Configurar a atribuição dinâmica de VLAN com NGWC e ACS 5.2

Contents

Introduction

Este documento descreve o conceito de atribuição de VLAN dinâmica. Ele também descreve como configurar o controlador de LAN sem fio (WLC) e um servidor RADIUS para atribuir dinamicamente clientes de LAN sem fio (WLAN) a uma VLAN específica. Neste documento, o servidor RADIUS é um Access Control Server (ACS) que executa o Cisco Secure Access Control System versão 5.2.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimento básico do WLC e dos LAPs (Lightweight Access Points, pontos de acesso

leves)
- Conhecimento funcional do servidor de autenticação, autorização e contabilização (AAA)
- Conhecimento completo da rede Wireless e problemas de segurança Wireless

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Controlador de LAN sem fio Cisco 5760 com Cisco IOS® XE Software Release 3.2.2 (Next Generation Wiring Closet, ou NGWC)
- Access point Cisco Aironet 3602 Series Lightweight
- Microsoft Windows XP com Intel Proset Supplicant
- Cisco Secure Access Control System versão 5.2
- Switch Cisco Catalyst 3560 Series

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.

Atribuição da VLAN (Rede local virtual) dinâmica com servidor Radius

Na maioria de sistemas de WLAN, cada WLAN tem uma política estática que se aplica a todos os clientes associados com um Service Set Identifier (SSID), ou o WLAN na terminologia do controlador. Embora poderoso, este método tem limitações porque exige que os clientes se associem com os diferentes SSID para herdar diferentes QoS e políticas de segurança.

Mas a solução de Cisco WLAN suporta identidades na rede. Isso permite que a rede anuncie um único SSID, mas permite que usuários específicos herdem diferentes QoS, atributos de VLAN e/ou políticas de segurança com base nas credenciais do usuário.

A atribuição da VLAN dinâmica é um recurso que coloca um usuário wireless em uma VLAN específica baseado nas credenciais fornecidas pelo usuário. Essa tarefa de atribuição de usuário a uma VLAN específica é tratada por um servidor de autenticação RADIUS, como um Cisco Secure ACS. Esse recurso pode ser usado, por exemplo, para permitir que o host sem fio permaneça na mesma VLAN à medida que se move dentro de uma rede de campus.

Como resultado, quando um cliente tenta se associar a um LAP registrado em um controlador, o LAP passa as credenciais do usuário ao servidor RADIUS para validação. Quando a autenticação é bem sucedida, o servidor Radius passa determinados atributos da Internet Engineering Task Force (IETF) ao usuário. Estes atributos RADIUS decidem a ID da VLAN que deve ser atribuído ao cliente wireless. O SSID do cliente (a WLAN, em termos de WLC) não importa porque o usuário é sempre atribuído a esse ID de VLAN predeterminado.

Os atributos do usuário do RADIUS usados para a atribuição de ID da VLAN são:

- IETF 64 (Tipo de túnel) - Definido como VLAN.
- IETF 65 (Tunnel Medium Type) - Definido como 802.
- IETF 81 (Tunnel-Private-Group-ID) - Definido como ID da VLAN.

O ID da VLAN é de 12 bits e tem um valor entre 1 e 4094, inclusive. Como Tunnel-Private-Group-ID é do tipo string, como definido em RFC 2868, RADIUS Attributes for Tunnel Protocol Support para uso com IEEE 802.1X, o valor inteiro da ID da VLAN é codificado como uma string. Quando estes atributos de túnel são enviados, é necessário preencher o campo Tag.

Como é explicado na RFC2868 , seção 3.1:

"O campo Tag tem um octeto de comprimento e se destina a fornecer um meio de agrupar atributos no mesmo pacote que se referem ao mesmo túnel."

Os valores válidos para o campo Tag são 0x01 a 0x1F, inclusive. Se o campo Tag não for utilizado, ele deve ser zero (0x00). Consulte na RFC 2868 mais informações sobre todos os atributos de RADIUS.

Configurar

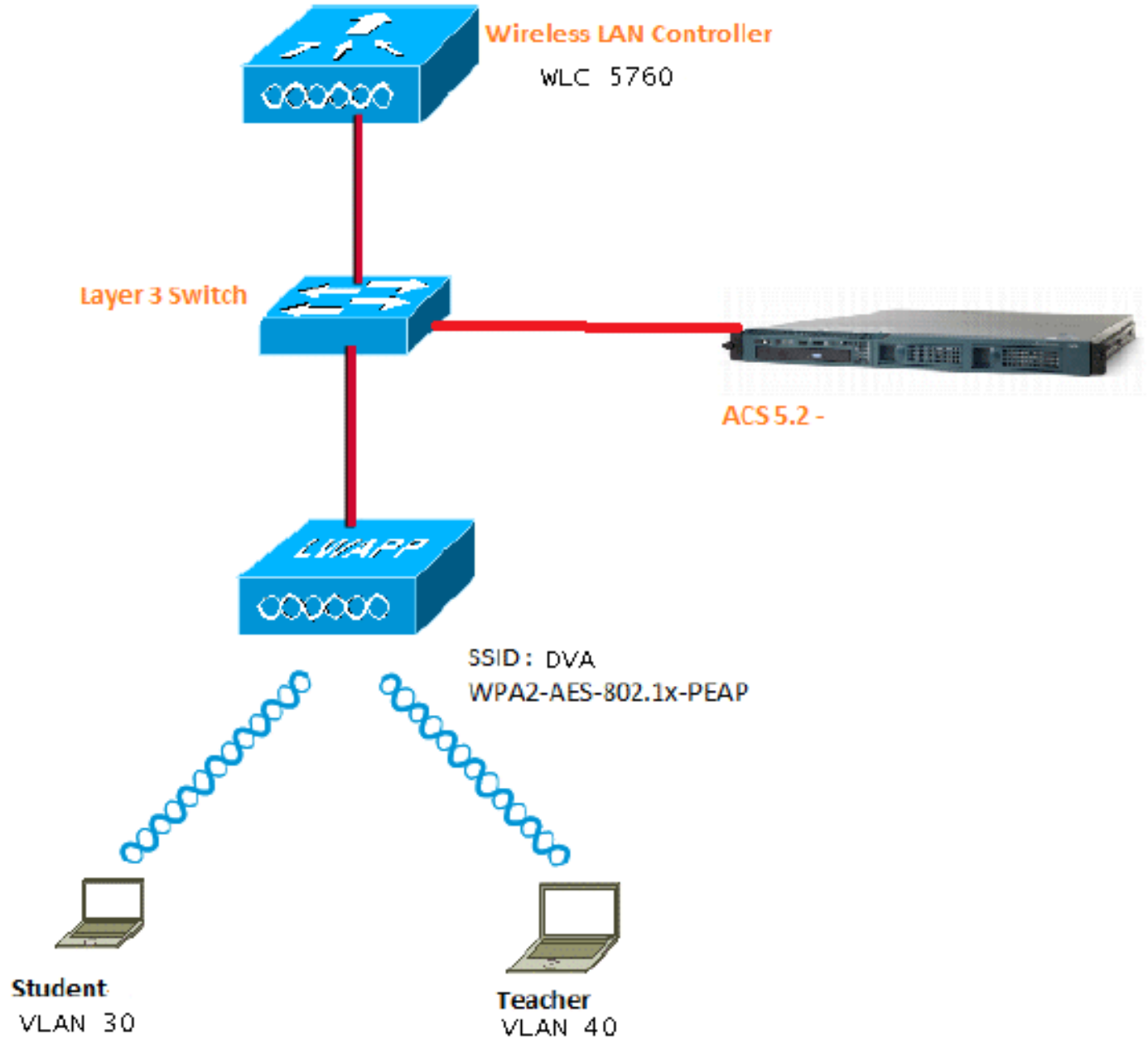
A configuração de uma atribuição de VLAN dinâmica consiste em duas etapas distintas:

1. Configure o WLC com a interface de linha de comando (CLI) ou com a GUI.
2. Configure o servidor RADIUS.

Note: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



Este documento usa 802.1X com PEAP (Protected Extensible Authentication Protocol) como mecanismo de segurança.

Hipóteses

- Os switches são configurados para todas as VLANs de Camada 3 (L3).
- O servidor DHCP recebe um escopo DHCP.
- A conectividade L3 existe entre todos os dispositivos na rede.
- O LAP já está associado à WLC.
- Cada VLAN tem uma máscara /24.
- O ACS 5.2 tem um certificado autoassinado instalado.

Configurar WLC com CLI

Configurar WLAN

Este é um exemplo de como configurar uma WLAN com o SSID do DVA:

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

Configurar o servidor RADIUS na WLC

Este é um exemplo da configuração do servidor RADIUS na 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
```

Configurar o pool DHCP para a VLAN do cliente

Este é um exemplo da configuração do pool DHCP para a VLAN 30 e VLAN 40 do cliente:

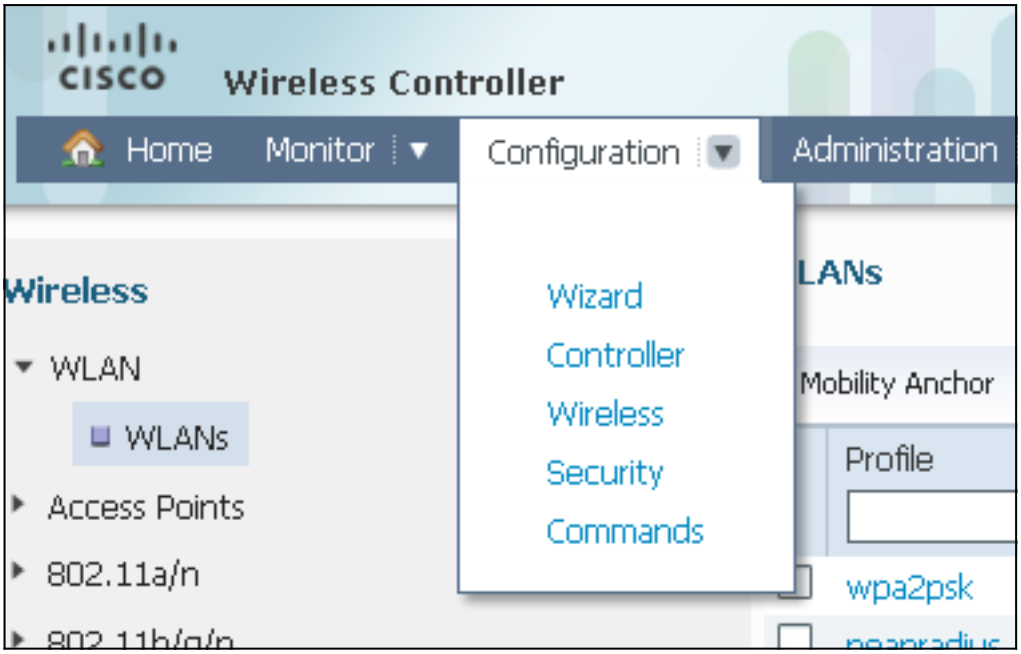
```
interface Vlan30
 ip address 30.30.30.1 255.255.255.0
!
interface Vlan40
 ip address 40.40.40.1 255.255.255.0

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
```

Configurar WLC com GUI

Configurar WLAN

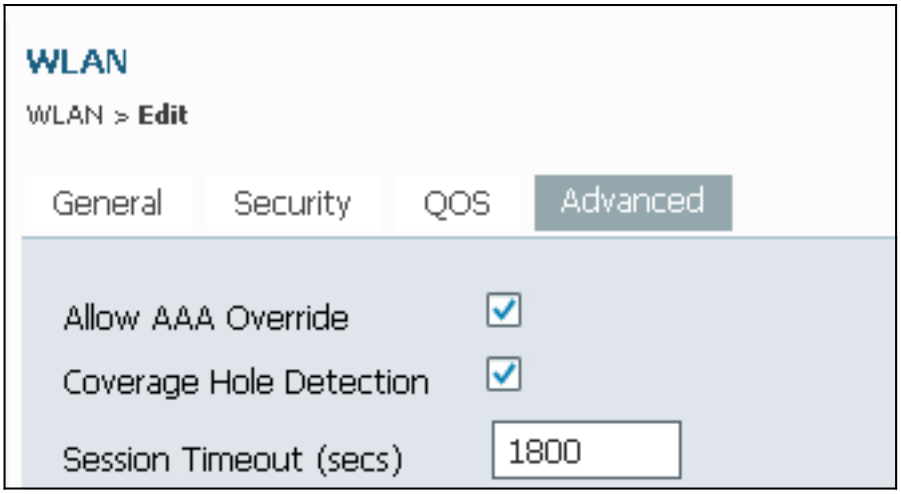
Este procedimento descreve como configurar a WLAN.

1. Navegue até a **guia Configuration > Wireless > WLAN > NEW**.

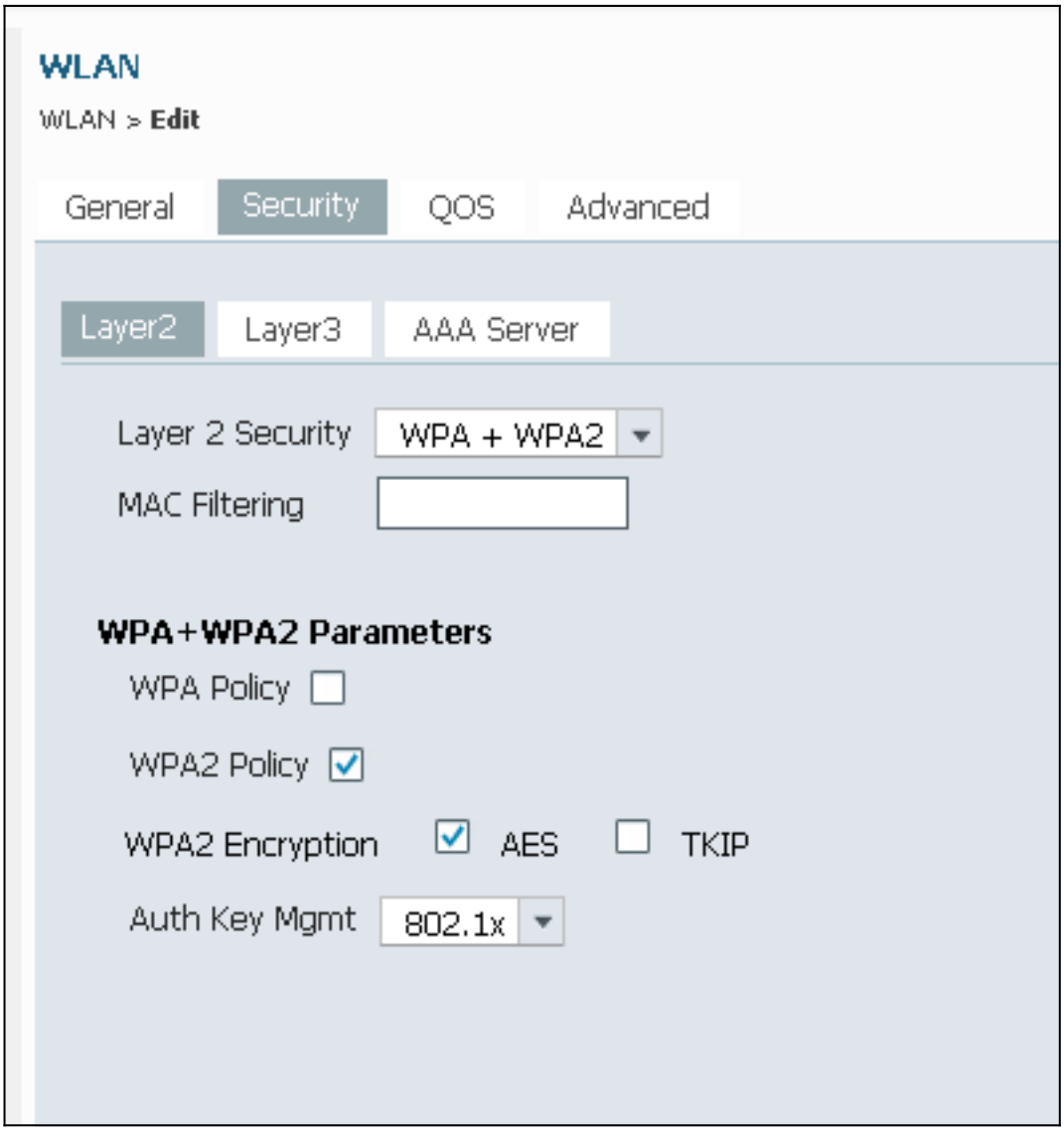


2. Clique na guia **Geral** para ver se a WLAN está configurada para WPA2-802.1X e mapeie a Interface/Grupo de Interface(G) para a VLAN 20 (**VLAN0020**).

3. Clique na guia **Avançado** e marque a caixa de seleção **Permitir substituição de AAA**. A substituição deve estar habilitada para que este recurso funcione.



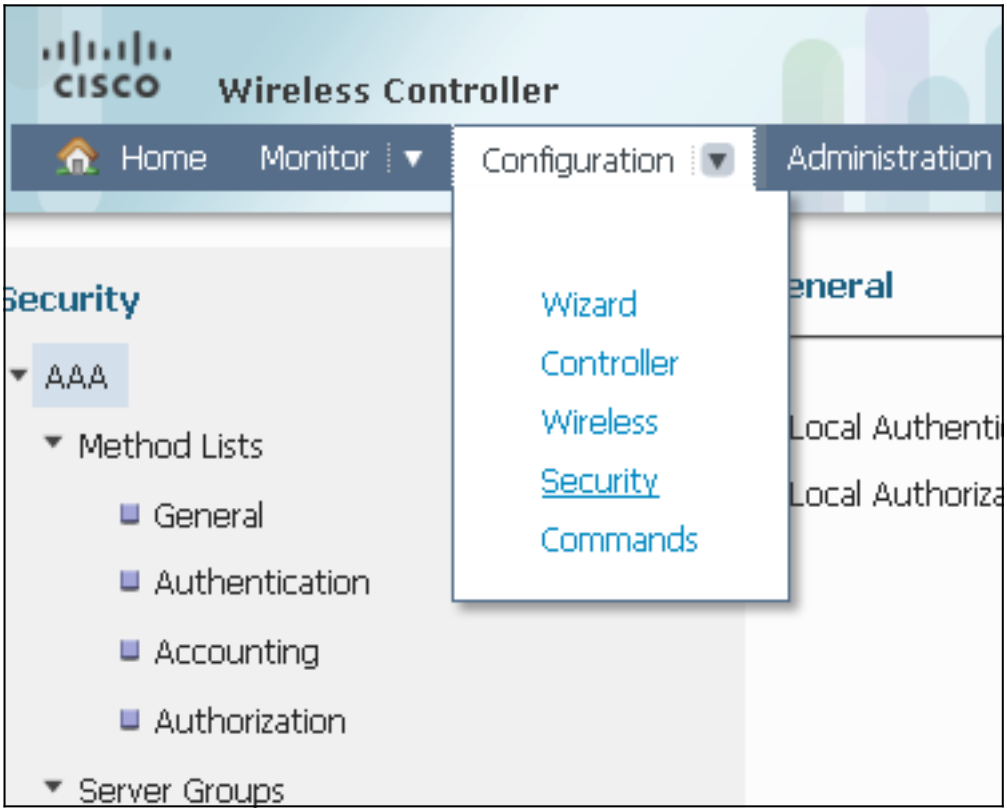
4. Clique na guia **Security** e na guia **Layer2**, marque a caixa de seleção WPA2 Encryption **AES** e selecione **802.1x** na lista suspensa Auth Key Management.



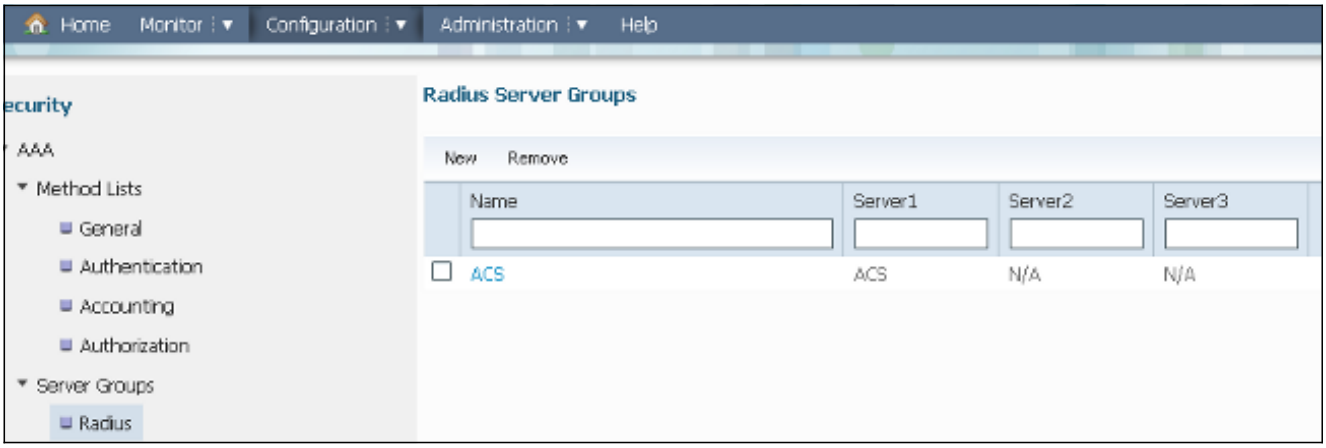
Configurar o servidor RADIUS na WLC

Este procedimento descreve como configurar o servidor RADIUS na WLC.

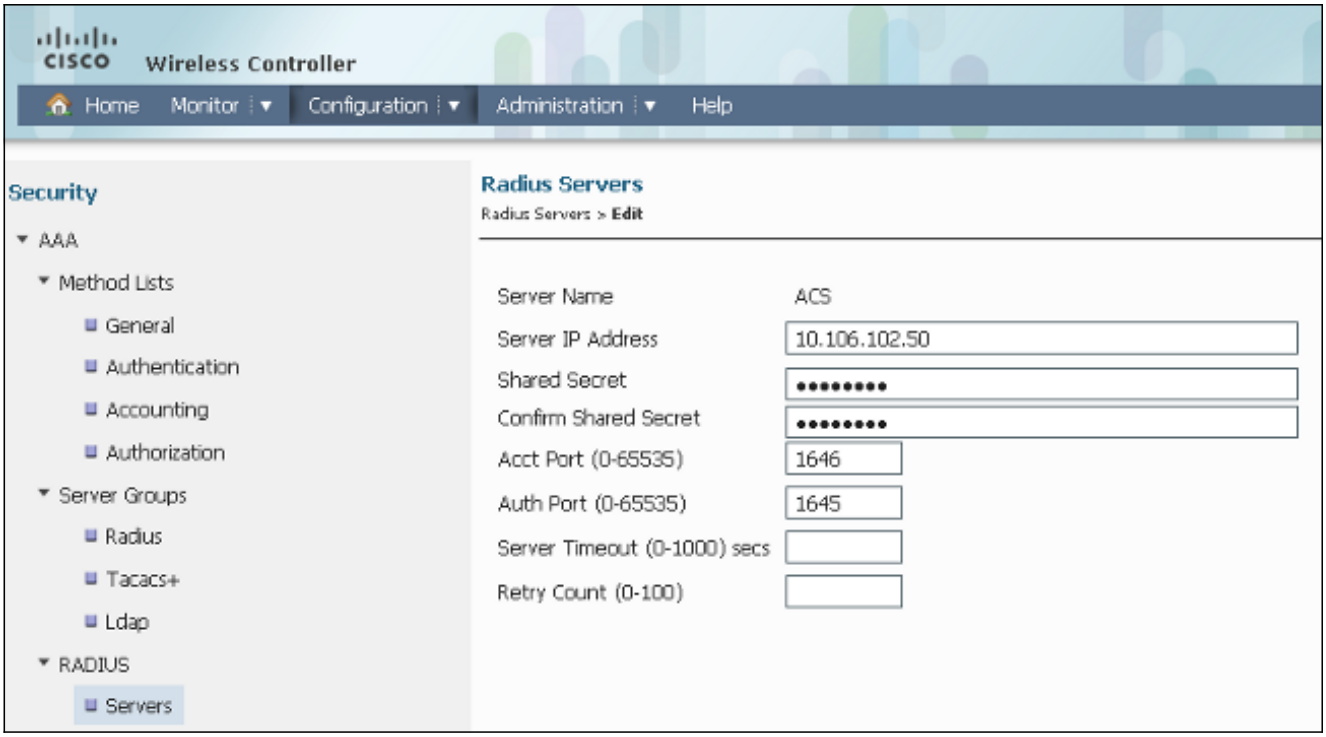
1. Navegue até a guia **Configuração > Segurança**.



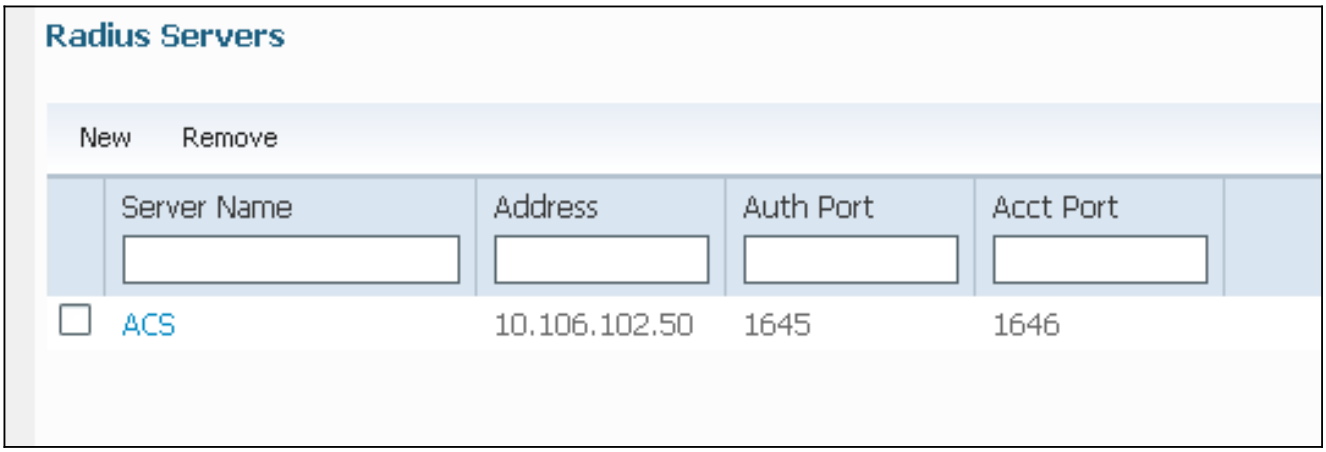
2. Navegue até **AAA > Server Groups > Radius** para criar os Radius Server Groups. Neste exemplo, o Grupo de Servidores Radius é chamado de ACS.



3. Edite a entrada do Servidor Radius para adicionar o Endereço IP do Servidor e o Segredo Compartilhado. Esse segredo compartilhado deve corresponder ao segredo compartilhado no WLC e no servidor RADIUS.



Este é um exemplo de uma configuração completa:

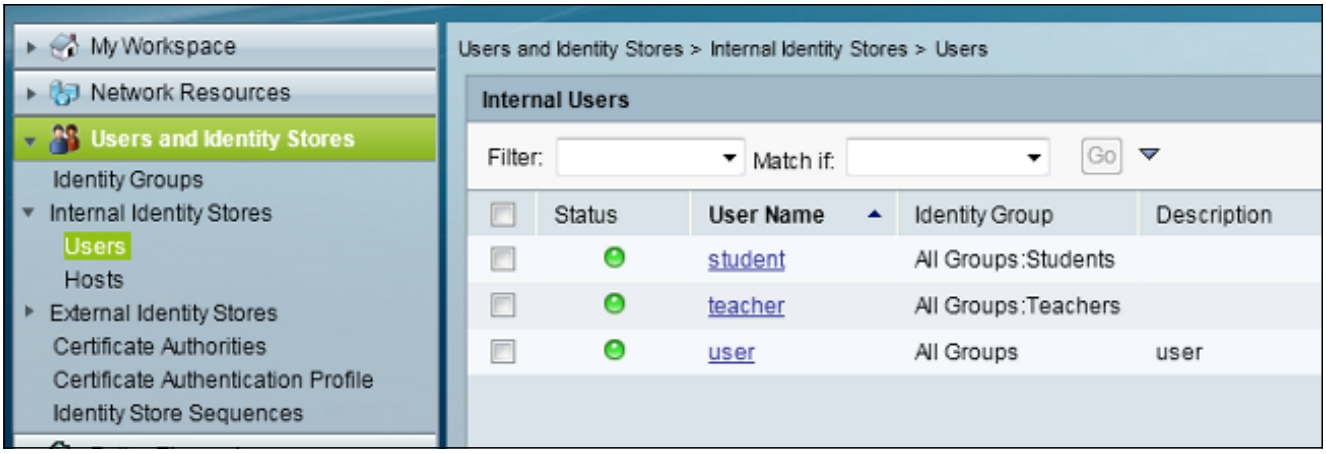


Configurar servidor RADIUS

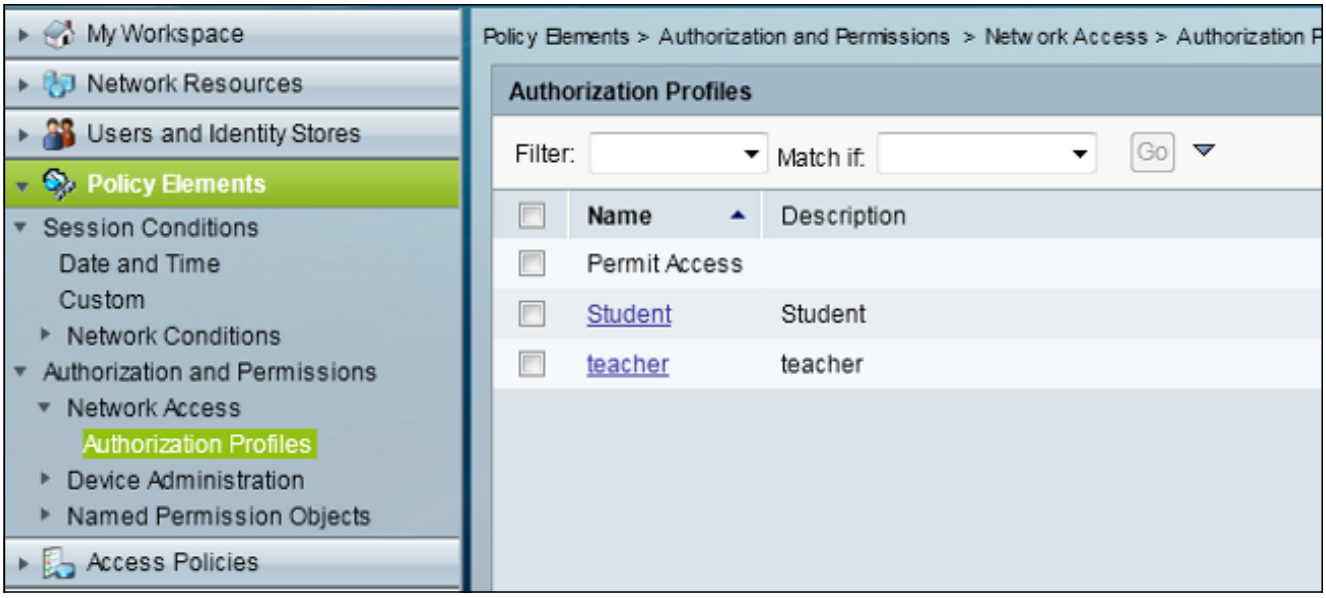
Este procedimento descreve como configurar o servidor RADIUS.

1. No servidor RADIUS, navegue para **Usuários e armazenamento de identidade > Repositórios internos de identidade > Usuários**.

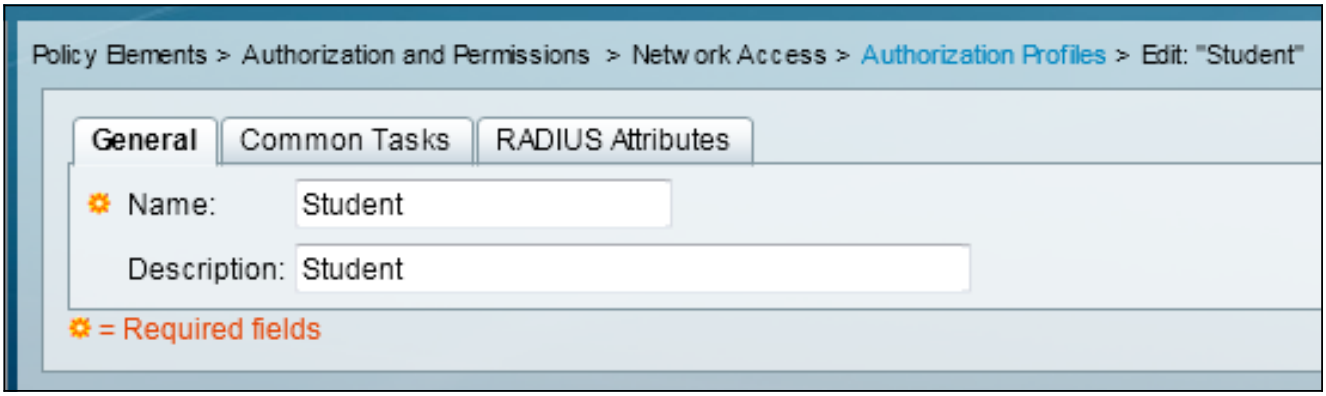
2. Crie os nomes de usuário e grupos de identidade apropriados. Neste exemplo, é aluno e todos os grupos:alunos, professor e todos os grupos:professores.



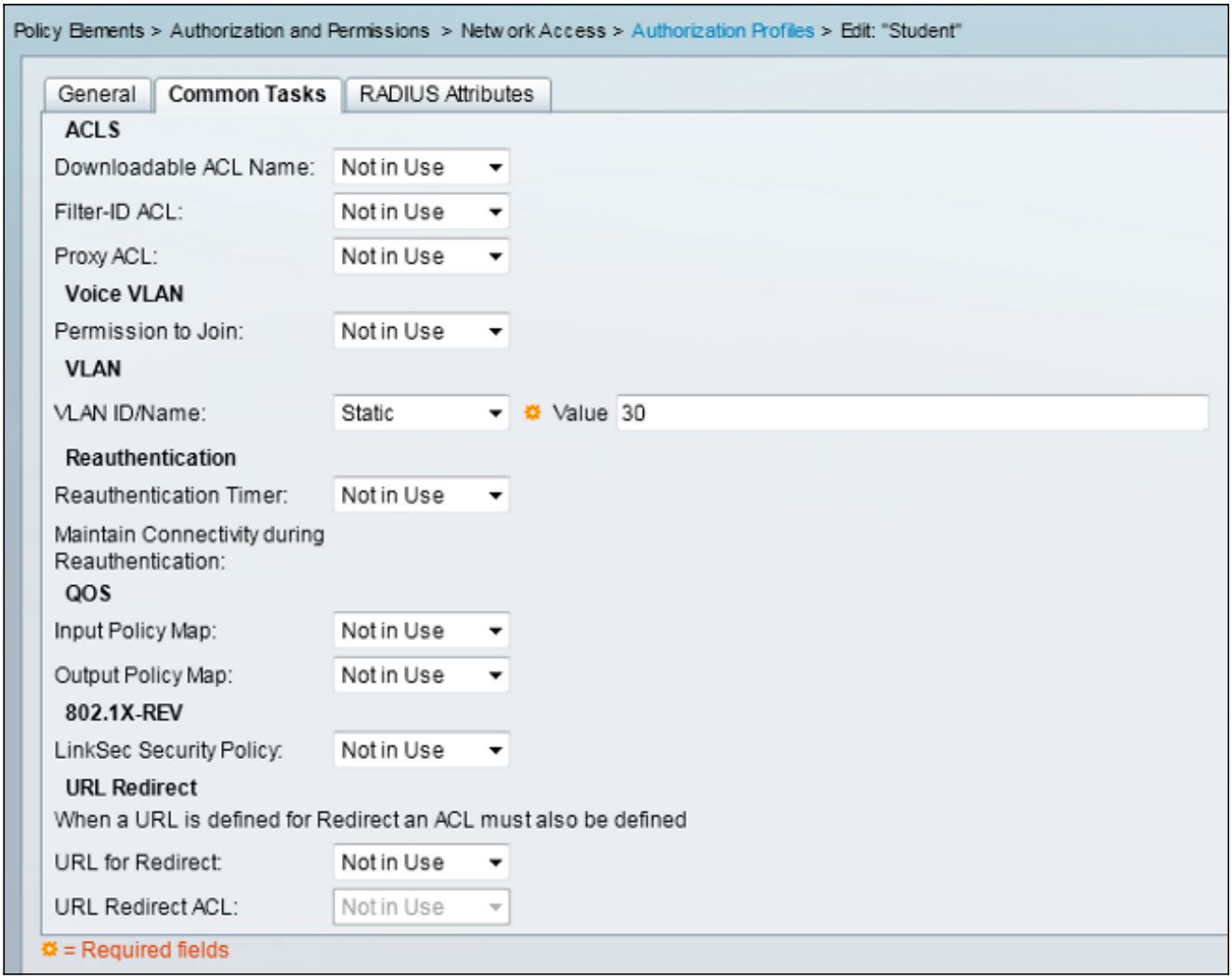
3. Navegue até **Elementos de política > Autorização e permissões > Acesso à rede > Perfis de autorização** e crie os Perfis de autorização para substituição de AAA.



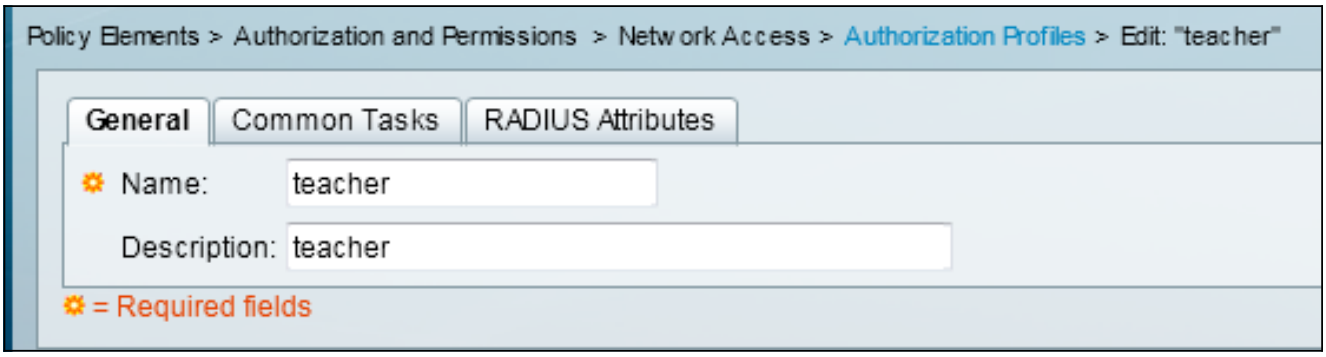
4. Edite o perfil de autorização do aluno.



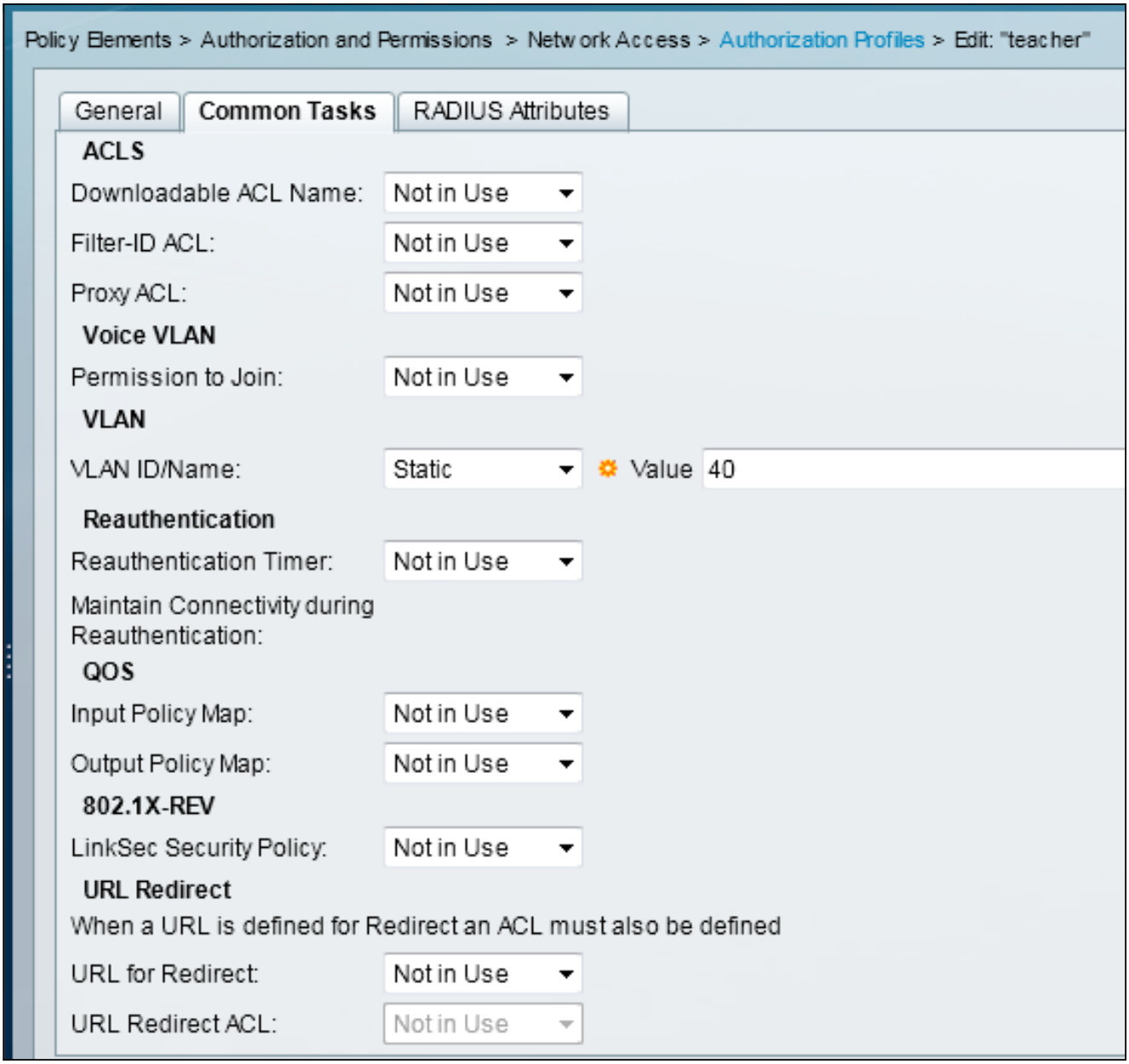
5. Defina o ID/nome da VLAN como **estático** com um valor de **30** (VLAN 30).



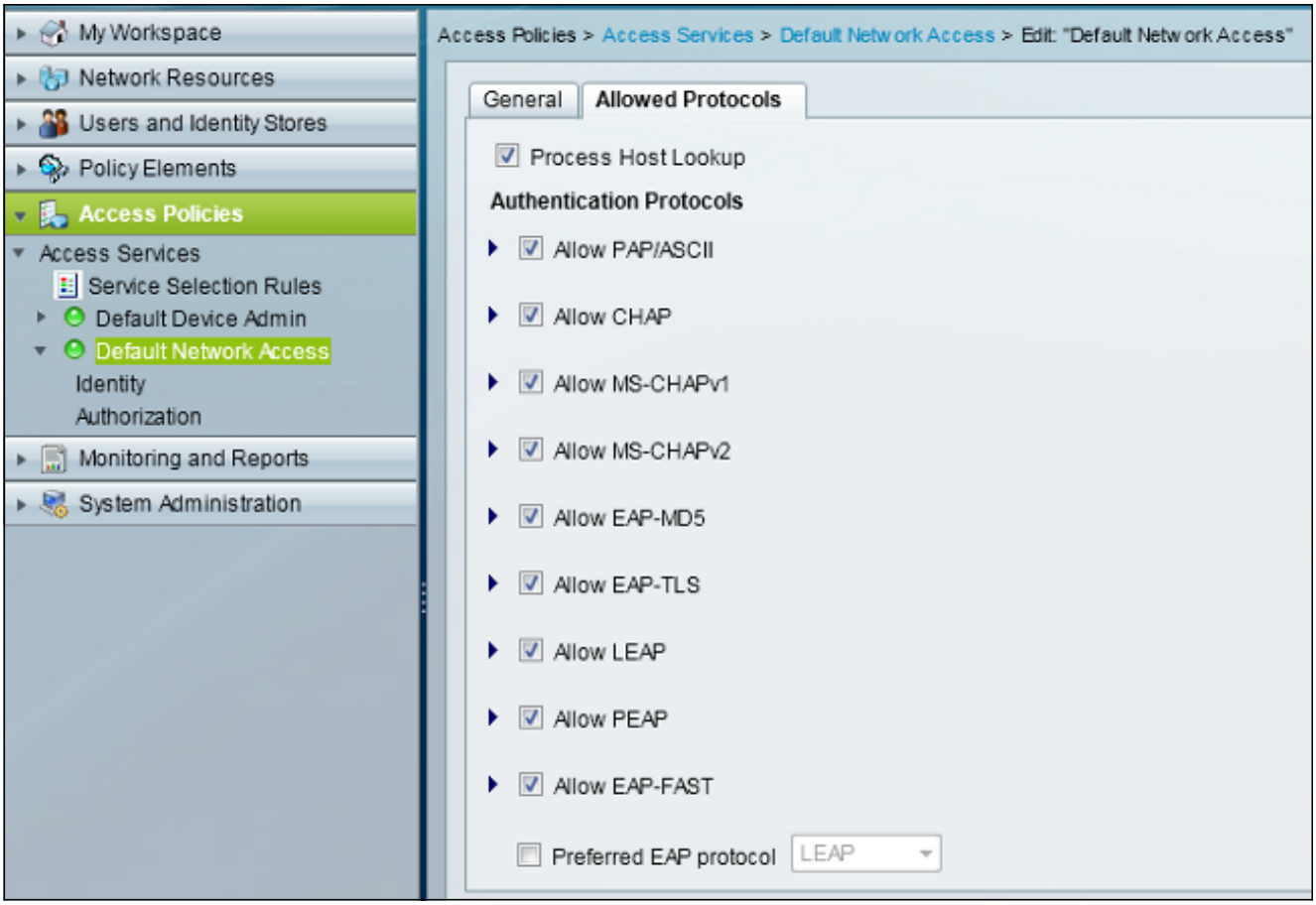
6. Edite o perfil de autorização do professor.



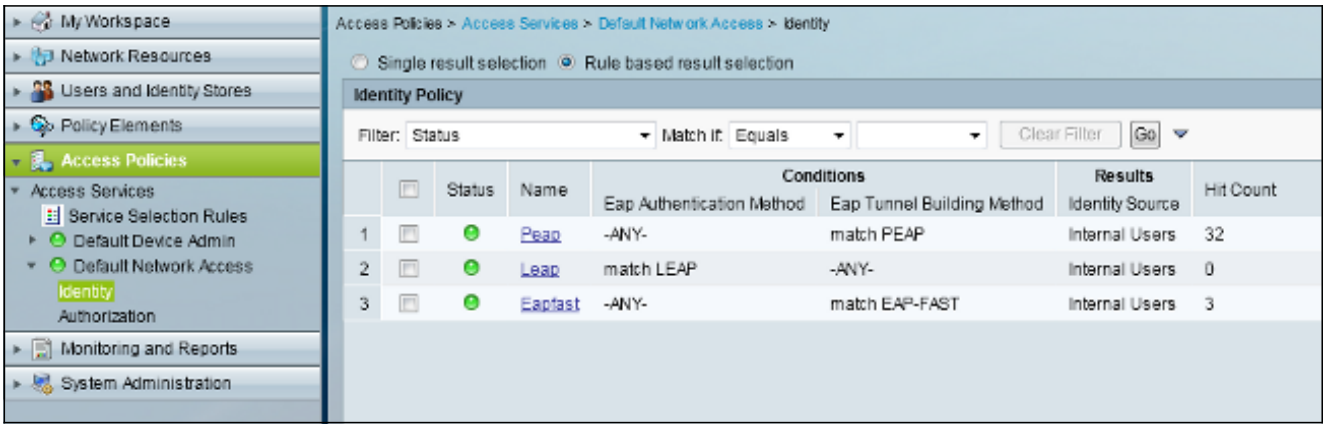
7. Defina o ID/nome da VLAN como **estático** com um valor de **40** (VLAN 40).



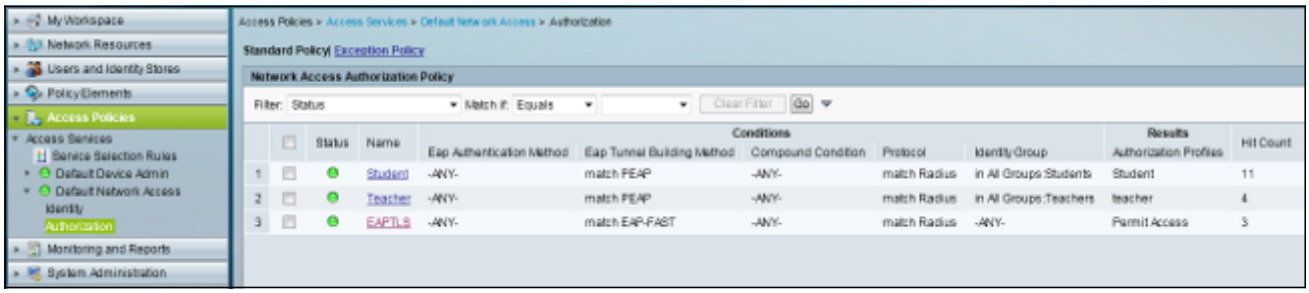
8. Navegue até **Access Policies > Access Services > Default Network Access** e clique na guia **Allowed Protocols**. Marque a caixa de seleção **Permitir PEAP**.



9. Navegue até **Identidade** e defina as regras para permitir usuários PEAP.



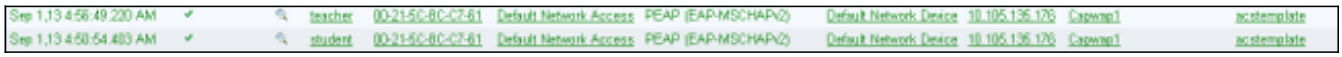
10. Navegue até **Autorização** e mapeie o aluno e o professor para a Política de Autorização; neste exemplo, o mapeamento deve ser Student para VLAN 30 e Teacher para VLAN 40.



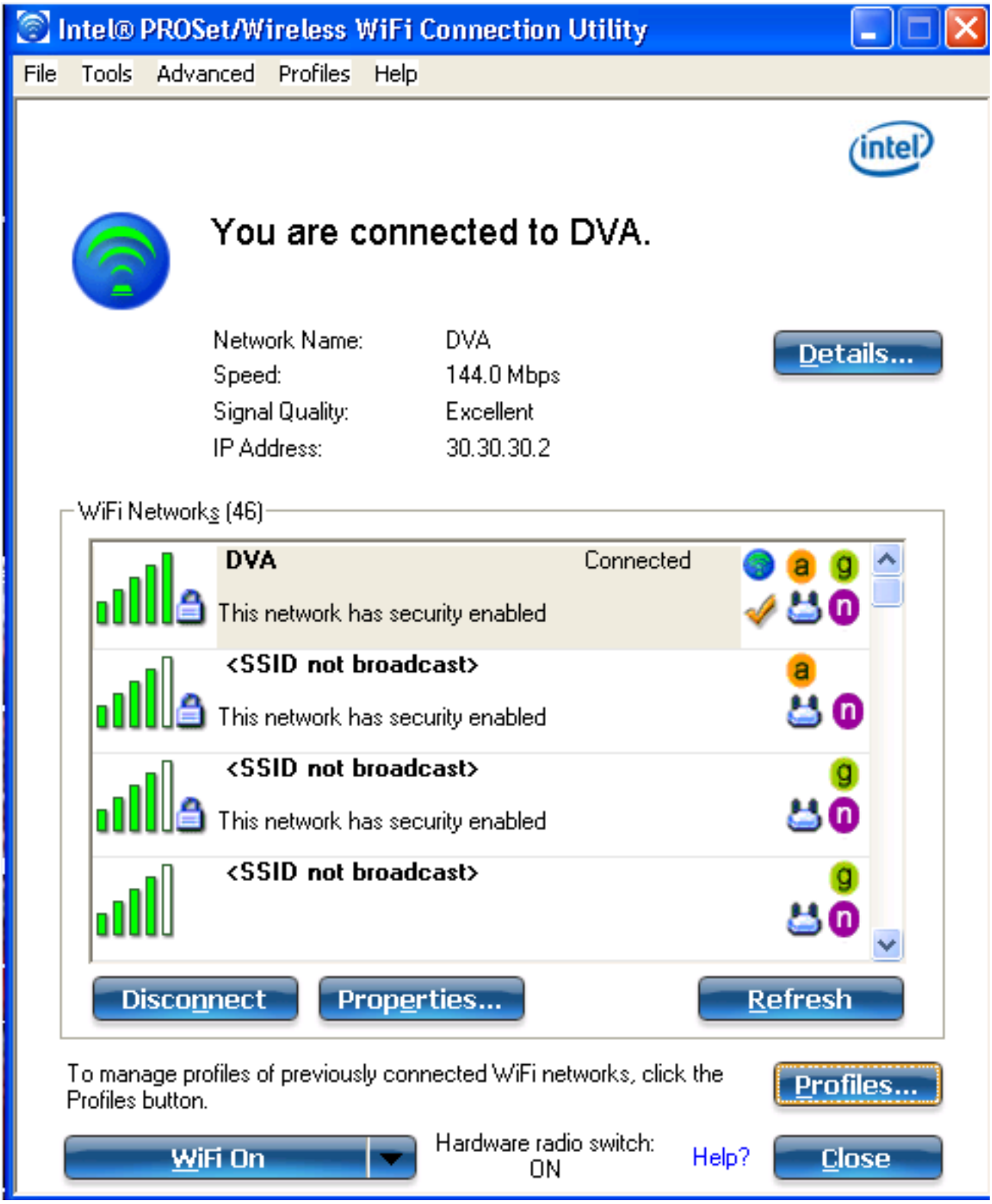
Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente. Estes são os processos de verificação:

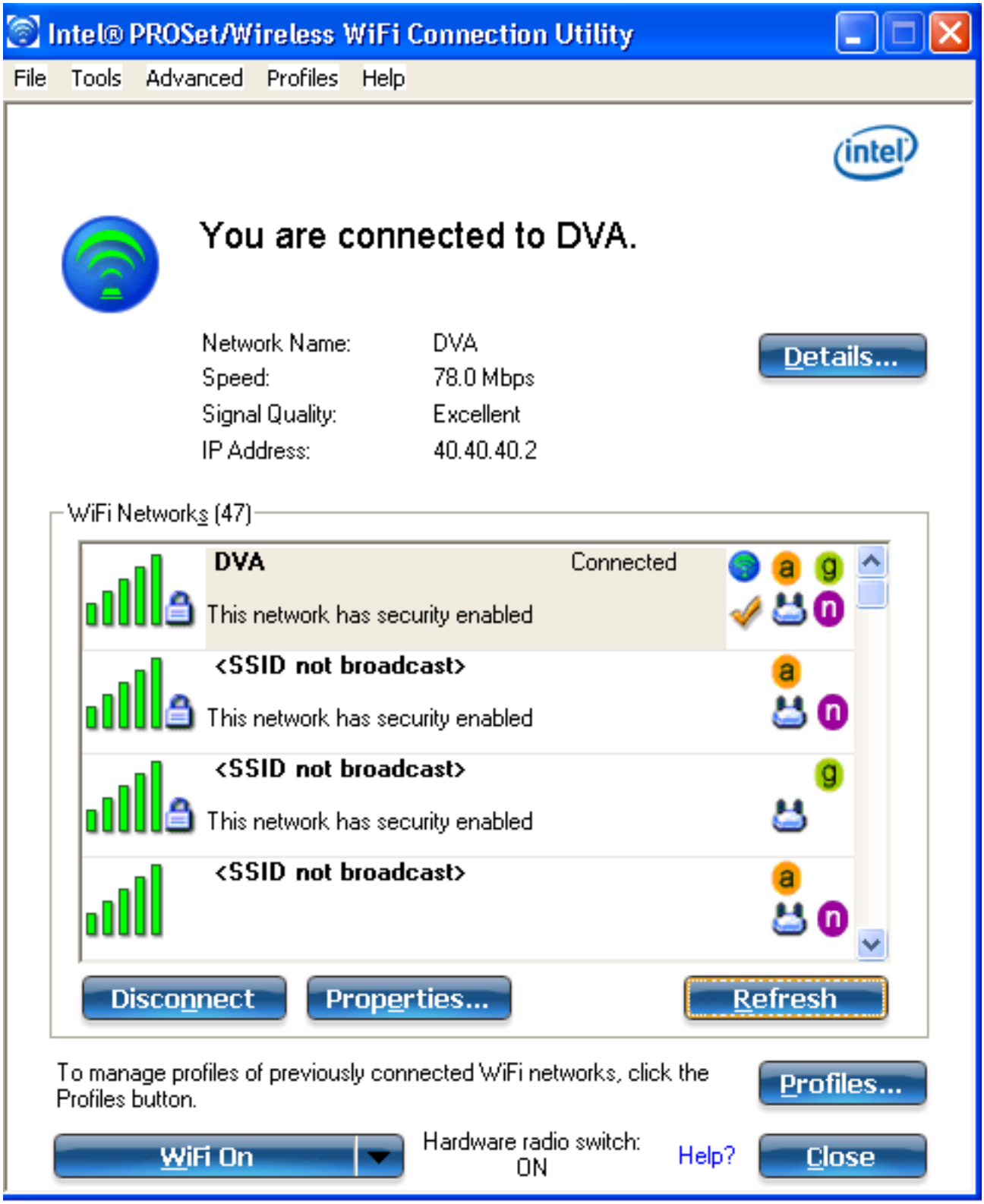
- Monitore a página no ACS que mostra quais clientes estão autenticados.



- Conecte-se à WLAN DVA com o grupo de alunos e examine o Utilitário de Conexão WiFi do cliente.



- Conecte-se à WLAN DVA com o grupo de professores e consulte o Utilitário de Conexão WiFi do cliente.



Troubleshoot

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

Notas:

Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

A ferramenta Output Interpreter (exclusiva para clientes registrados) é compatível com alguns comandos de exibição.. Use a ferramenta Output Interpreter para visualizar uma análise do resultado gerado pelo comando show..

Consulte Informações Importantes sobre Comandos de Depuração antes de usar comandos **debug.**

As depurações úteis incluem **debug client mac-address** *mac*, bem como estes comandos de rastreamento NGWC:

- **set trace group-wireless-client level debug**
- **set trace group-wireless-client filter mac** *xxxx.xxxx.xxxx*
- **show trace sys-filtrated-traces**

O rastreamento NGWC não inclui dot1x/AAA, portanto, use esta lista inteira de rastreamentos combinados para dot1x/AAA:

- **set trace group-wireless-client level debug**
- **set trace wcm-dot1x event level debug**
- **set trace wcm-dot1x aaa level debug**
- **set trace aaa wireless events level debug**
- **set trace access-session core sm level debug**
- **set trace access-session method dot1x level debug**
- **set trace group-wireless-client filter mac** *xxxx.xxxx.xxxx*
- **set trace wcm-dot1x event filter mac** *xxxx.xxxx.xxxx*
- **set trace wcm-dot1x aaa filter mac** *xxxx.xxxx.xxxx*
- **set trace aaa wireless events filter mac** *xxxx.xxxx.xxxx*
- **set trace access-session core sm filter mac** *xxxx.xxxx.xxxx*
- **set trace access-session method dot1x filter mac** *xxxx.xxxx.xxxx*
- **show trace sys-filtrated-traces**

Quando a atribuição de VLAN dinâmica está funcionando corretamente, você deve ver esse tipo de saída das depurações:

```
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)