Asignación del VLAN dinámico con el ejemplo de configuración NGWC y ACS 5.2

Contenido

Introducción

Este documento describe el concepto de asignación del VLAN dinámico. También describe cómo configurar el regulador del Wireless LAN (WLC) y a un servidor de RADIUS para asignar a los clientes del Wireless LAN (red inalámbrica (WLAN)) a un VLA N específico dinámicamente. En este documento, el servidor de RADIUS es un Access Control Server (ACS) esa versión 5.2 del Cisco Secure Access Control System de los funcionamientos.

Prerequisites

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimiento básico del WLC y de los Puntos de acceso ligeros (revestimientos)

- Conocimiento funcional del servidor del Authentication, Authorization, and Accounting (AAA)
- Conocimiento completo de las redes inalámbricas y de los problemas de seguridad inalámbrica

Componentes Utilizados

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

- Regulador del Wireless LAN de Cisco 5760 con la versión de software 3.2.2 (Wiring Closet del ® XE del Cisco IOS de la última generación, o NGWC)
- Lightweight Access Point de las 3602 Series del Cisco Aironet
- Microsoft Windows XP con el supplicant de Intel Proset
- Versión 5.2 del Cisco Secure Access Control System
- Cisco Catalyst 3560 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.

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, los atributos del VLA N, y/o las políticas de seguridad basadas en los credenciales 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 la asignación del usuario a un VLA N específico es manejada por un servidor de autenticación de RADIUS, tal como un Cisco Secure ACS. Esta característica 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.

Como consecuencia, 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 del cliente (la red inalámbrica (WLAN), en términos de WLC) 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 al VLA N.
- IETF 65 (tipo medio del túnel) - fije a 802.
- IETF 81 (Túnel-Soldado-Grupo-ID) - Fije 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 RFC 2868, los atributos de RADIUS para el soporte del Tunnel Protocol para el uso con el IEEE 802.1X, el valor del número entero VLAN ID se codifican 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 el campo de la etiqueta 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

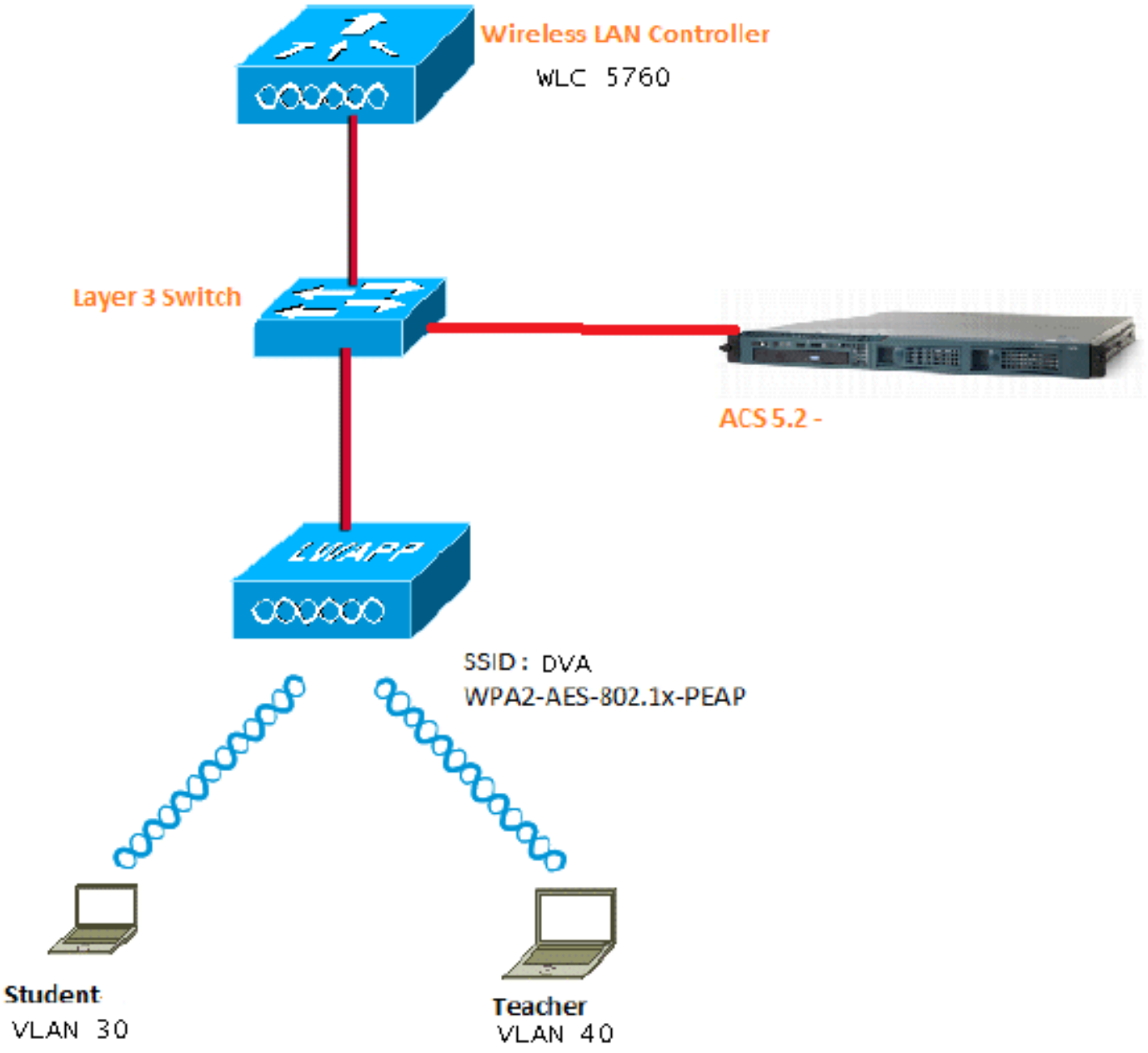
La configuración de una asignación del VLAN dinámico consiste en dos pasos claros:

1. Configure el WLC con el comando line interface(cli) o con el GUI.
2. Configure al servidor de RADIUS.

Note: Use la Command Lookup Tool (clientes registrados solamente) para obtener más información sobre los comandos usados en esta sección.

Diagrama de la red

En este documento, se utiliza esta configuración de red:



Este documento utiliza el 802.1x con el protocolo extensible authentication protegido (PEAP) como el mecanismo de seguridad.

Suposición

- El Switches se configura para todos los VLA N de la capa 3 (L3).
- Asignan el servidor DHCP un alcance de DHCP.
- La Conectividad L3 existe entre todos los dispositivos en la red.
- El REVESTIMIENTO se une a ya al WLC.
- Cada VLA N tiene una máscara de /24.
- El ACS 5.2 tiene un certificado autofirmado instalado.

WLC de la configuración con el CLI

red inalámbrica (WLAN) de la configuración

Éste es un ejemplo de cómo configurar una red inalámbrica (WLAN) con el SSID de DVA:

```
wlan DVA 3 DVA
 aaa-override
 client vlan VLAN0020
 security dot1x authentication-list ACS
 session-timeout 1800
 no shutdown
```

Servidor de RADIUS de la configuración en el WLC

Éste es un ejemplo de la configuración del servidor de RADIUS en el WLC:

```
aaa new-model
!
!
aaa group server radius ACS
 server name ACS
!
aaa authentication dot1x ACS group ACS

radius server ACS
 address ipv4 10.106.102.50 auth-port 1645 acct-port 1646
 key Cisco123

dot1x system-auth-control
```

Agrupamiento DHCP de la configuración para el VLA N del cliente

Éste es un ejemplo de la configuración del agrupamiento DHCP para el VLAN 30 y el VLA N 40 del cliente:

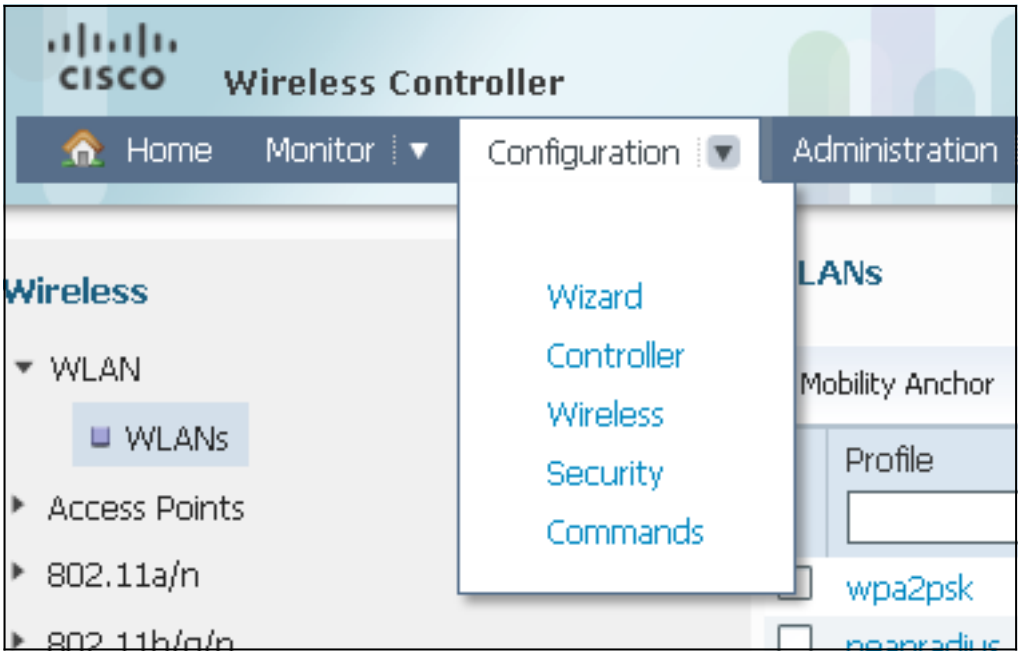
```
interface Vlan30
 ip address 30.30.30.1 255.255.255.0
!
interface Vlan40
 ip address 40.40.40.1 255.255.255.0

ip dhcp pool vla30
 network 30.30.30.0 255.255.255.0
 default-router 30.30.30.1
!
ip dhcp pool vlan40
 network 40.40.40.0 255.255.255.0
 default-router 40.40.40.1

ip dhcp snooping vlan 30,40
ip dhcp snooping
```

WLC de la configuración con el GUI

red inalámbrica (WLAN) de la configuración

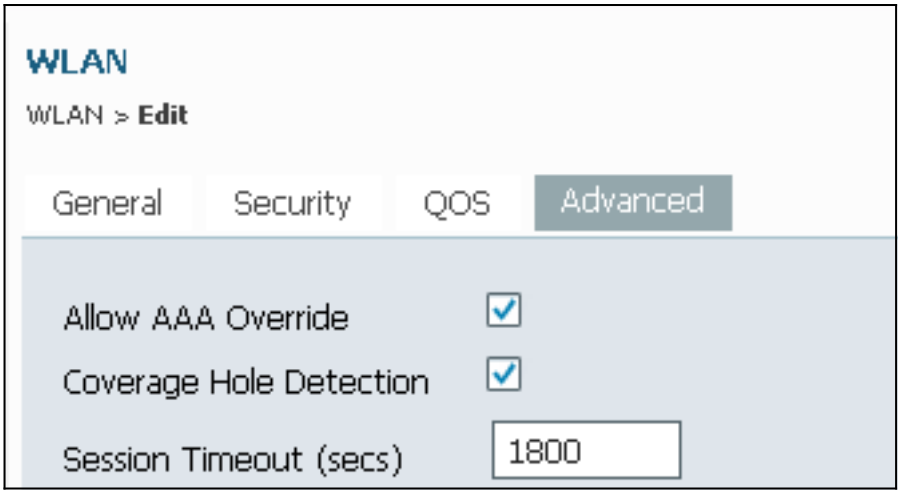
Este procedimiento describe cómo configurar la red inalámbrica (WLAN).

1. Navegue a la **configuración** > a la **Tecnología inalámbrica** > a la **red inalámbrica (WLAN)** > **NUEVA** lengueta.

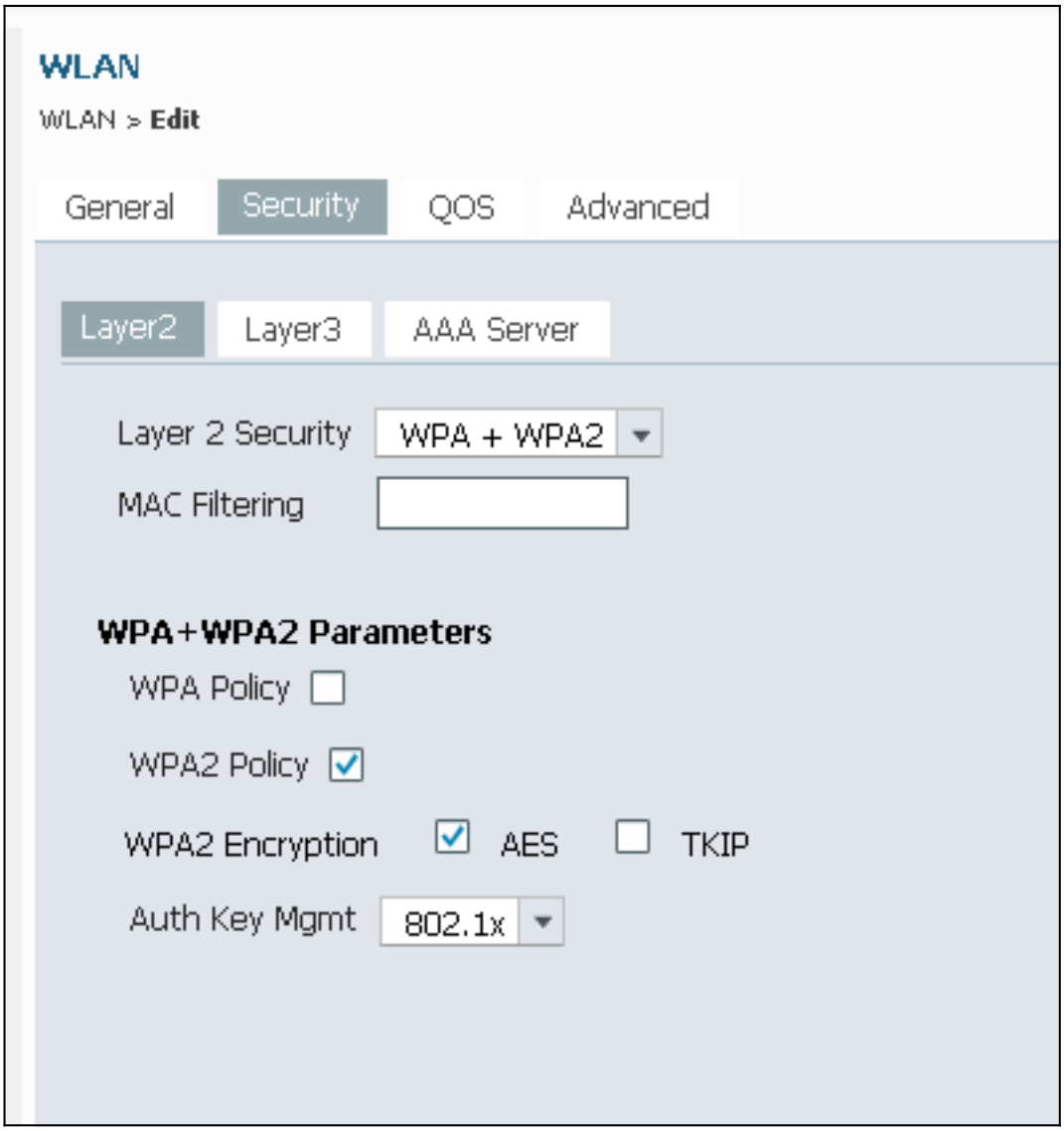


2. Haga clic la **ficha general** para ver que la red inalámbrica (WLAN) está configurada para WPA2-802.1X, y asociar la interfaz/el grupo de Interfrace (G) a VLAN20 (**VLAN0020**).

3. Haga clic la **ficha Avanzadas**, y marque la casilla de verificación de la **invalidación de la permit AAA**. La invalidación se debe habilitar para que esta característica trabaje.



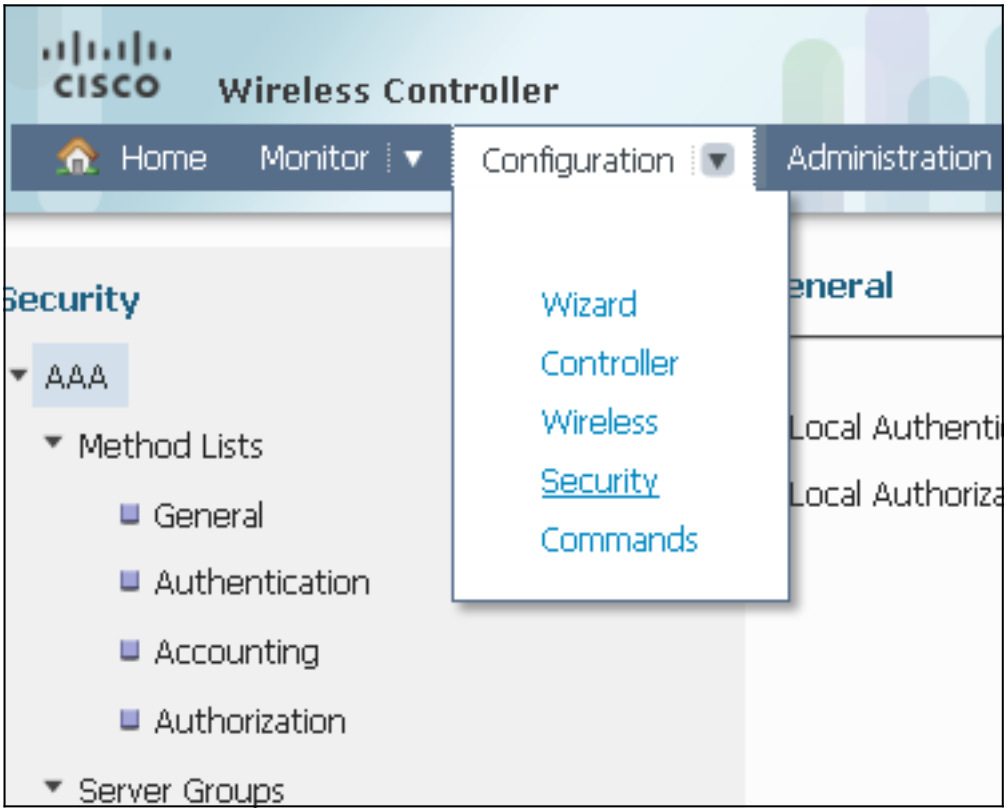
4. Haga clic la **ficha de seguridad** y la lengueta **Layer2**, marque WPA2 la casilla de verificación del cifrado **AES**, y seleccione el **802.1x de la** lista desplegable del mgmt de la clave del auth.



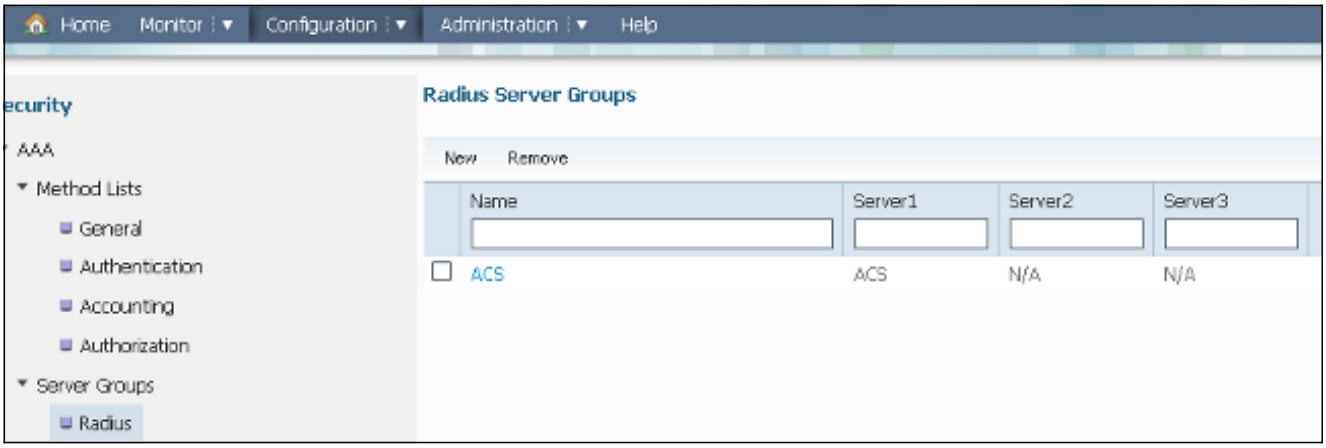
Configure al servidor de RADIUS en el WLC

Este procedimiento describe cómo configurar al servidor de RADIUS en el WLC.

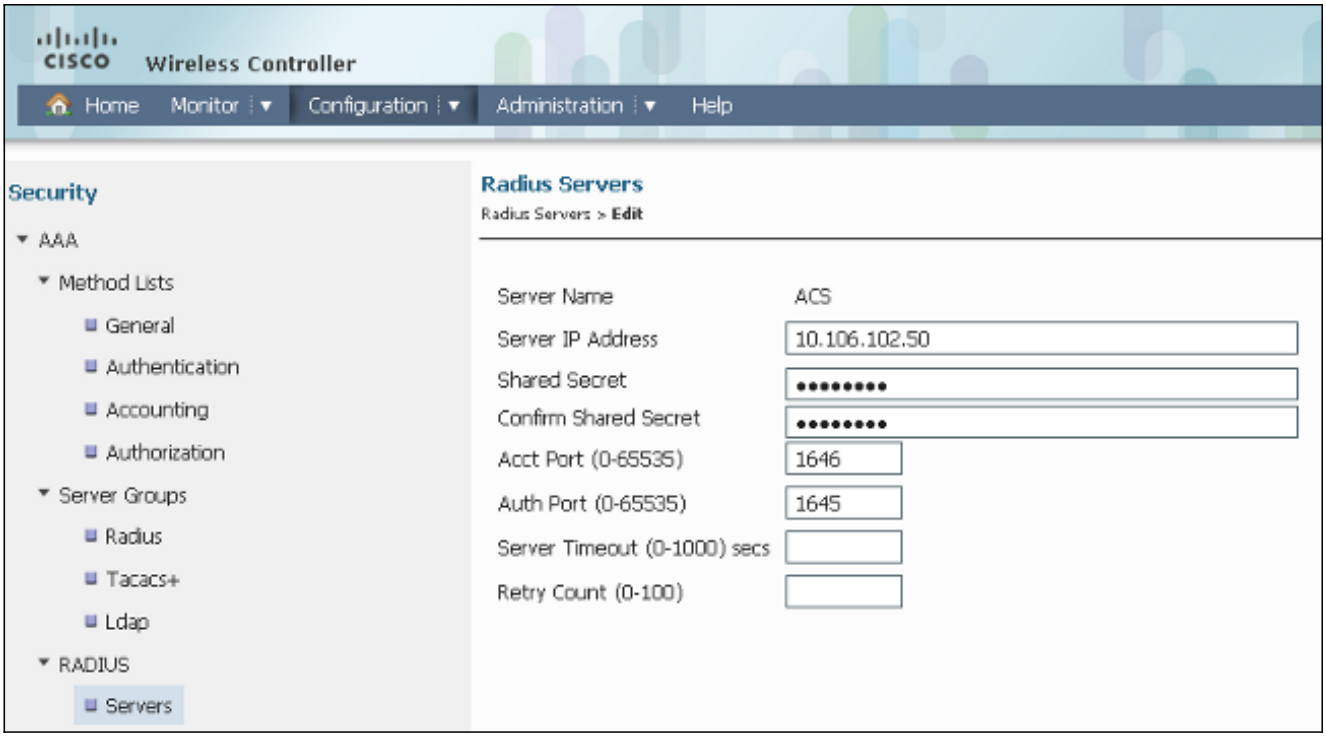
1. Navegue a la lengueta del > Security (Seguridad) de la **configuración**.



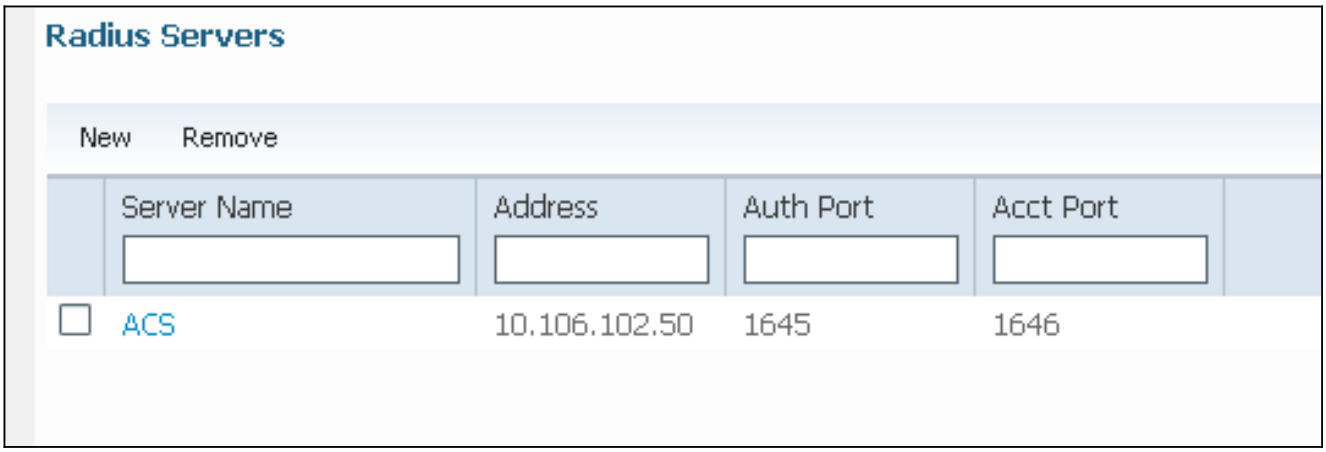
2. Navegue a **AAA** > los **grupos de servidores** > **radio** para crear a los grupos de servidor de RADIUS. En este ejemplo, llaman el grupo de servidor de RADIUS ACS.



3. Edite la entrada del servidor de RADIUS para agregar el dirección IP del servidor y el secreto compartido. Este secreto compartido debe hacer juego el secreto compartido en el WLC y el servidor de RADIUS.



Éste es un ejemplo de una configuración completa:

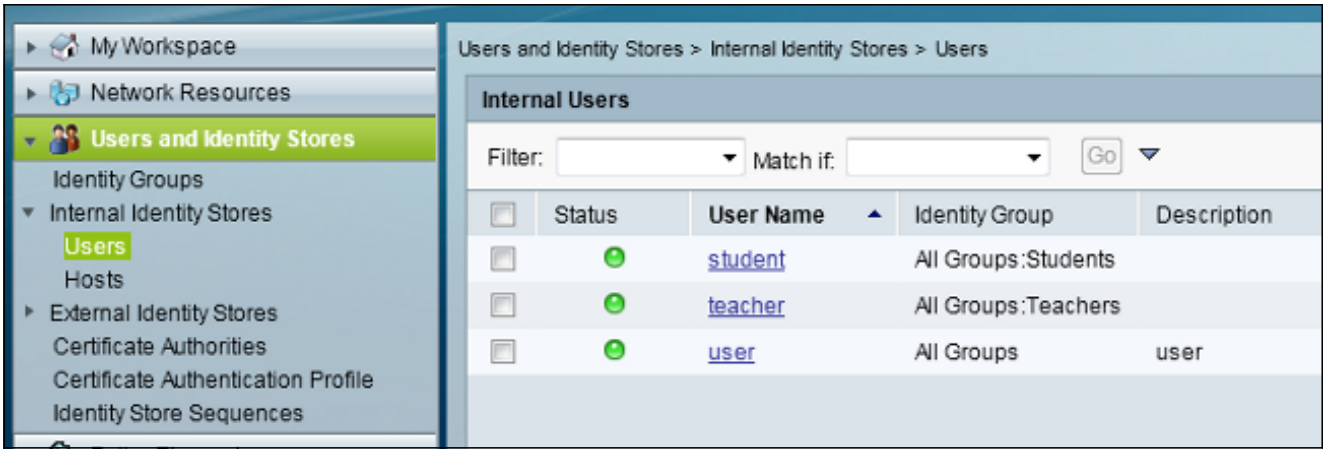


Servidor de RADIUS de la configuración

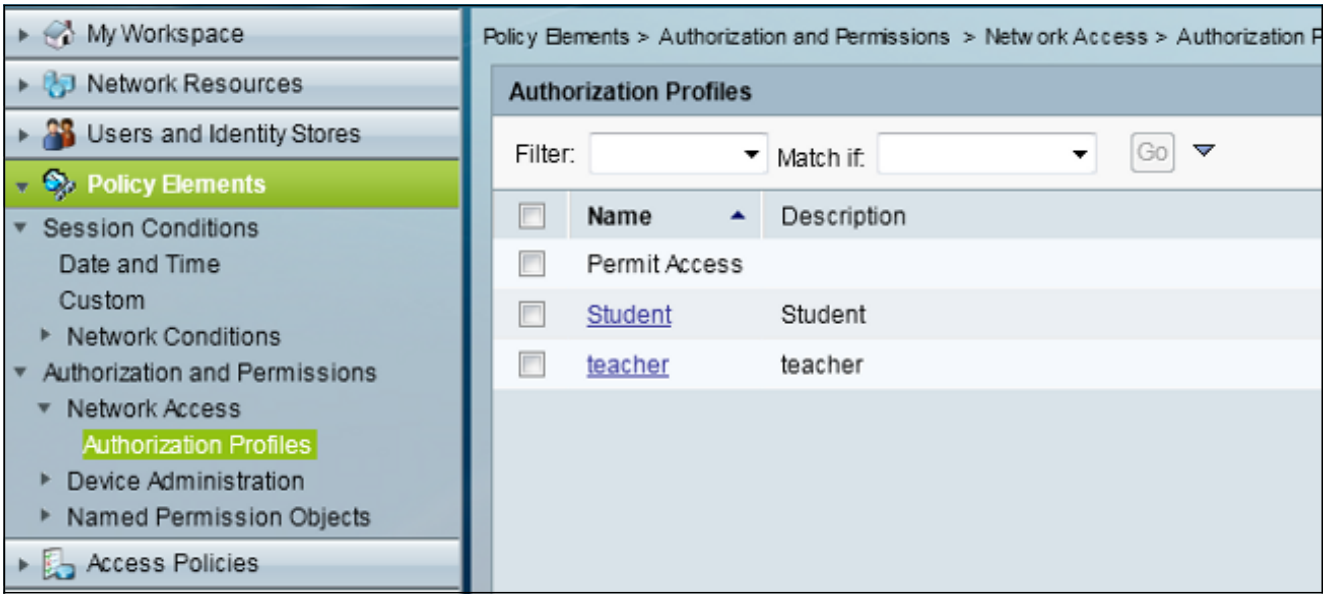
Este procedimiento describe cómo configurar al servidor de RADIUS.

1. En el servidor de RADIUS, navegue a los **usuarios y la identidad salva** > los **almacenes internos de la identidad** > Users.

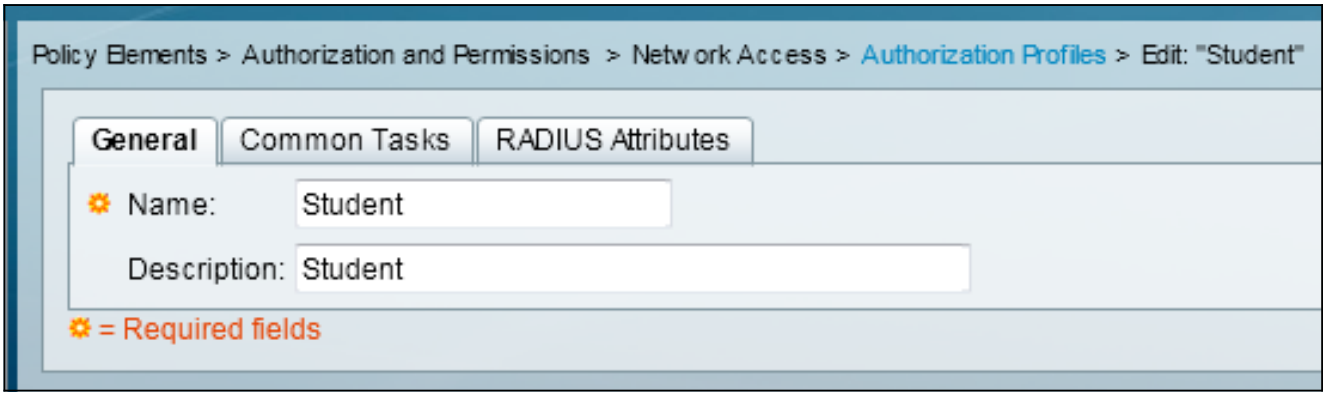
2. Cree los Nombres de usuario y a los grupos apropiados de la identidad. En este ejemplo, es estudiante y todos los grupos: Estudiantes, y profesor y AllGroups: Profesores.



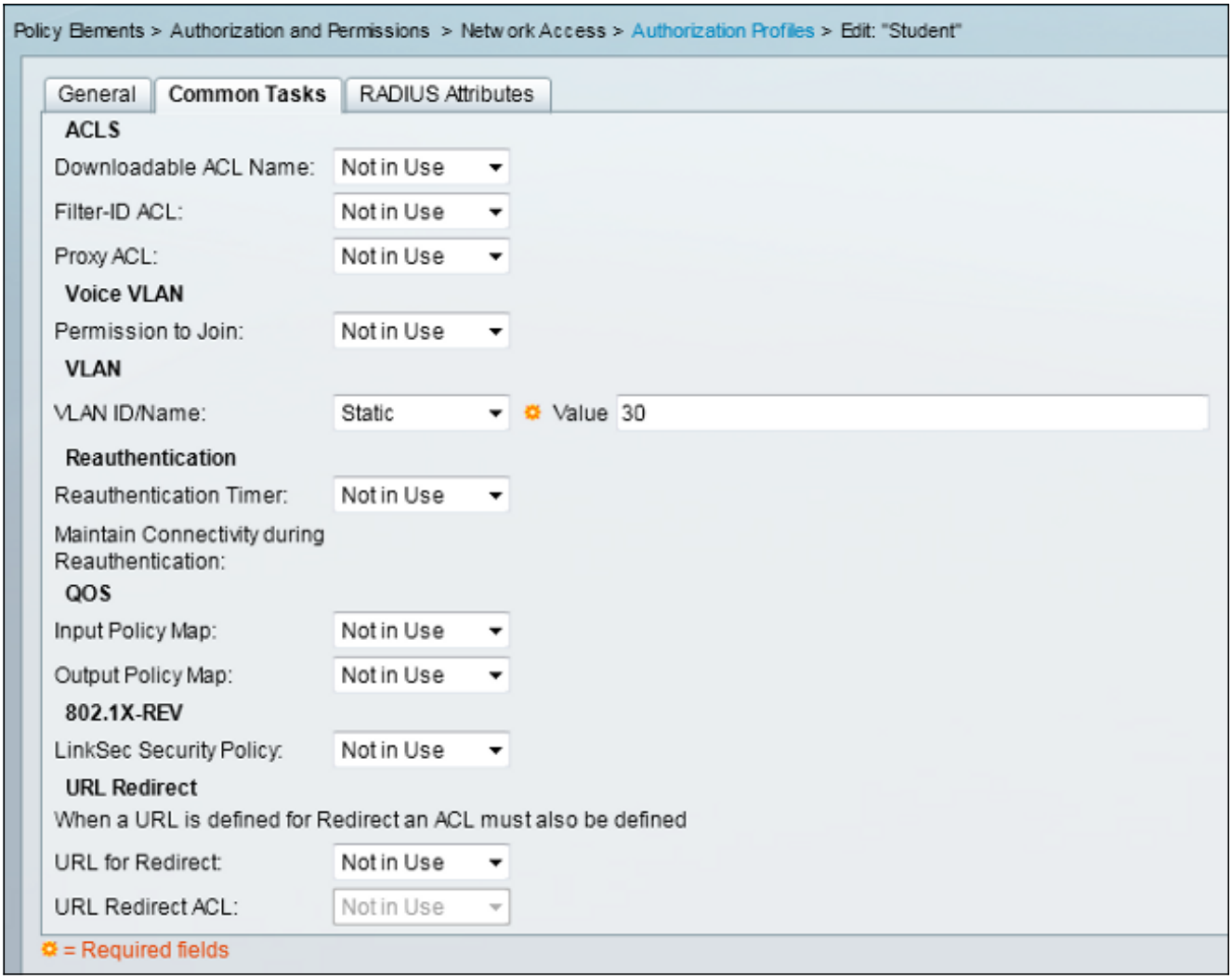
3. Navegue a los **elementos de la directiva >** a la **autorización y a los permisos >** a los **perfiles del acceso a la red >** de la **autorización**, y cree los perfiles de la autorización para la invalidación AAA.



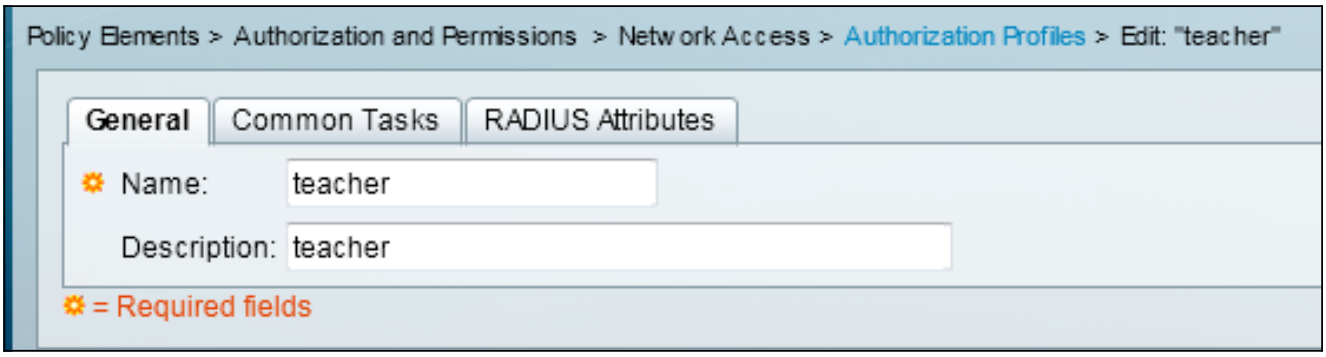
4. Edite el perfil de la autorización para el estudiante.



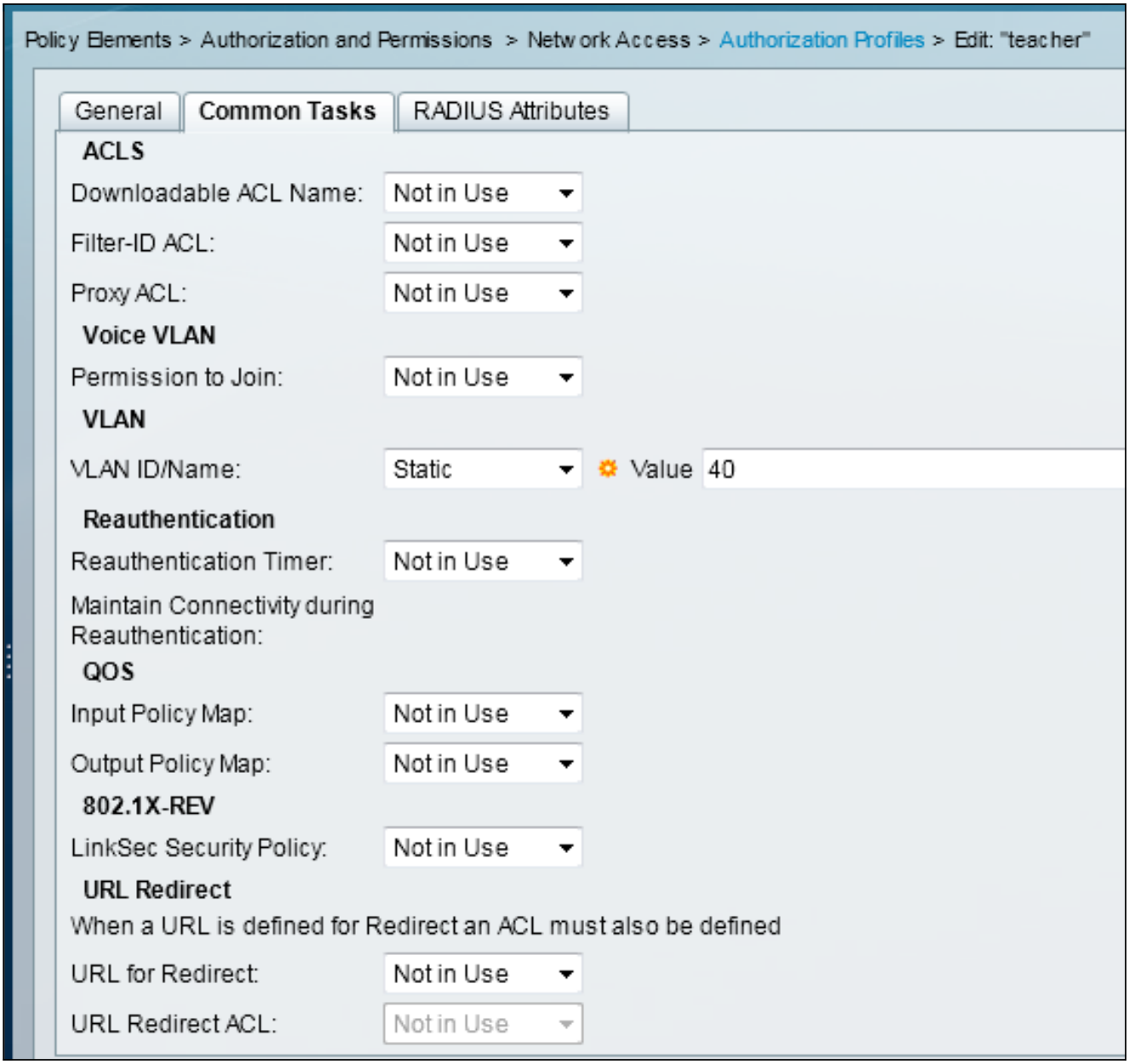
5. Fije el VLA N ID/Name como **parásitos atmosféricos** con un valor de **30** (VLAN 30).



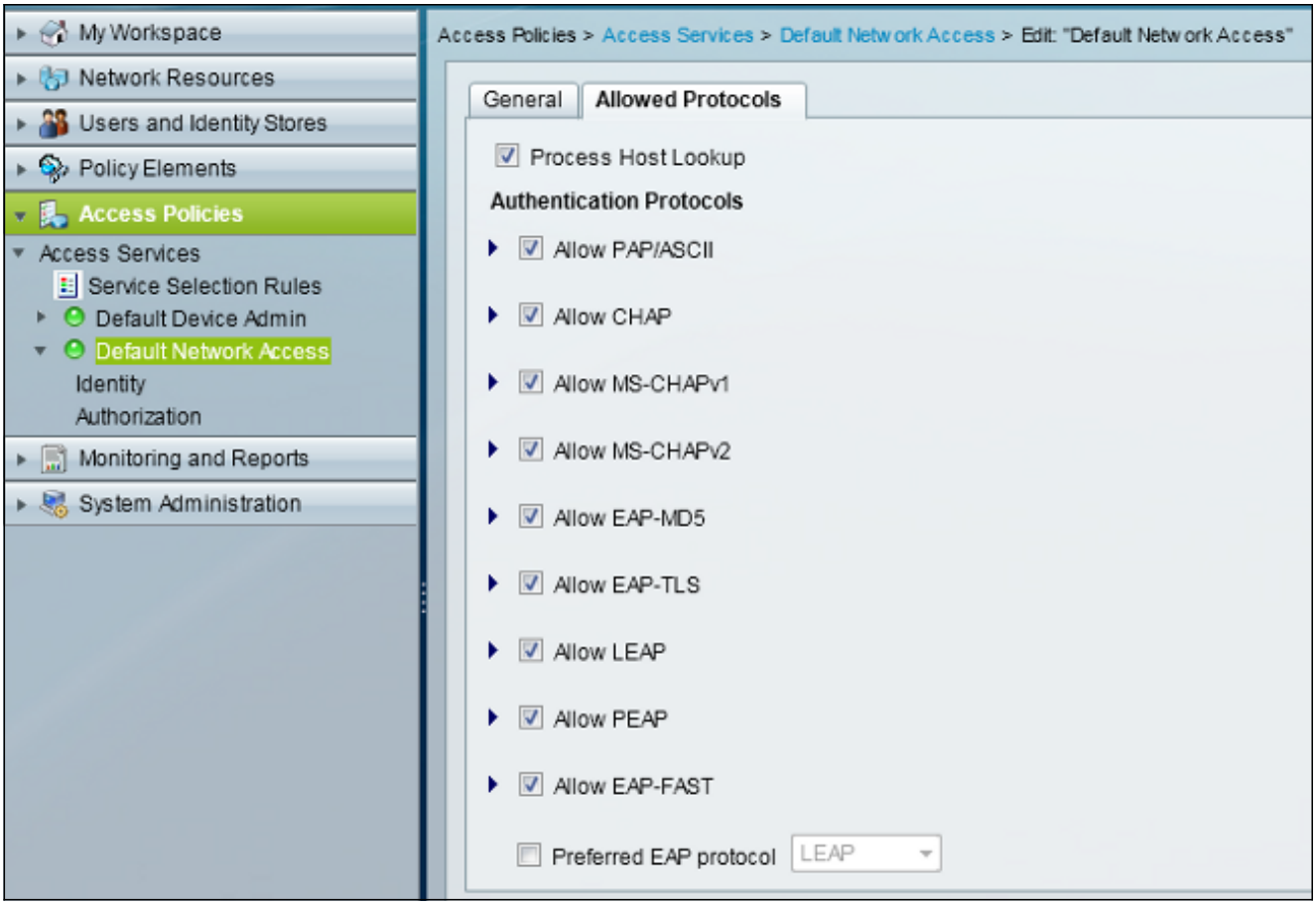
6. Edite el perfil de la autorización para el profesor.



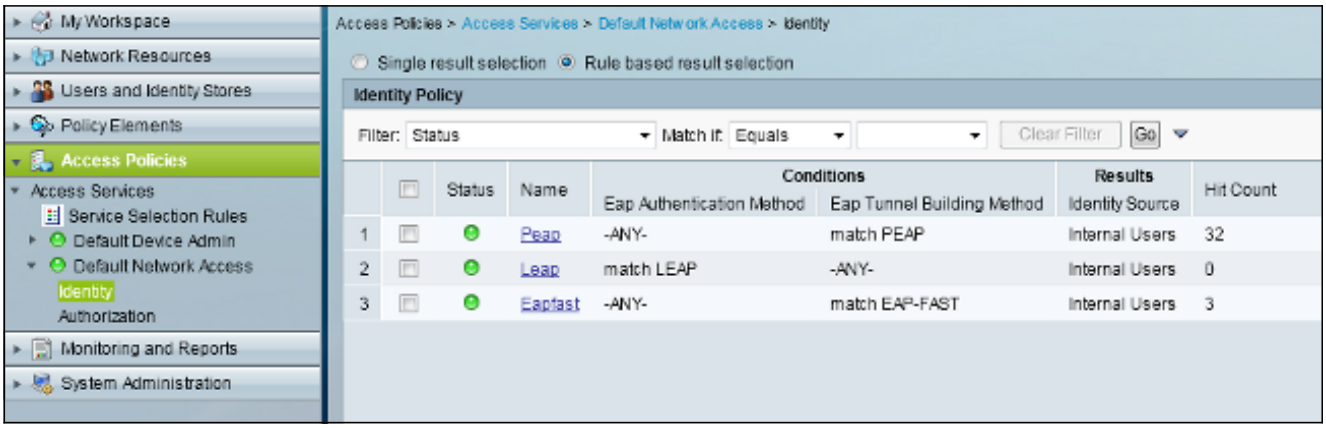
7. Fije el VLA N ID/Name como **parásitos atmosféricos** con un valor de **40** (VLA N 40).



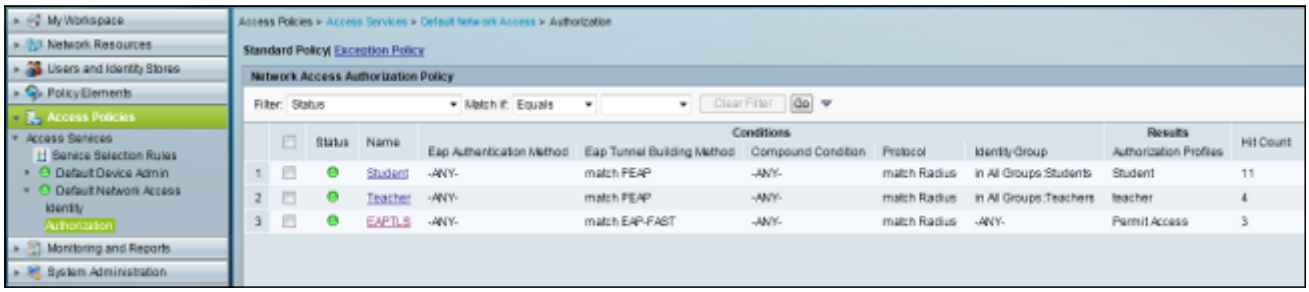
8. Navegue a las **políticas de acceso** > al **acceso mantiene > acceso de red predeterminada**, y hace clic la lengueta **permitida de los protocolos**. Marque el checkbox de la **permit PEAP**.



9. Navegue a la **identidad**, y defina las reglas para permitir a los usuarios PEAP.



10. Navegue a la **autorización**, y estudiante y profesor de la correspondencia a la directiva de la autorización; en este ejemplo, la asignación debe ser estudiante para el VLAN 30 y profesor para el VLA N 40.

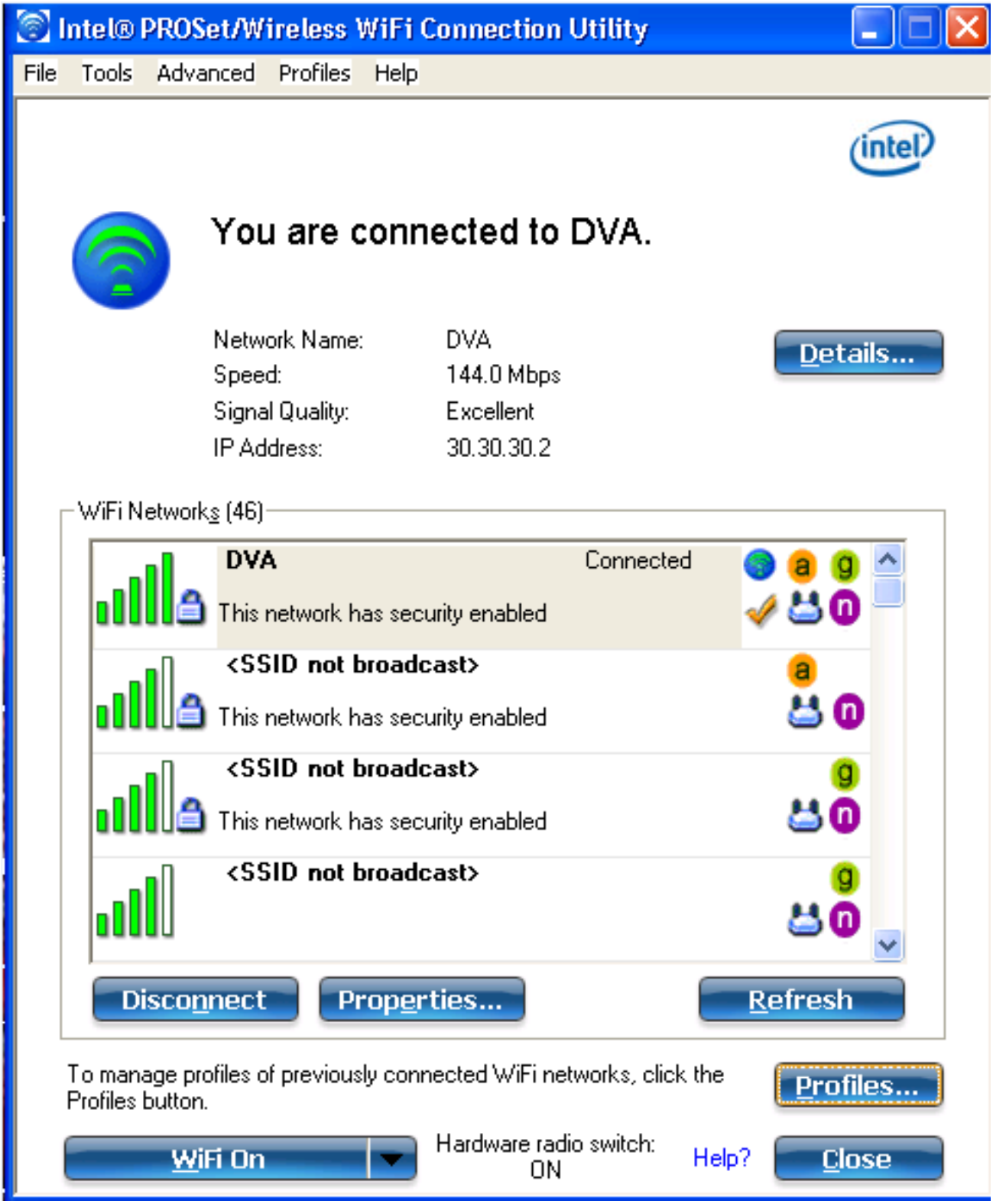


Verificación

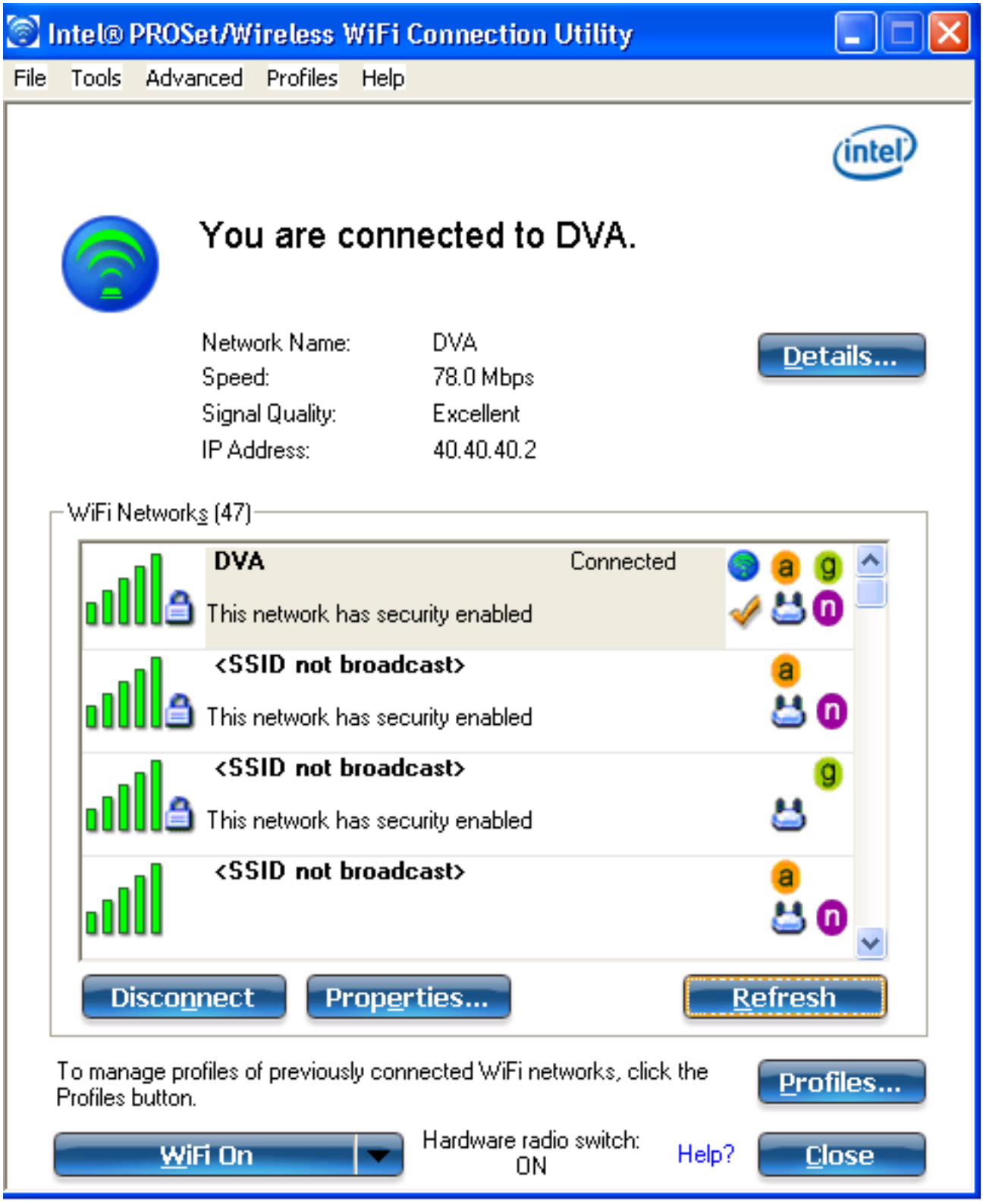
Use esta sección para confirmar que su configuración funciona correctamente. Éstos son los procesos de verificación:

- Monitoree la página en el ACS ese las demostraciones que autentican los clientes.

- Conecte con la red inalámbrica (WLAN) DVA con el grupo de estudiantes, y revise la utilidad de la conexión de WiFi del cliente.



- Conecte con la red inalámbrica (WLAN) DVA con el grupo del profesor, y revise la utilidad de la conexión de WiFi del cliente.



Troubleshooting

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

Notas:

Use la Command Lookup Tool (clientes registrados solamente) para obtener más información sobre los comandos usados en esta sección.

> La herramienta del Output Interpreter (clientes registrados solamente) apoya los ciertos comandos show. Utilice la herramienta del Output Interpreter para ver una análisis de la salida del comando show.
>
> Consulte Información Importante sobre Comandos de Debug antes de usar un **comando debug**.

Los debugs útiles incluyen el *mac del* **MAC Address del cliente del debug**, así como estos comandos trace NGWC:

- **fije el debug del nivel del grupo-Tecnología inalámbrica-cliente de la traza**
- **fije el mac** *xxxx.xxxx.xxxx del* **filtro del grupo-Tecnología inalámbrica-cliente de la traza**
- **muestre las sys-filtrar-trazas de la traza**

La traza NGWC no incluye dot1x/AAA, así que utilice esta lista entera de trazas combinadas para dot1x/AAA:

- **fije el debug del nivel del grupo-Tecnología inalámbrica-cliente de la traza**
- **fije el debug del nivel del evento de la traza wcm-dot1x**
- **fije el debug del nivel de la traza wcm-dot1x aaa**
- **fije el debug llano de los eventos inalámbricos aaa de la traza**
- **fije el debug del nivel de la base SM de la acceso-sesión de la traza**
- **fije el debug llano del dot1x del método de la acceso-sesión de la traza**
- **fije el mac** *xxxx.xxxx.xxxx del* **filtro del grupo-Tecnología inalámbrica-cliente de la traza**
- **fije el mac** *xxxx.xxxx.xxxx del* **filtro del evento de la traza wcm-dot1x**
- **fije el mac** *xxxx.xxxx.xxxx del* **filtro de la traza wcm-dot1x aaa**
- **fije el mac inalámbrico** *xxxx.xxxx.xxxx del* **filtro de los eventos aaa de la traza**
- **fije el mac** *xxxx.xxxx.xxxx del* **filtro de la base SM de la acceso-sesión de la traza**
- **fije el mac** *xxxx.xxxx.xxxx del* **filtro del dot1x del método de la acceso-sesión de la traza**
- **muestre las sys-filtrar-trazas de la traza**

Cuando la asignación del VLAN dinámico está trabajando correctamente, usted debe ver este tipo de salida de los debugs:

```
09/01/13 12:13:28.598 IST 1ccc 5933] 0021.5C8C.C761 1XA: Received Medium tag (0)
Tunnel medium type (6) and Tunnel-Type tag (0) and Tunnel-type (13)
Tunnel-Private-Id (30)
[09/01/13 12:13:28.598 IST 1ccd 5933] 0021.5C8C.C761 Tunnel-Group-Id is 30
[09/01/13 12:13:28.598 IST 1cce 5933] 0021.5C8C.C761 Checking Interface
Change - Current VlanId: 40 Current Intf: VLAN0040 New Intf: VLAN0030 New
GroupIntf:  intfChanged: 1
[09/01/13 12:13:28.598 IST 1ccf 5933] 0021.5C8C.C761 Incrementing the
Reassociation Count 1 for client (of interface VLAN0040)
 --More--         [09/01/13 12:13:28.598 IST 1cd0 5933] 0021.5C8C.C761
Clearing Address 40.40.40.2 on mobile
[09/01/13 12:13:28.598 IST 1cd1 5933] 0021.5C8C.C761 Applying new AAA override
for station  0021.5C8C.C761
[09/01/13 12:13:28.598 IST 1cd2 5933] 0021.5C8C.C761 Override values (cont..)
dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, rTimeBurstC: -1
    vlanIfName: 'VLAN0030', aclName: ''

[09/01/13 12:13:28.598 IST 1cd3 5933] 0021.5C8C.C761 Clearing Dhcp state for
station  ---
[09/01/13 12:13:28.598 IST 1cd4 5933] 0021.5C8C.C761 Applying WLAN ACL policies
```

to client
[09/01/13 12:13:28.598 IST 1cd5 5933] 0021.5C8C.C761 No Interface ACL used for
Wireless client in WCM(NGWC)
[09/01/13 12:13:28.598 IST 1cd6 5933] 0021.5C8C.C761 Inserting AAA Override
struct for mobile
   MAC: 0021.5C8C.C761 , source 4

**[09/01/13 12:13:28.598 IST 1cd7 5933] 0021.5C8C.C761 Inserting new RADIUS
override into chain for station 0021.5C8C.C761**
[09/01/13 12:13:28.598 IST 1cd8 5933] 0021.5C8C.C761 Override values (cont..)
dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, rTimeBurstC: -1
   vlanIfName: 'VLAN0030', aclName: ''

 --More--   [09/01/13 12:13:28.598 IST 1cd9 5933] 0021.5C8C.C761
Applying override policy from source Override Summation:

[09/01/13 12:13:28.598 IST 1cda 5933] 0021.5C8C.C761 Override values (cont..)
dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, rTimeBurstC: -1
   vlanIfName: 'VLAN0030', aclName: ''

**[09/01/13 12:13:28.598 IST 1cdb 5933] 0021.5C8C.C761 Applying local bridging
Interface Policy for station 0021.5C8C.C761 - vlan 30, interface 'VLAN0030'**
[09/01/13 12:13:28.598 IST 1cdc 5933] 0021.5C8C.C761 1XA: Setting reauth timeout
to 1800 seconds from WLAN config
[09/01/13 12:13:28.598 IST 1cdd 5933] 0021.5C8C.C761 1XA: Setting reauth timeout
to 1800 seconds
[09/01/13 12:13:28.598 IST 1cde 5933] 0021.5C8C.C761 1XK: Creating a PKC PMKID
Cache entry (RSN 1)
[09/01/13 12:13:28.598 IST 1cdf 5933] 0021.5C8C.C761 1XK: Set Link Secure: 0

**[09/01/13 12:08:59.553 IST 1ae1 5933] 0021.5C8C.C761 1XA: Received Medium tag (0)
Tunnel medium type (6) and Tunnel-Type tag (0) and Tunnel-type (13)
Tunnel-Private-Id (40)**
[09/01/13 12:08:59.553 IST 1ae2 5933] 0021.5C8C.C761 Tunnel-Group-Id is 40
 --More--   [09/01/13 12:08:59.553 IST 1ae3 5933] 0021.5C8C.C761
Checking Interface Change - Current VlanId: 20 Current Intf: VLAN0020 New Intf:
VLAN0040 New GroupIntf: intfChanged: 1
[09/01/13 12:08:59.553 IST 1ae4 5933] 0021.5C8C.C761 Applying new AAA override for
station 0021.5C8C.C761
**[09/01/13 12:08:59.553 IST 1ae5 5933] 0021.5C8C.C761 Override values (cont..)
dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, rTimeBurstC: -1
    vlanIfName: 'VLAN0040', aclName: ''**

[09/01/13 12:08:59.553 IST 1ae6 5933] 0021.5C8C.C761 Clearing Dhcp state for
station ---
[09/01/13 12:08:59.553 IST 1ae7 5933] 0021.5C8C.C761 Applying WLAN ACL policies
to client
[09/01/13 12:08:59.553 IST 1ae8 5933] 0021.5C8C.C761 No Interface ACL used for
Wireless client in WCM(NGWC)
[09/01/13 12:08:59.553 IST 1ae9 5933] 0021.5C8C.C761 Inserting AAA Override struct
for mobile
   MAC: 0021.5C8C.C761 , source 4

**[09/01/13 12:08:59.553 IST 1aea 5933] 0021.5C8C.C761 Inserting new RADIUS override
into chain for station 0021.5C8C.C761**
[09/01/13 12:08:59.553 IST 1aeb 5933] 0021.5C8C.C761 Override values (cont..)
dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, rTimeBurstC: -1
   vlanIfName: 'VLAN0040', aclName: ''
 --More--
**[09/01/13 12:08:59.553 IST 1aec 5933] 0021.5C8C.C761 Applying override policy
from source Override Summation:**

[09/01/13 12:08:59.553 IST 1aed 5933] 0021.5C8C.C761 Override values (cont..)

dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, rTimeBurstC: -1
   vlanIfName: 'VLAN0040', aclName: ''

[09/01/13 12:08:59.553 IST 1aee 5933] 0021.5C8C.C761 Applying local bridging Interface Policy for station 0021.5C8C.C761 - vlan 40, interface 'VLAN0040'
[09/01/13 12:08:59.553 IST 1aef 5933] 0021.5C8C.C761 1XA: Setting reauth timeout to 1800 seconds from WLAN config
[09/01/13 12:08:59.553 IST 1af0 5933] 0021.5C8C.C761 1XA: Setting reauth timeout to 1800 seconds
[09/01/13 12:08:59.553 IST 1af1 5933] 0021.5C8C.C761 1XK: Creating a PKC PMKID Cache entry (RSN 1)