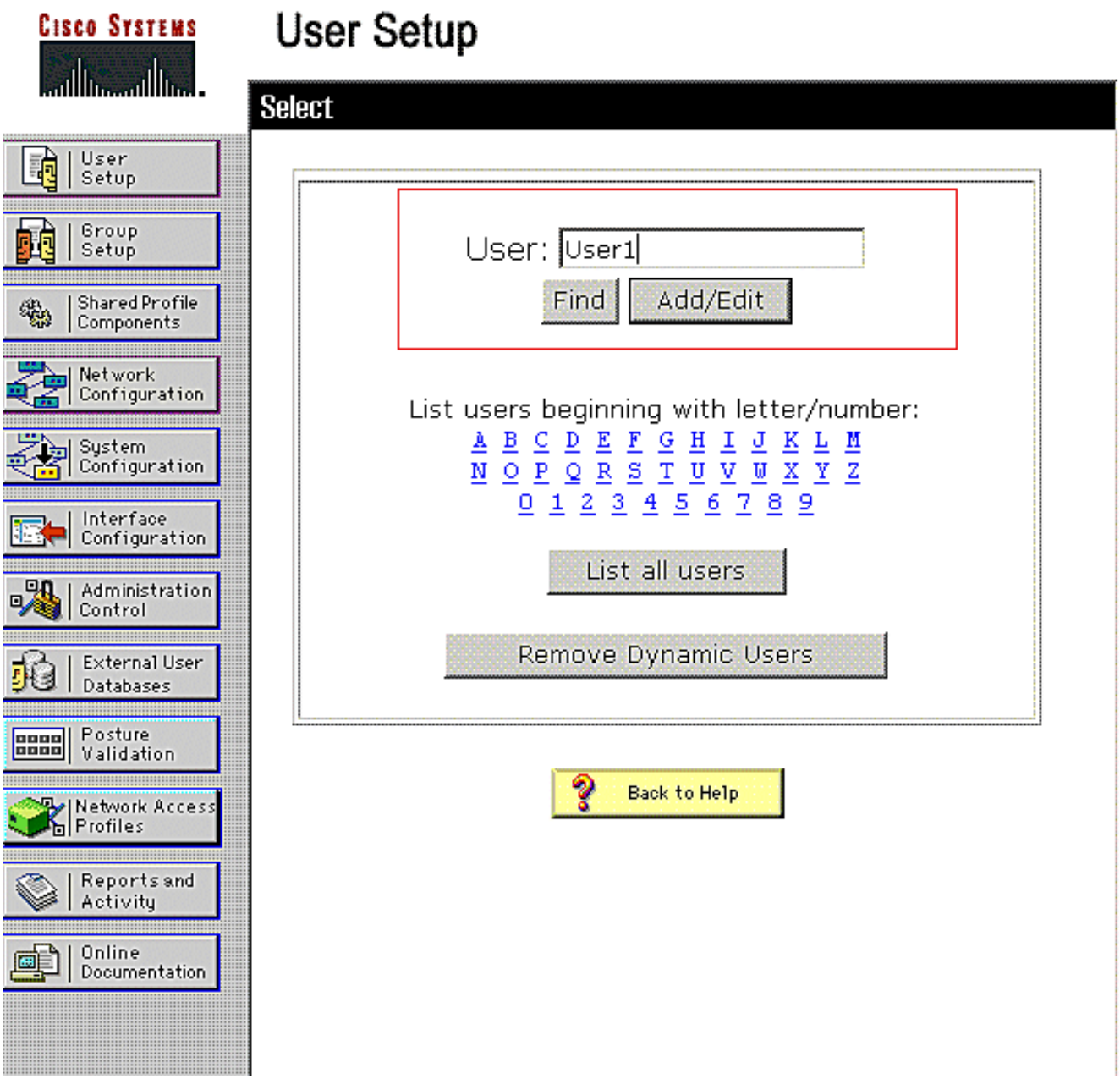


Configure los usuarios y los atributos RADIUS (IETF) usados para la asignación del VLAN dinámico en el servidor de RADIUS

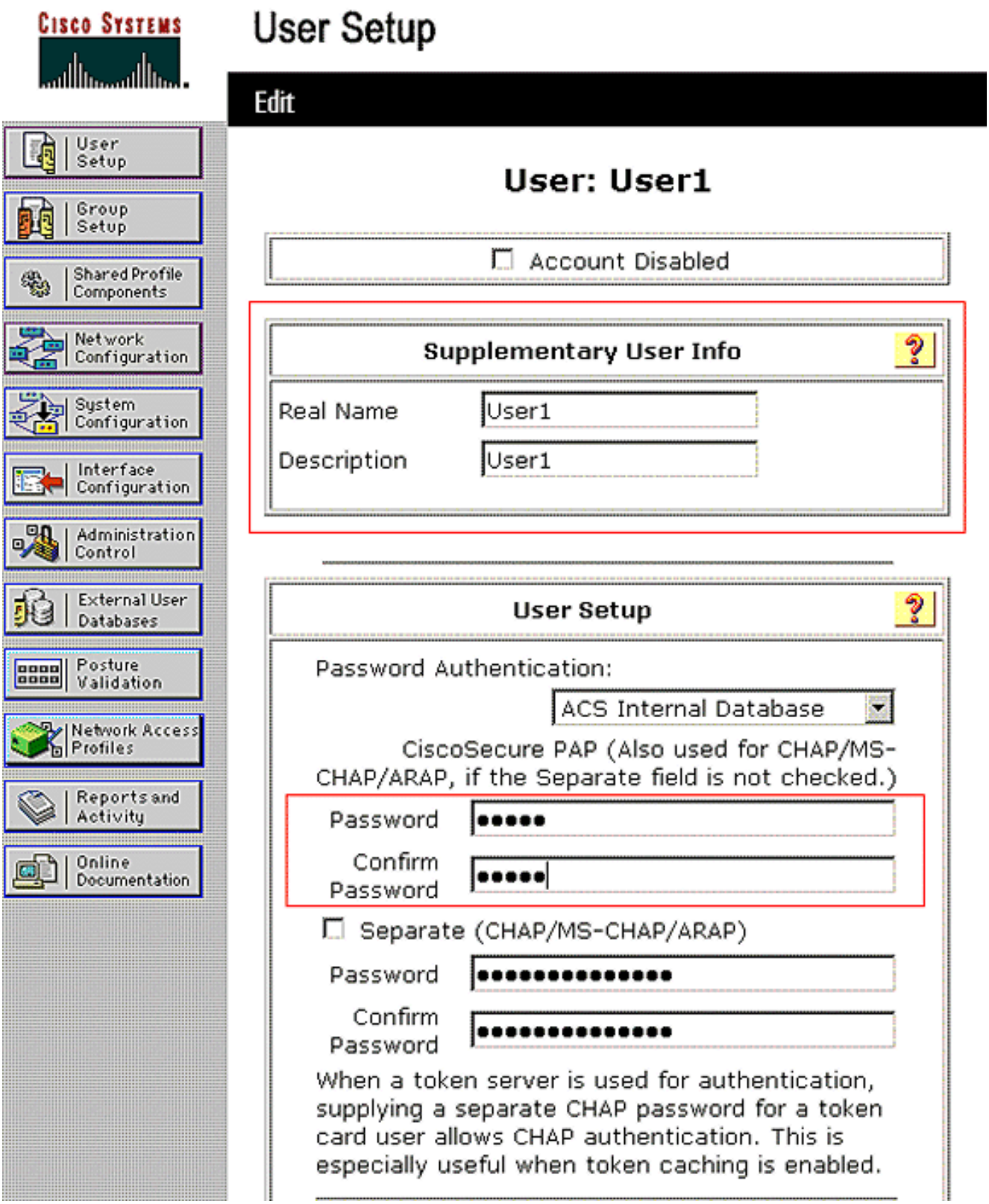
Este procedimiento explica cómo configurar a los usuarios en el servidor de RADIUS y los atributos RADIUS (IETF) usados para asignar las identificaciones de VLAN a estos usuarios.

Complete estos pasos:

1. Del ACS GUI, haga clic la **configuración de usuario**.
2. En la ventana de la configuración de usuario, ingrese un nombre de usuario en el campo del usuario y el tecleo
agrega/edita.

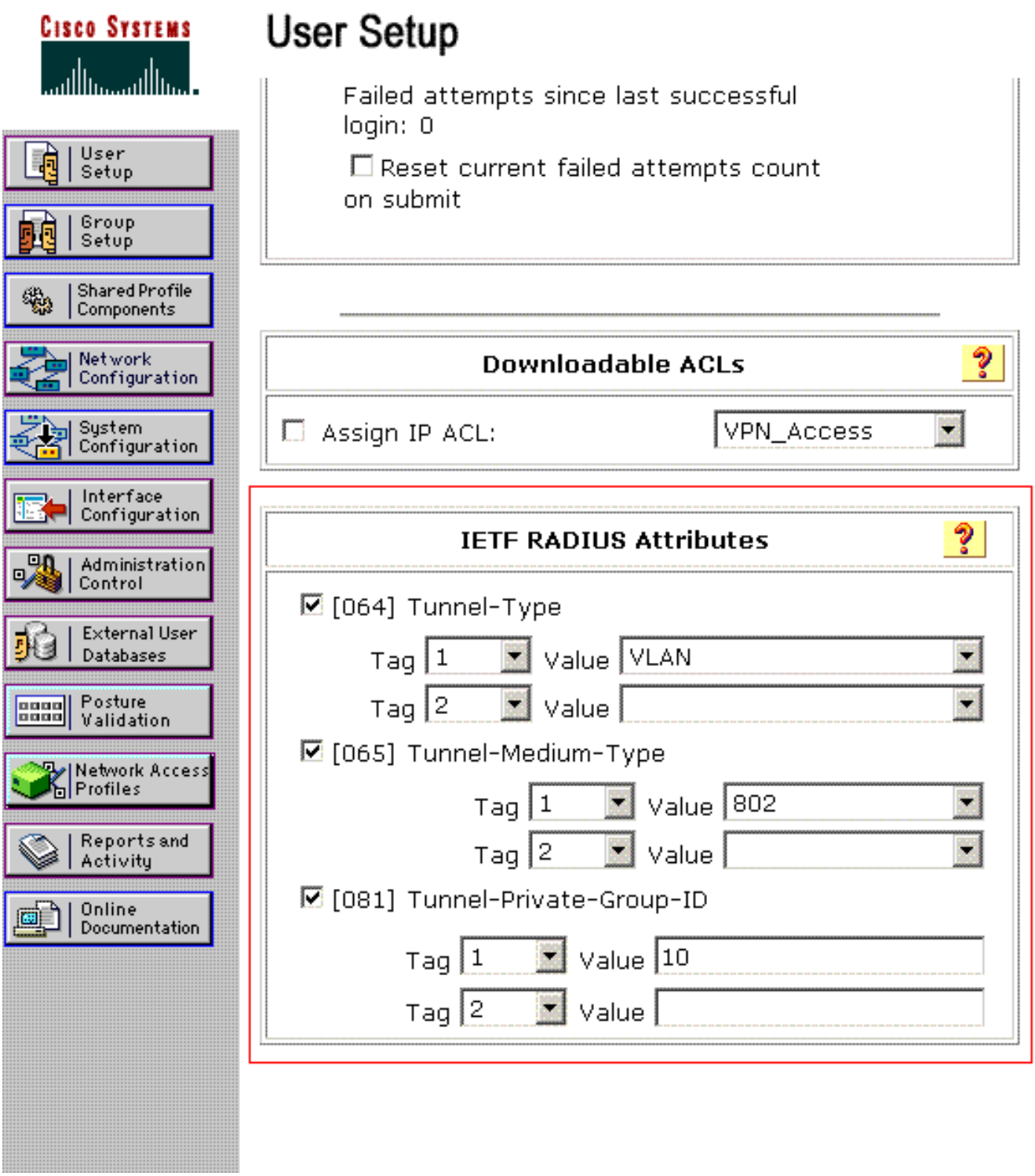


3. En la página del editar, ingrese la información del usuario necesaria como se muestra aquí:

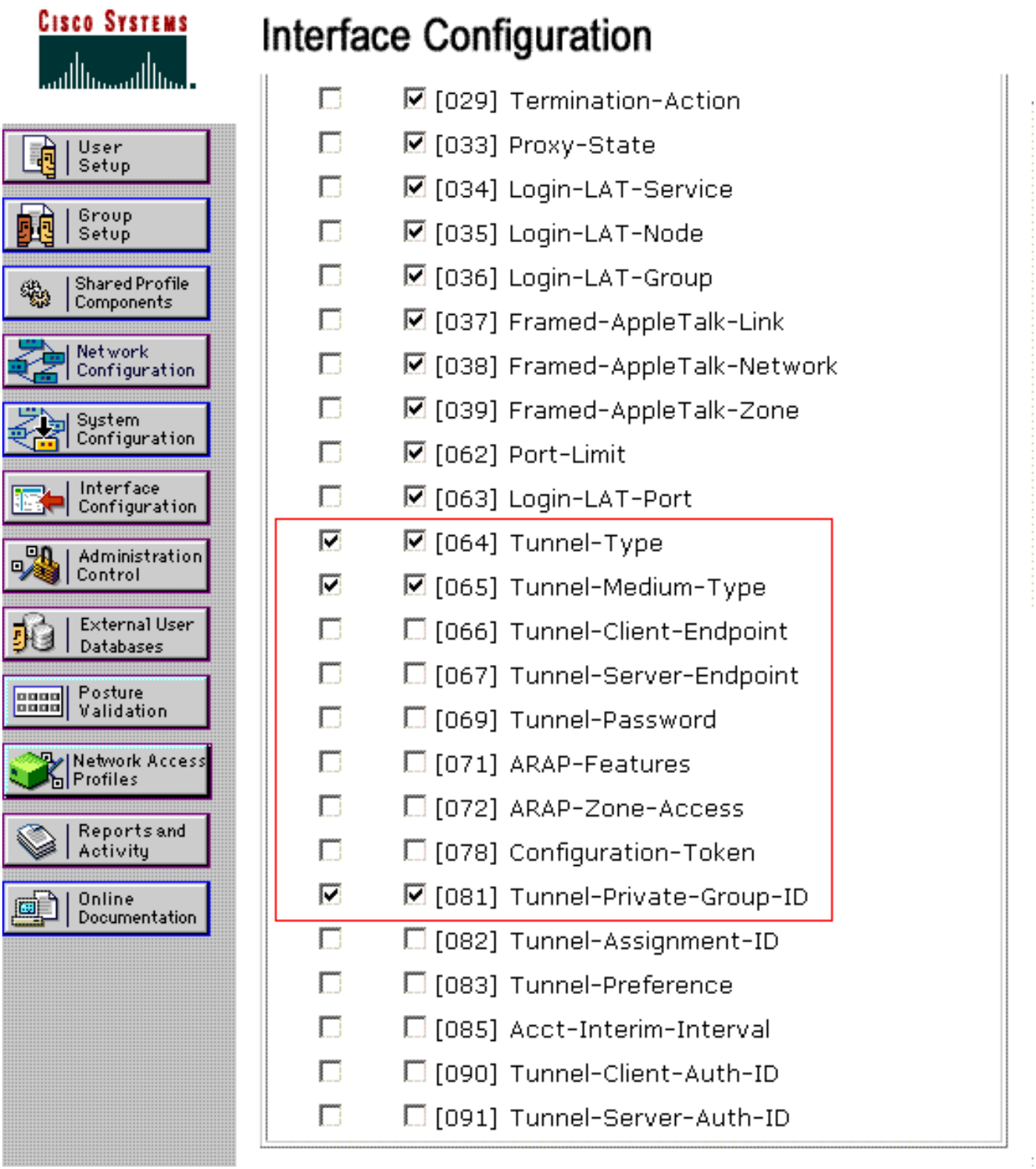


En este diagrama, note que la contraseña que usted proporciona conforme a la sección de configuración de usuario debe ser lo mismo que la que está proporcionada en el lado del cliente durante la autenticación de usuario.

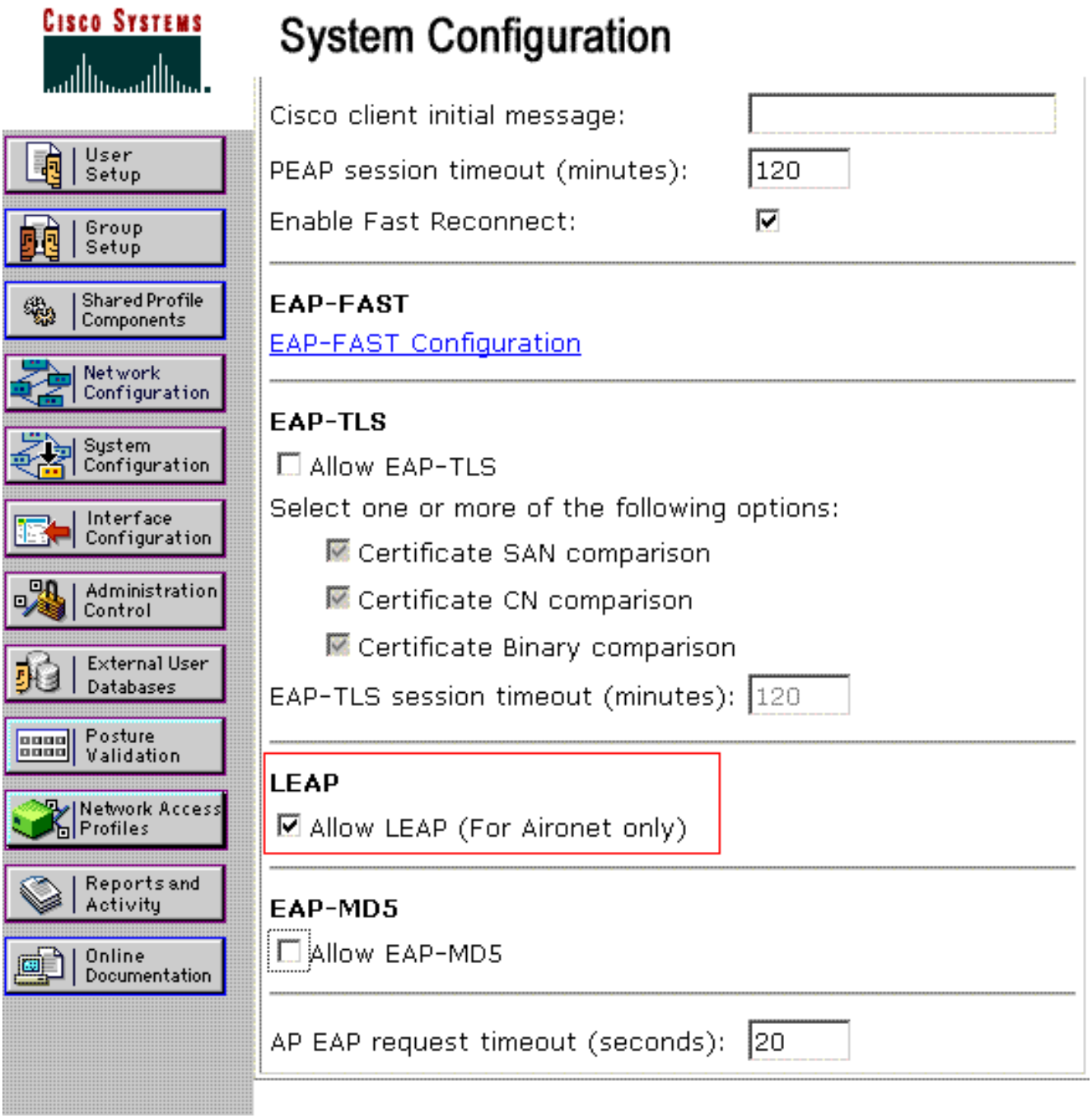
4. Navegue hacia abajo la página del editar y encuentre el campo de los **atributos IETF RADIUS**.
5. En los atributos IETF RADIUS coloque, marque las casillas de verificación al lado de los tres atributos del túnel y configure los valores de atributo como se muestra aquí:



Nota: En la configuración inicial del servidor ACS, los atributos IETF RADIUS no pudieron ser visualizados.Elija la **configuración de la interfaz > RADIUS (IETF)** para habilitar los atributos IETF en la ventana de la configuración de usuario.Entonces, marque las casillas de verificación para los atributos **64, 65, y 81** en las columnas del usuario y del grupo.



Nota: Para que al servidor de RADIUS asigne dinámicamente al cliente a un VLA N específico, **requieren que el VLAN-ID configurado bajo campo IETF 81 (Túnel-Soldado-Grupo-ID) del servidor de RADIUS existe en el WLC.**Marque **por la** casilla de verificación del atributo del **usuario TACACS+/RADIUS** debajo Interface Configuration > Advanced Options para habilitar al servidor de RADIUS para por las configuraciones de usuario.También, porque el SALTO se utiliza como el protocolo de autenticación, asegúrese de que el SALTO esté habilitado en la ventana de la configuración del sistema del servidor de RADIUS como se muestra
aquí:



Configure el ACS con los atributos del Airespace VSA de Cisco para la asignación del VLAN dinámico

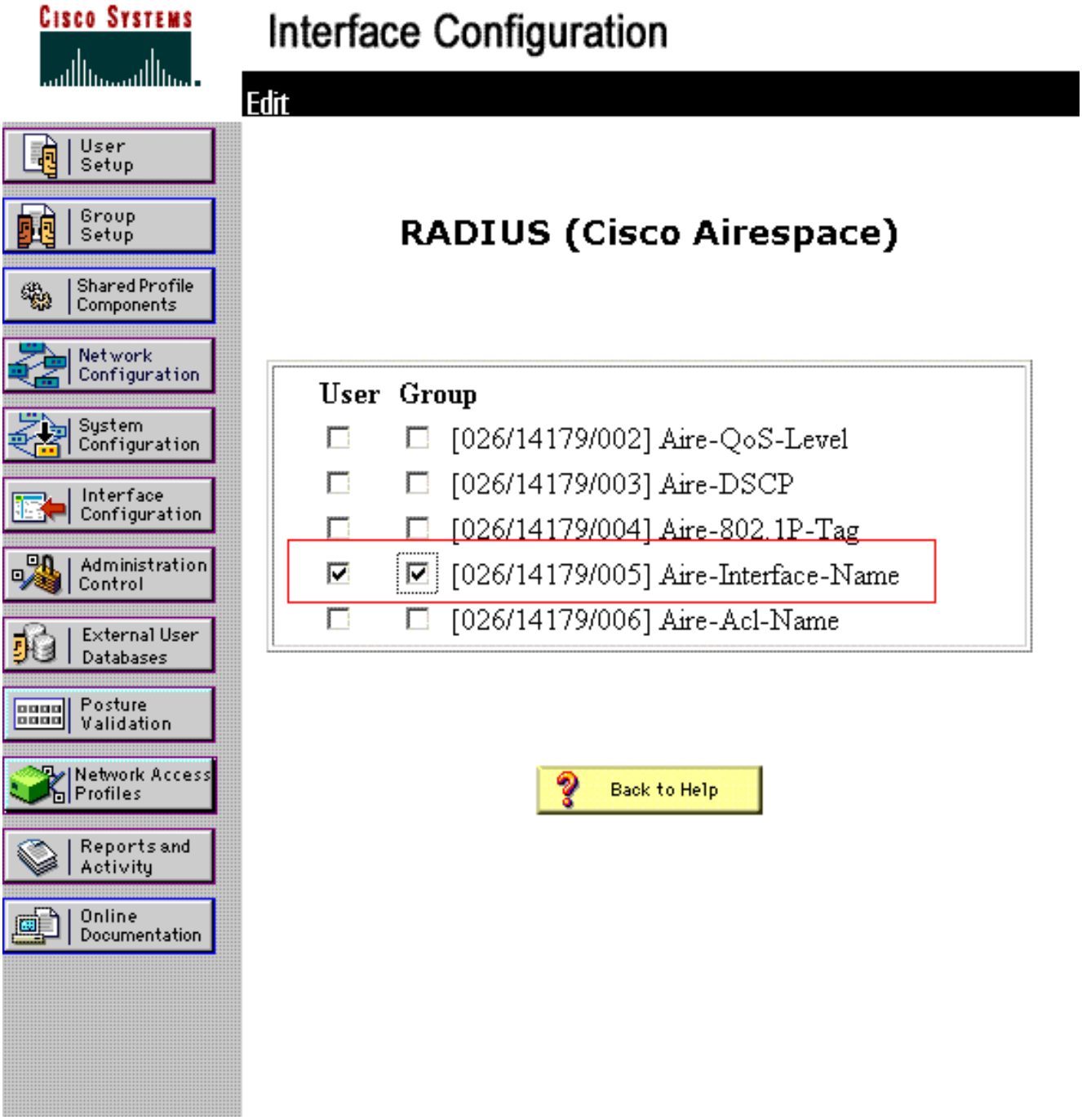
En los últimos ACS versión, usted puede también configurar el [VSA (Vendor-Specific)] del Airespace de Cisco atributo para asignar con éxito a un usuario autenticado con un nombre de la interfaz VLAN (no el VLAN ID) según la configuración de usuario en el ACS. Para lograr esto, realice los pasos en esta sección.

Nota: Esta sección utiliza la versión ACS 4.1 para configurar el atributo del Airespace VSA de Cisco.

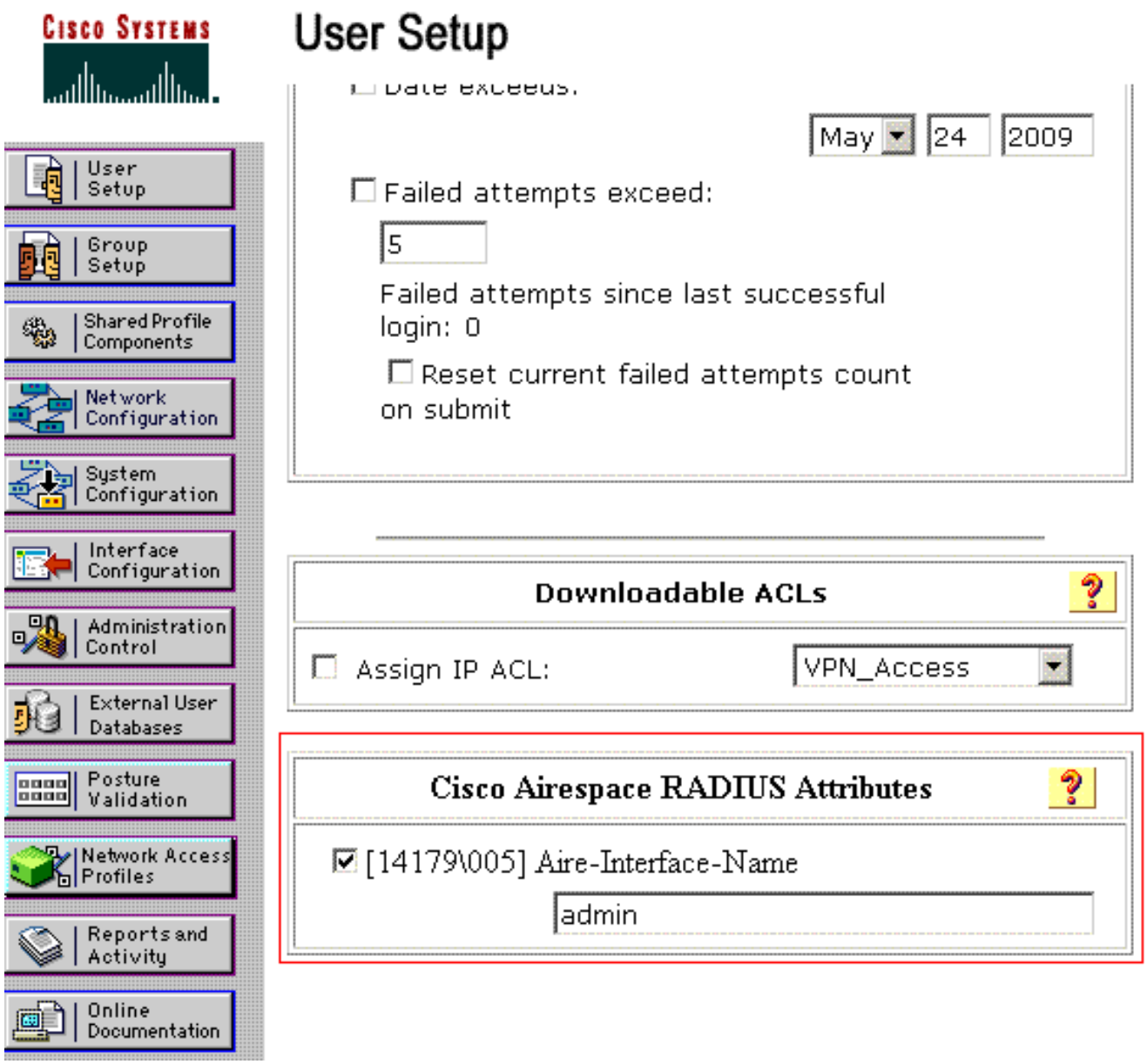
Configure al grupo ACS con la opción del atributo del Airespace VSA de Cisco

Complete estos pasos:

1. Del ACS 4.1 GUI, haga clic la **configuración de la interfaz de la** barra de navegación. Entonces, **RADIUS** selecto **(Airespace de Cisco) de la** página de la configuración de la interfaz para configurar la opción del atributo del Airespace de Cisco.
2. De la ventana RADIUS (Airespace de Cisco), marque la casilla de verificación del usuario (cuadro de casilla del grupo si es necesario) al lado del **aire - el interface name** para visualizarlo en el usuario edita la página. Entonces, el tecleo **somete**.



3. Vaya al user1 editan la página.
4. Del usuario edite la página, navegan hacia abajo a los **atributos de RADIUS del Airespace de Cisco la** sección. Marque la casilla de verificación al lado del **aire -** atributo de **interface name** y especifique el nombre de la interfaz dinámica que se asignará sobre la autenticación de usuario acertada.Este ejemplo asigna al usuario al VLA N **admin**.



5. Haga clic en Submit (Enviar).

Configure el Switch para los VLAN múltiples

Para permitir los VLAN múltiples a través del Switch, usted necesita publicar estos comandos de configurar el puerto del switch conectado con el regulador:

1. Conmute al **modo troncal del** #switchport (del config-if)
2. Conmute el **dot1q de la encapsulación del tronco del** #switchport (del config-if)

Nota: Por abandono, la mayor parte del Switches permite todos los VLA N creados en ese Switch vía el puerto troncal.

Estos comandos varían para un Switch del Catalyst Operating System (CatOS).

Si una red alámbrica está conectada con el Switch, después esta misma configuración se puede aplicar al puerto del switch que conecta con la red alámbrica. Esto habilita la comunicación entre los mismos VLA N en haber atado con alambre y la red inalámbrica.

Nota: Este documento no discute entre VLAN la comunicación. Esto está fuera del alcance de este documento. Usted debe entender que para el Routing entre VLAN, un switch de la capa 3 o

un router externo con el VLA N y las configuraciones de conexión de troncal apropiados es necesario. Hay varios documentos que explican la configuración del Routing entre VLAN.

Configuración del WLC

La configuración requiere estos pasos:

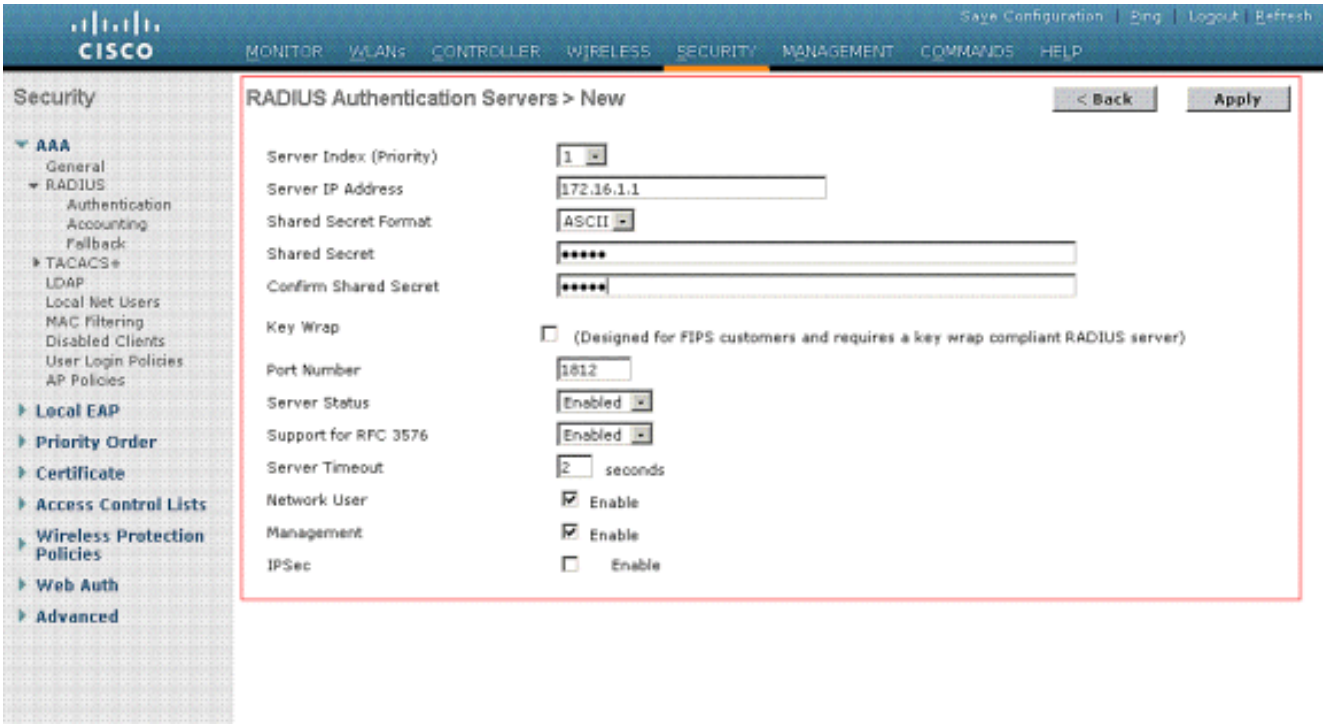
- Configure el WLC con los detalles del servidor de autenticación
- Configure las interfaces dinámicas (los VLA N)
- Configure los WLAN (el SSID)

Configure el WLC con los detalles del servidor de autenticación

Es necesario configurar el WLC así que puede comunicar con el servidor de RADIUS para autenticar a los clientes, y también para cualquier otra transacción.

Complete estos pasos:

1. Del regulador GUI, haga clic la **Seguridad**.
2. Ingrese el IP Address del servidor de RADIUS y de la clave secreta compartida usados entre el servidor de RADIUS y el WLC.Esta clave secreta compartida debe ser lo mismo que la que está configurada en el servidor de RADIUS bajo entrada de los clientes AAA de la Configuración de la red > Add. Aquí está una ventana de muestra del WLC:



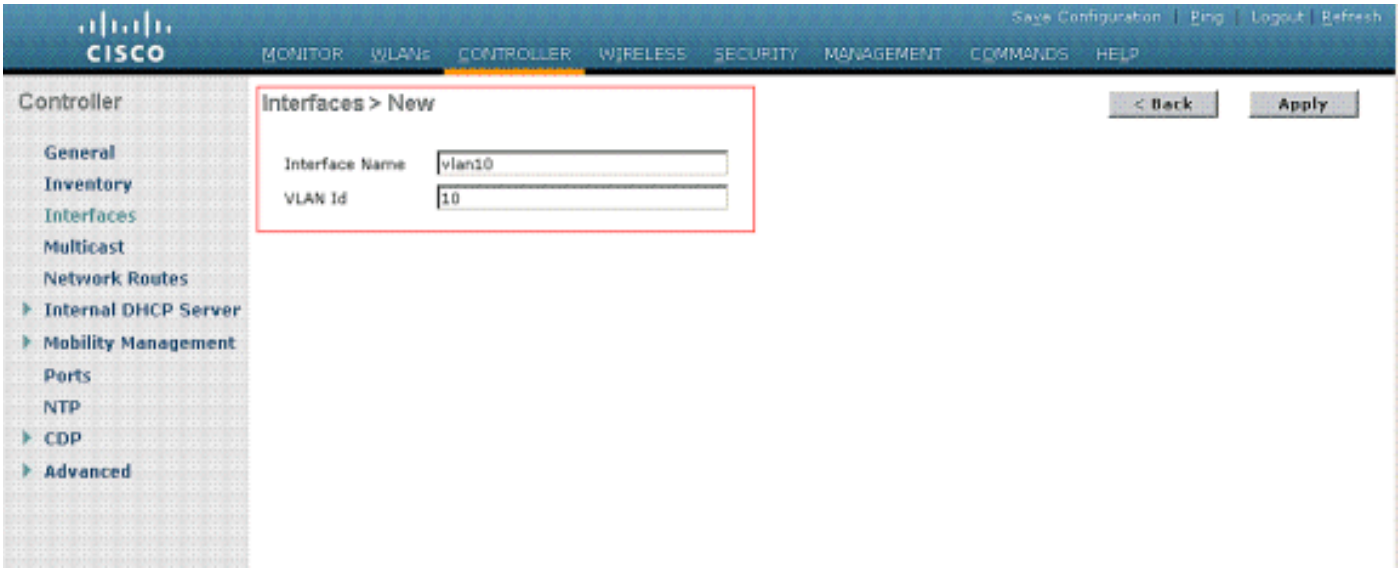
Configure las interfaces dinámicas (los VLA N)

Este procedimiento explica cómo configurar las interfaces dinámicas en el WLC. Según lo explicado anterior en este documento, el VLAN ID especificado bajo atributo del Túnel-Soldado-grupo ID del servidor de RADIUS debe también existir en el WLC.

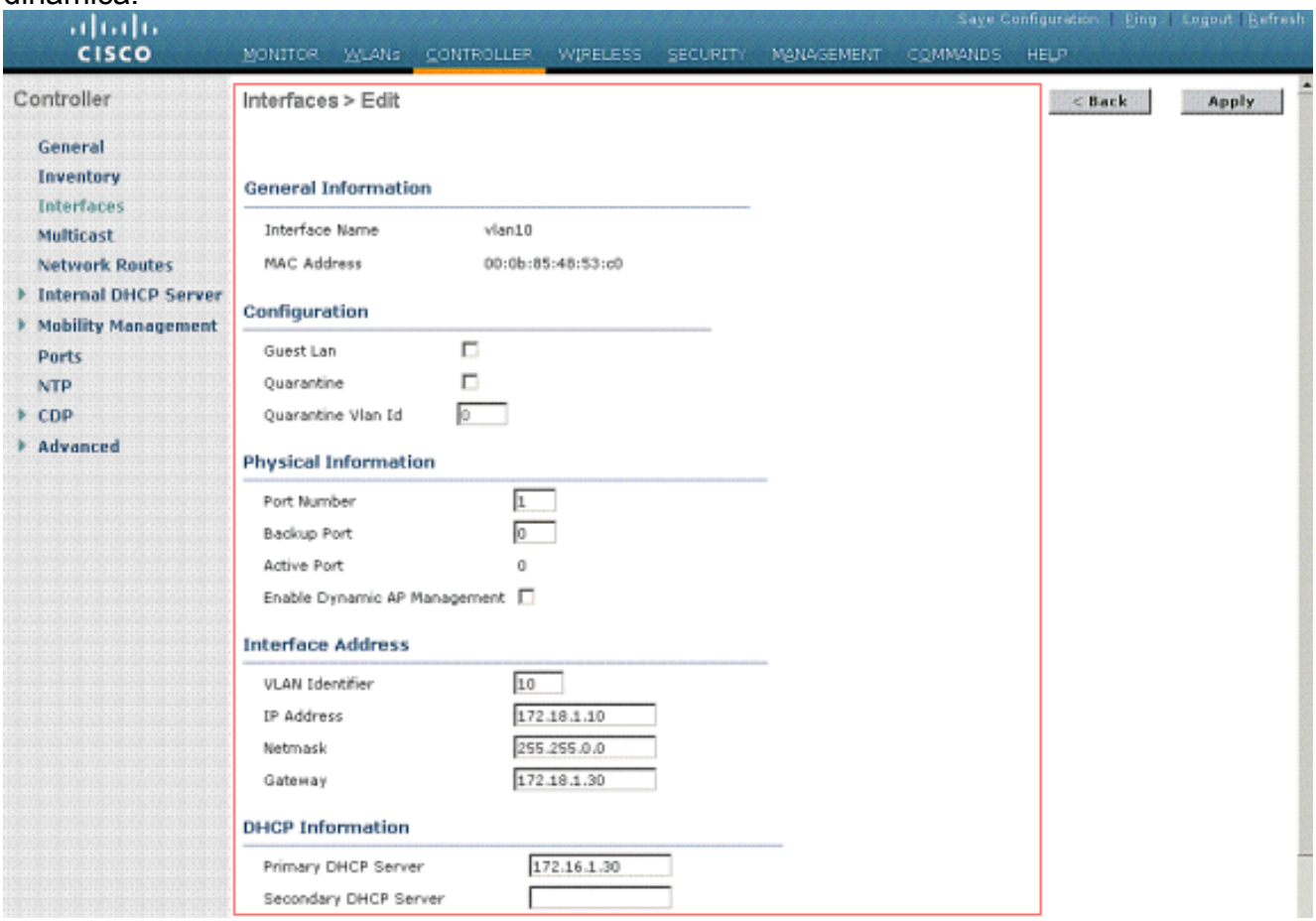
En el ejemplo, el user1 se especifica con el Túnel-Soldado-**grupo ID de 10 (VLAN=10)** en el

servidor de RADIUS. Vea la sección de los atributos IETF RADIUS de la ventana de la configuración de usuario del user1.

Usted puede ver la misma interfaz dinámica (VLAN=10) configurada en el WLC en este ejemplo. Del regulador GUI, bajo la ventana del regulador > de las interfaces, se configura la interfaz dinámica.



1. El tecleo **se aplica** en esta ventana.Esto le lleva a la ventana del editar de esta interfaz dinámica (VLAN10 aquí).
2. Ingrese el IP Address y el default gateway de esta interfaz dinámica.



Nota: Porque este documento utiliza a un servidor DHCP interno en el regulador, el campo primario de las puntas de esta ventana a la interfaz de administración del WLC sí mismo del

servidor DHCP. Usted puede también utilizar un servidor DHCP externo, un router, o al servidor de RADIUS sí mismo como servidor DHCP a los clientes de red inalámbrica. En estos casos, el campo primario del servidor DHCP señala a la dirección IP de ese dispositivo usado como el servidor DHCP. Refiera a su documentación del servidor DHCP para más información.

3. Haga clic en Apply (Aplicar).Ahora le configuran con una interfaz dinámica en su WLC. Semejantemente, usted puede configurar varias interfaces dinámicas en su WLC. Sin embargo, recuerde que el mismo VLAN ID debe también existir en el servidor de RADIUS para que ese VLAN determinado sea asignado al cliente.

Configure los WLAN (el SSID)

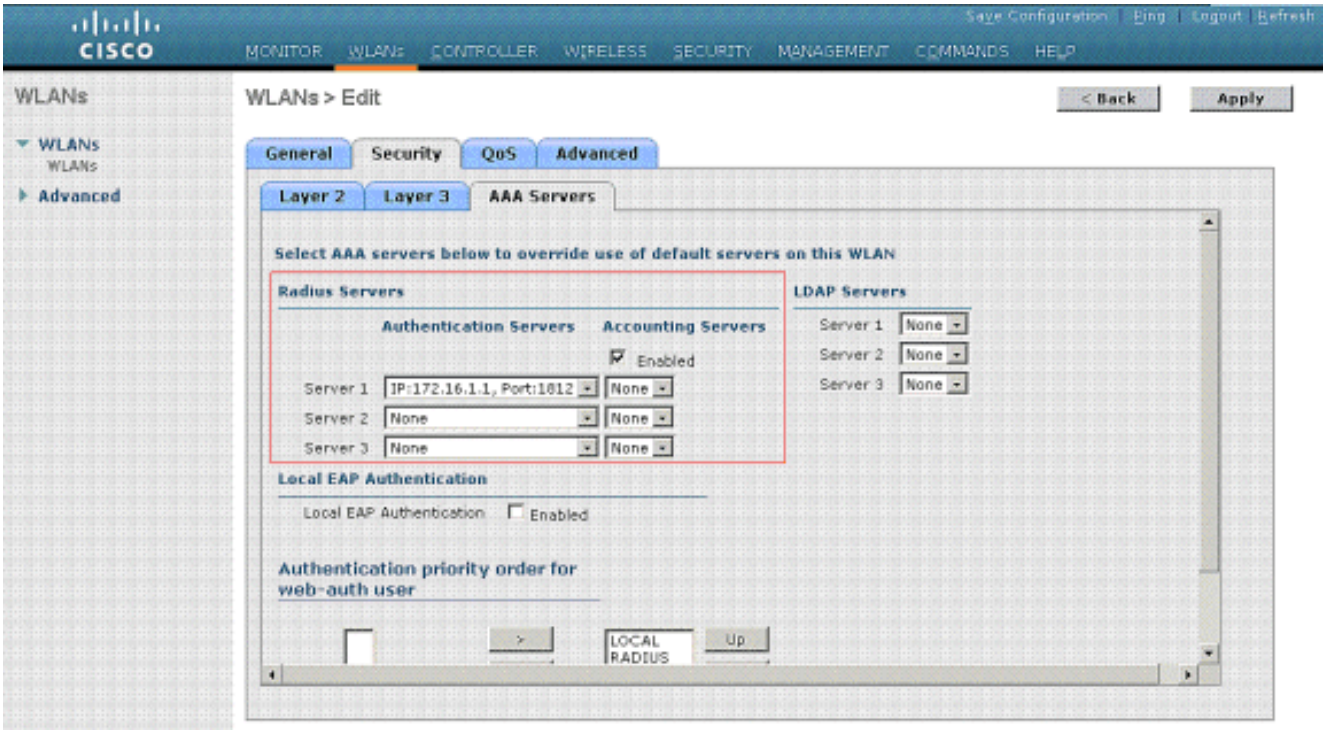
Este procedimiento explica cómo configurar los WLAN en el WLC.

Complete estos pasos:

1. Del regulador GUI, elija los **WLAN > nuevo** para crear una nueva red inalámbrica (WLAN).Se visualiza la nueva ventana del WLAN.
2. Ingrese la información del ID DE WLAN y WLAN SSID.Usted puede ingresar cualquier nombre para ser el WLAN SSID. Este ejemplo utiliza el VLAN10 como la red inalámbrica (WLAN)
SSID.

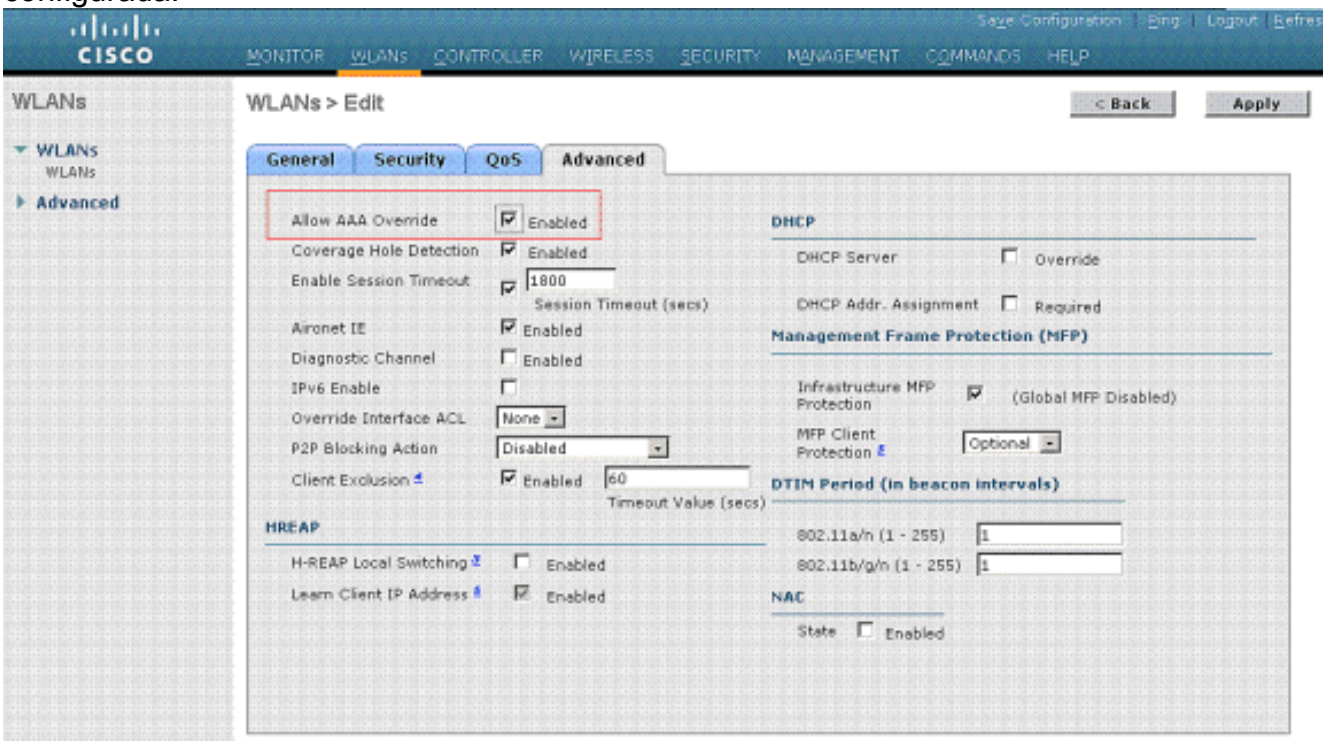
3. El tecleo **se aplica** para ir a la ventana del editar de la red inalámbrica (WLAN) SSID10.

Normalmente, en un regulador del Wireless LAN, cada red inalámbrica (WLAN) se asocia a un VLA N específico (SSID) para poner un usuario determinado que pertenezca a esa red inalámbrica (WLAN) en el VLA N específico asociado. Esta asignación se hace normalmente bajo campo de nombre de la interfaz de la ventana SSID de la red inalámbrica (WLAN).



En el ejemplo proporcionado, es el trabajo del servidor de RADIUS asignar a un cliente de red inalámbrica a un VLA N específico sobre la autenticación satisfactoria. Los WLAN no necesitan ser asociados a una interfaz dinámica específica en el WLC. O, aunque la red inalámbrica (WLAN) a la asignación de la interfaz dinámica se hace en el WLC, el servidor de RADIUS reemplaza esta asignación y asigna al usuario que viene con esa red inalámbrica (WLAN) al VLA N especificado bajo campo del usuario Túnel-Grupo-Soldado-**ID** en el servidor de RADIUS.

4. Marque la casilla de verificación de la **invalidación de la permit AAA** para reemplazar las configuraciones del WLC del servidor de RADIUS.
5. Habilite la invalidación de la permit AAA en el regulador para cada red inalámbrica (WLAN) (SSID)
configurada.



Cuando se habilita la invalidación AAA, y un cliente tiene el AAA y parámetros de

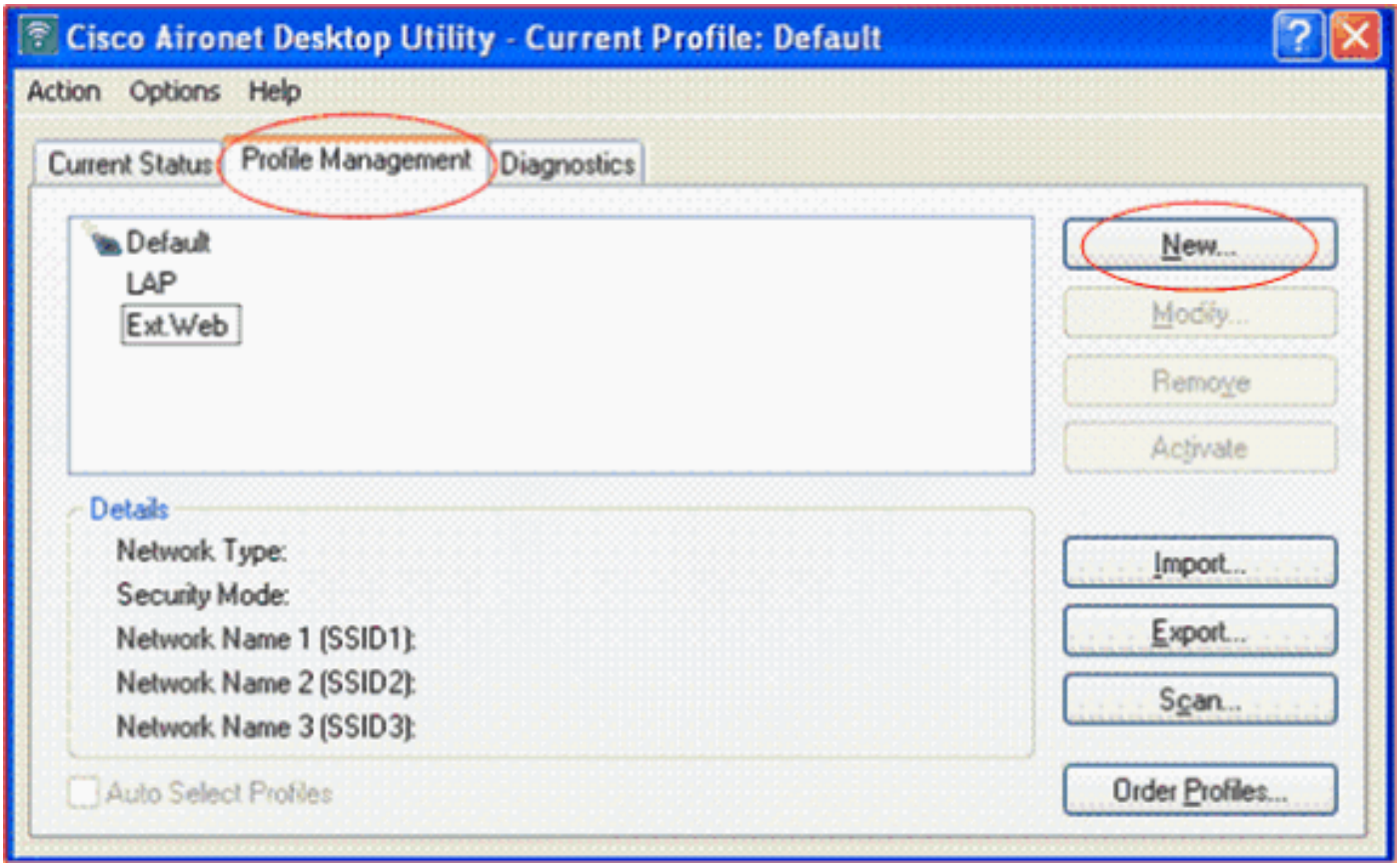
autenticación de la red inalámbrica (WLAN) del regulador que están en conflicto, la autenticación de cliente es realizada por el servidor AAA (RADIUS). Como parte de esta autenticación, el sistema operativo mueve a los clientes a un VLA N vuelto por el servidor de AAA. Esto se predefine en la configuración de la interfaz del regulador.Por ejemplo, si la red inalámbrica (WLAN) corporativa utiliza sobre todo una interfaz de administración asignada al VLAN2, y si la invalidación AAA vuelve una reorientación al VLAN 100, el sistema operativo reorienta todas las transmisiones del cliente al VLAN 100 incluso si el puerto físico al cual se asigna el VLAN 100. Cuando se inhabilita la invalidación AAA, toda la autenticación de cliente omite las configuraciones del parámetro de autenticación del regulador, y la autenticación es realizada solamente por el servidor de AAA si la red inalámbrica (WLAN) del regulador no contiene ninguna parámetros de autenticación cliente-específica.

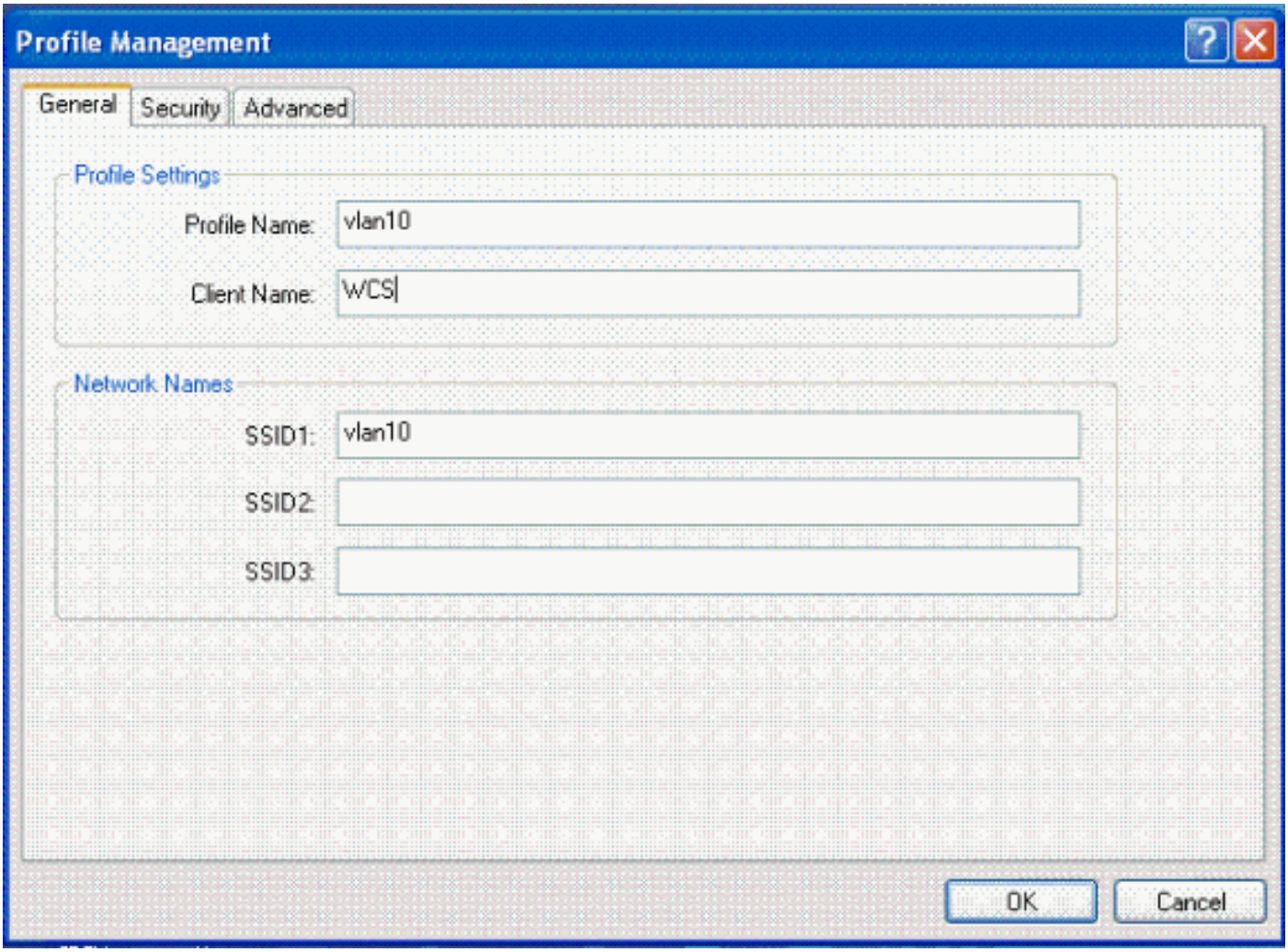
Configuración de utilidad del cliente de red inalámbrica

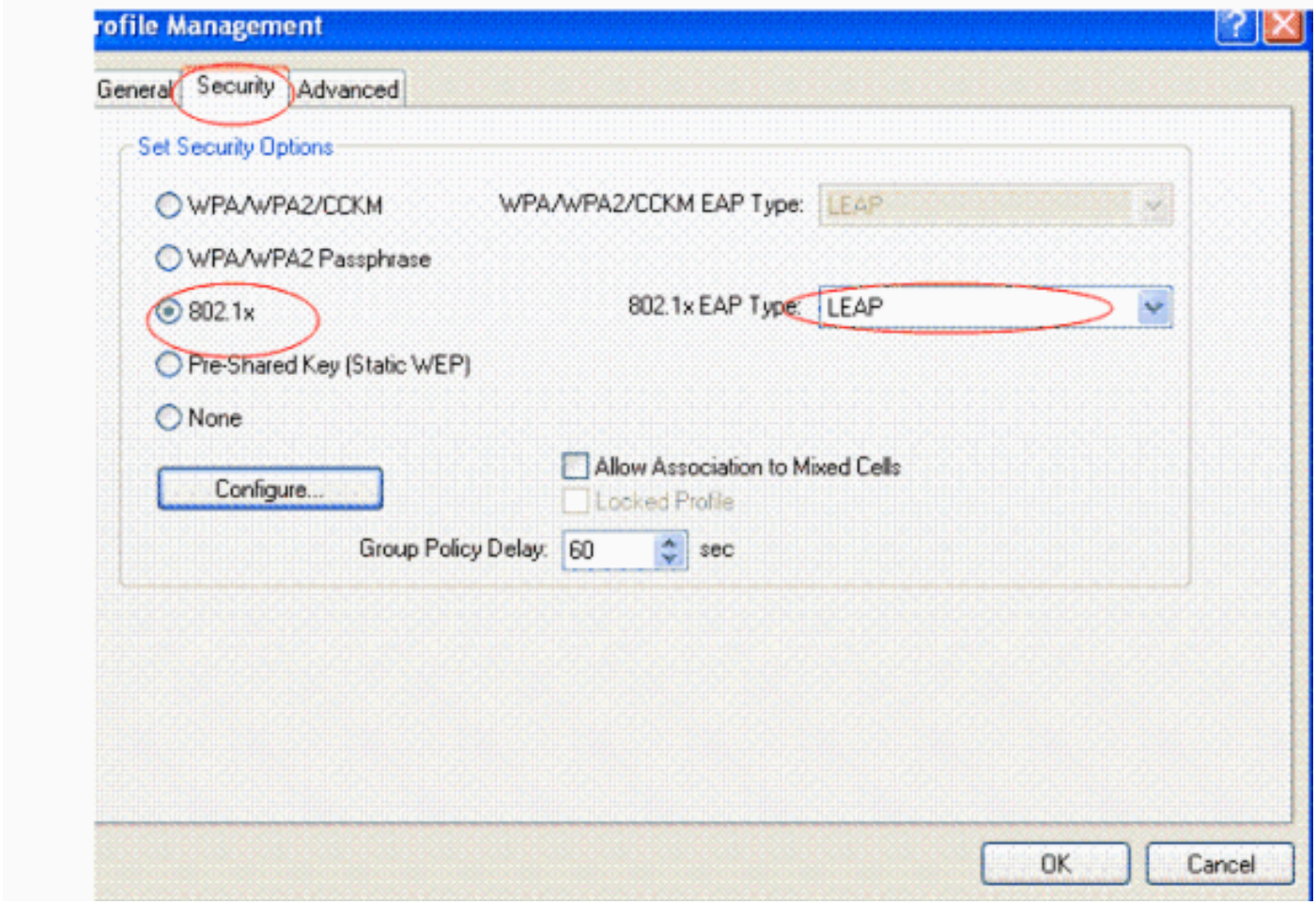
Este documento utiliza el ADU como la utilidad de cliente para la configuración de los perfiles del usuario. Esta configuración también utiliza el SALTO como el protocolo de autenticación. Configure el ADU tal y como se muestra en del ejemplo en esta sección.

De la barra de menú ADU, elija la **Administración del perfil > nuevo** para crear un nuevo perfil.

Configuran al cliente del ejemplo para ser una parte de SSID VLAN10. Estos diagramas muestran cómo configurar un perfil del usuario en un cliente:




Profile Management
General
Security
Advanced
Profile Settings
Profile Name:
vlan10
Client Name:
WCS
Network Names
SSID1:
vlan10
SSID2:
SSID3:
OK
Cancel


rofile Management
General
Security
Advanced
Set Security Options
WPA/WPA2/CCKM
WPA/WPA2/CCKM EAP Type:
LEAP
WPA/WPA2 Passphrase
802.1x
802.1x EAP Type:
LEAP
Pre-Shared Key (Static WEP)
None
Configure...
Allow Association to Mixed Cells
Locked Profile
Group Policy Delay:
60
sec
OK
Cancel

Verificación

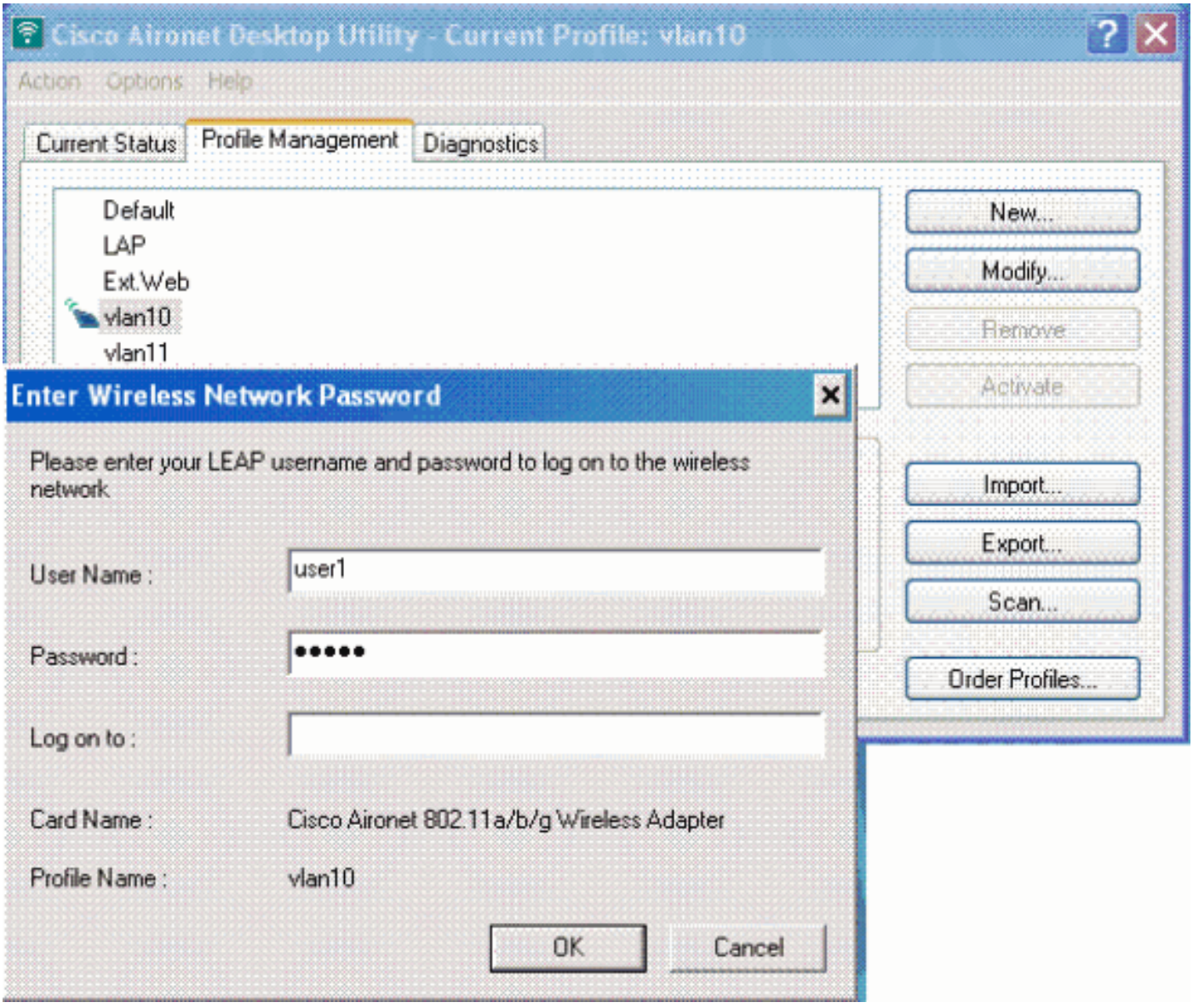
Active el perfil del usuario que usted ha configurado en el ADU. De acuerdo con la configuración, le indican para un nombre de usuario y contraseña. Usted puede también dar instrucciones el ADU para utilizar el nombre de usuario de Windows y la contraseña para autenticación. Hay varias opciones de las cuales el cliente puede recibir la autenticación. Usted puede configurar estas opciones bajo lengueta del Security (Seguridad) > Configure (Configurar) del perfil del usuario que usted ha creado.

En el ejemplo anterior, note que el user1 está asignado al VLAN10 como se especifica en el servidor de RADIUS.

Este ejemplo utiliza este nombre de usuario y contraseña del lado del cliente para recibir la autenticación y para ser asignado a un VLA N por el servidor de RADIUS:

- Nombre de usuario = user1
- Contraseña = user1

Este ejemplo muestra cómo el SSID VLAN10 se indica para el nombre de usuario y contraseña. El nombre de usuario y contraseña se ingresa en este ejemplo:

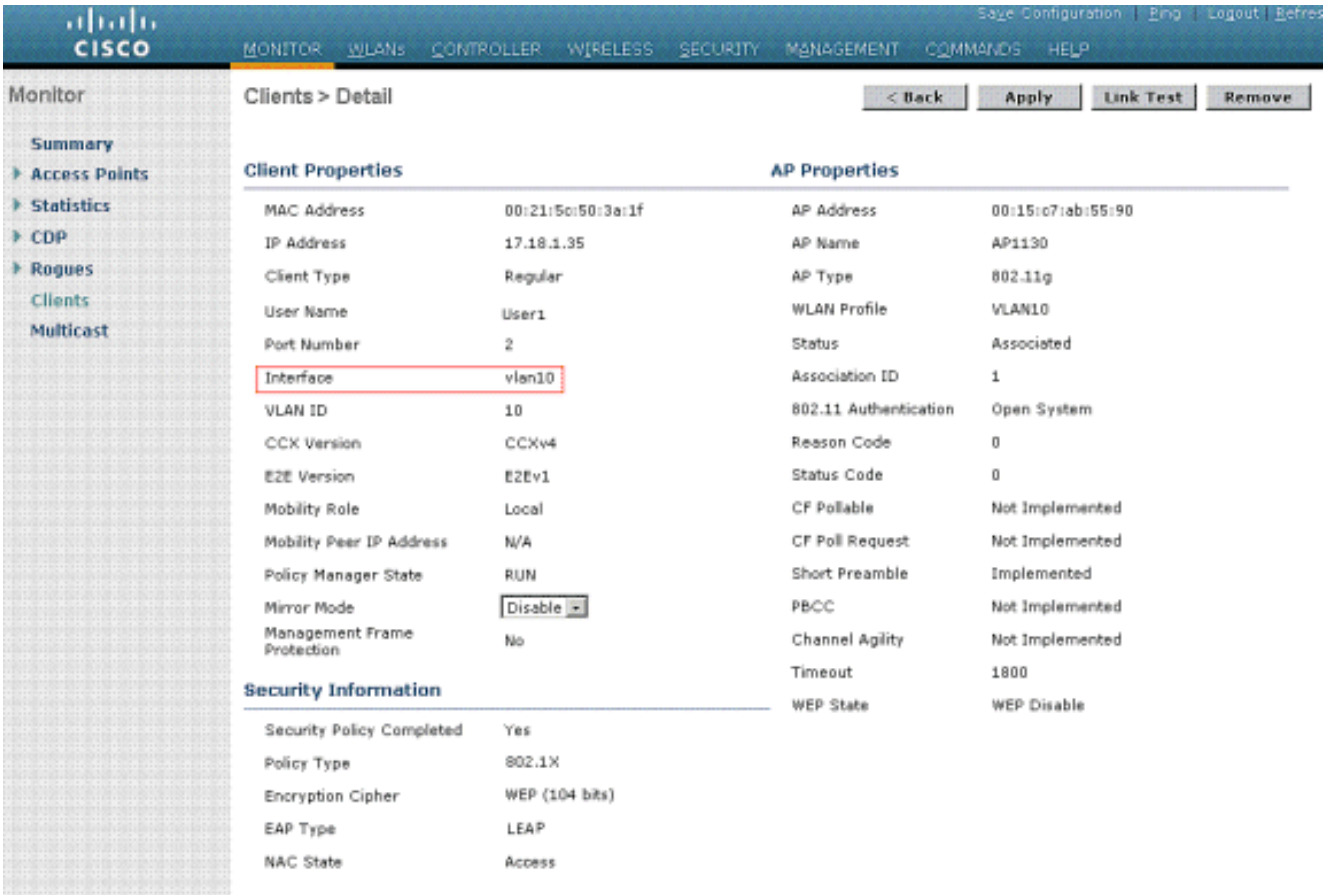


Una vez la autenticación y la validación correspondiente es acertadas, usted reciben el éxito como el mensaje de estado.

Entonces, usted necesita verificar que asignen su cliente al VLA N apropiado según los atributos de RADIUS enviados. Complete estos pasos para lograr esto:

1. Del regulador GUI, elija la **Tecnología inalámbrica > el AP**.
2. Haga clic a los **clientes**, que aparece en la esquina izquierda de la ventana del (APS) de los Puntos de acceso.Se visualizan las estadísticas del cliente.

3. Haga clic los **detalles** para identificar a los detalles completos del cliente, tales como dirección IP, el VLA N al cual se asigna, y así sucesivamente.Este ejemplo visualiza a estos detalles del cliente, user1:



De esta ventana, usted puede observar que asignan este cliente al VLAN10 según los atributos de RADIUS configurados en el servidor de RADIUS.**Nota:** Si la asignación del VLAN dinámico se basa en la configuración del **atributo del Airespace VSA de Cisco**, el **nombre de la interfaz la visualizará pues admin** según este ejemplo en la página de los detalles del cliente.

Use esta sección para confirmar que su configuración funciona correctamente.

- **haga el debug del permiso de los eventos aaa** — Este comando se puede utilizar para asegurar la transferencia acertada de los atributos de RADIUS al cliente vía el regulador. Esta porción de la salida de los debugs asegura una transmisión exitosa de los atributos de RADIUS:`Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 processing avps[0]:`
`attribute 64, vendorId 0, valueLen 4`
`Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 processing avps[1]:`
`attribute 65, vendorId 0, valueLen 4`
`Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 processing avps[2]:`
`attribute 81, vendorId 0, valueLen 3`
`Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 processing avps[3]:`
`attribute 79, vendorId 0, valueLen 32`
`Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 Received EAP Attribute`
`(code=2, length=32,id=0) for mobile 00:40:96:ac:e6:57`
`Fri Jan 20 02:25:08 2006: 00000000: 02 00 00 20 11 01 00 18`
`4a 27 65 69 6d e4 05 f5`
`........J'eim...00000010: d0 98 0c cb 1a 0c 8a 3c`
`........44 a9 da 6c 36 94 0a f3  <D..l6...`
**`Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 processing avps[4]: attribute 1, vendorId 9, valueLen 16 Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 processing avps[5]: attribute 25, vendorId 0, valueLen 28 Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 processing avps[6]: attribute 80, vendorId 0, valueLen 16 Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 Tunnel-Type 16777229 should be 13 for STA 00:40:96:ac:e6:57 Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 Tunnel-Medium-Type 16777222 should be 6 for STA 00:40:96:ac:e6:57`** `Fri Jan 20 02:30:00 2006: 00:40:96:ac:e6:57 Station 00:40:96:ac:e6:57 setting dot1x reauth timeout = 1800`
- Estos comandos pueden también ser útiles:**permiso aaa del dot1x del debugpermiso de los paquetes aaa del debug**

Troubleshooting

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Nota: La asignación del VLAN dinámico no trabaja para la autenticación Web de un WLC.

Información Relacionada

- Autenticación EAP con el servidor de RADIUS
- Cisco LEAP
- Guía de configuración del Controlador de LAN de la Red Inalámbrica Cisco, versión 4.0
- Soporte Técnico y Documentación - Cisco Systems