使用NGWC和ACS 5.2配置动态VLAN分配

目录

简介

本文档介绍动态VLAN分配的概念。还介绍如何配置无线LAN控制器(WLC)和RADIUS服务器，以便将无线LAN(WLAN)客户端动态分配给特定VLAN。在本文档中，RADIUS服务器是运行Cisco安全访问控制系统版本5.2的访问控制服务器(ACS)。

先决条件

要求

Cisco 建议您了解以下主题：

- WLC和轻量接入点(LAP)的基本知识
- 身份验证、授权和记帐(AAA)服务器的功能知识
- 全面了解无线网络和无线安全问题

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 带Cisco IOS® XE软件版本3.2.2的Cisco 5760无线LAN控制器（下一代配线间或NGWC）
- 思科Aironet 3602系列轻量接入点
- Microsoft Windows XP，带Intel Proset请求方
- 思科安全访问控制系统版本5.2
- Cisco Catalyst 3560 系列交换机

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

使用 RADIUS 服务器执行动态 VLAN 分配

在大多数 WLAN 系统中，每个 WLAN 都有适用于与服务集标识符 (SSID) 关联的所有客户端的静态策略，即以控制器术语表示 WLAN。虽然此方法功能强大，但也具有局限性，这是因为，它要求客户端与不同的 SSID 相关联以便继承不同的 QoS 和安全策略。

然而，Cisco WLAN 解决方案支持网络标识。这允许网络通告单个SSID，但允许特定用户根据用户凭证继承不同的QoS、VLAN属性和/或安全策略。

动态 VLAN 分配便是一项这样的功能，它根据无线用户提供的凭证将该用户置于特定 VLAN 中。用户分配到特定VLAN的此任务由RADIUS身份验证服务器（如Cisco Secure ACS）处理。例如，此功能可用于允许无线主机在园区网络内移动时保留在同一VLAN中。

因此，当客户端尝试与向控制器注册的LAP关联时，LAP会将用户的凭证传递到RADIUS服务器进行验证。成功执行身份验证后，RADIUS 服务器便会将某些 Internet 工程任务组 (IETF) 属性传递给用户。这些 RADIUS 属性确定应该分配给无线客户端的 VLAN ID。客户端的SSID（WLAN，就WLC而言）并不重要，因为用户始终被分配到此预定VLAN ID。

用于 VLAN ID 分配的 RADIUS 用户属性包括：

- IETF 64（隧道类型）— 设置为VLAN。
- IETF 65（隧道中型）— 设置为802。
- IETF 81(Tunnel-Private-Group-ID) — 设置为VLAN ID。

VLAN ID为12位，值介于1和4094之间（含1和4094）。由于Tunnel-Private-Group-ID的类型为字符串(如RFC 2868、RADIUS Attributes for Tunnel Protocol Support中所定义)，因此VLAN ID整数值将编码为字符串。当发送这些隧道属性时，需要填写 Tag 字段。

如 RFC2868 的 3.1 部分中所述：

"Tag字段长度为一个二进制八位数，旨在提供在指向同一隧道的同一数据包中对属性进行分组的方法。"

“标记”(Tag)字段的有效值为0x01至0x1F（含0x01至0x1F）。如果未使用 Tag 字段，则它一定为零(0x00)。 有关所有 RADIUS 属性的详细信息，请参阅 RFC 2868。

配置

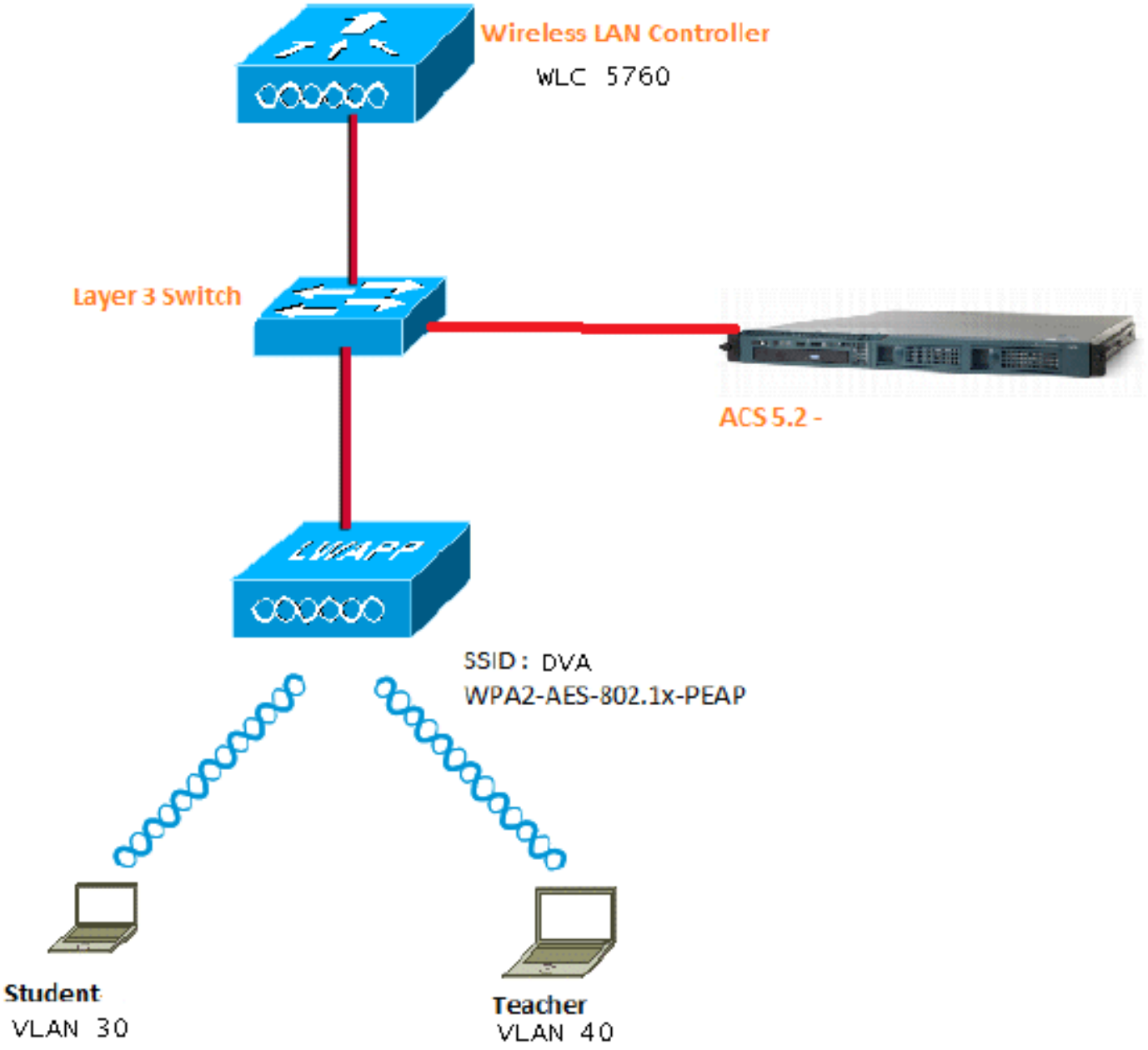
动态VLAN分配的配置由两个不同的步骤组成：

1. 使用命令行界面(CLI)或GUI配置WLC。
2. 配置 RADIUS 服务器。

注意：使用命令查找工具（仅限注册用户）可获取有关本部分所使用命令的详细信息。

网络图

本文档使用以下网络设置：



本文档使用带有受保护可扩展身份验证协议(PEAP)的802.1X作为安全机制。

假设

- 交换机配置为所有第3层(L3)VLAN。
- 为DHCP服务器分配了DHCP范围。
- 网络中所有设备之间都存在L3连接。
- LAP已加入WLC。
- 每个VLAN都有/24掩码。
- ACS 5.2安装了自签名证书。

使用CLI配置WLC

配置WLAN

以下是使用SSID DVA配置WLAN的示例：

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

在WLC上配置RADIUS服务器

以下是WLC上RADIUS服务器配置的示例：

```
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
```

为客户端VLAN配置DHCP池

以下是客户端VLAN 30和VLAN 40的DHCP池配置示例：

```
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
```

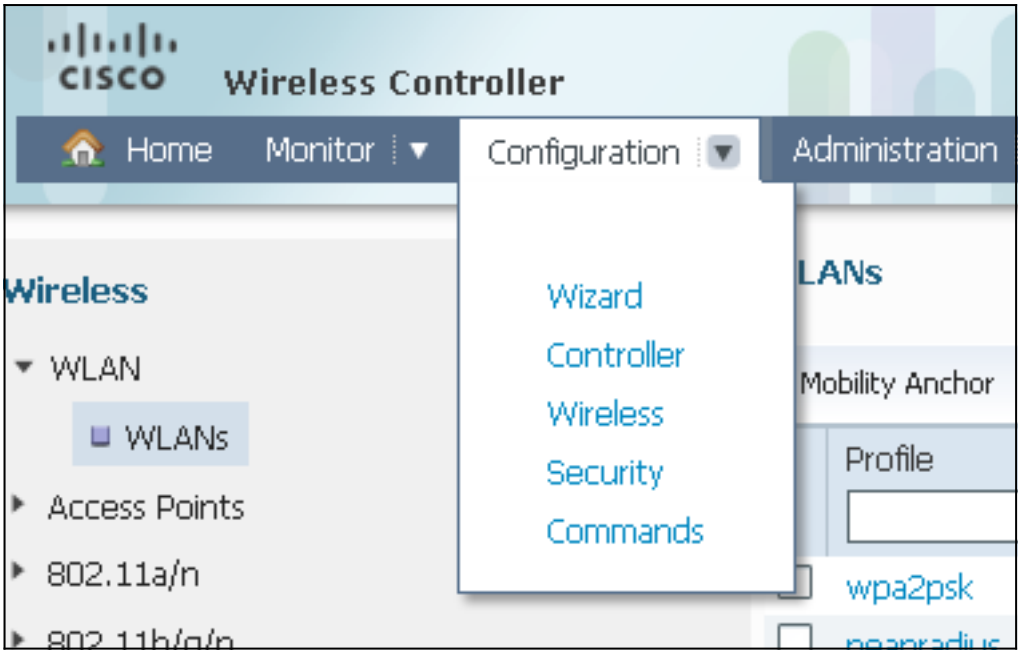
```
!
ip dhcp pool vlan40
 network 40.40.40.0 255.255.255.0
 default-router 40.40.40.1

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

使用GUI配置WLC

配置WLAN

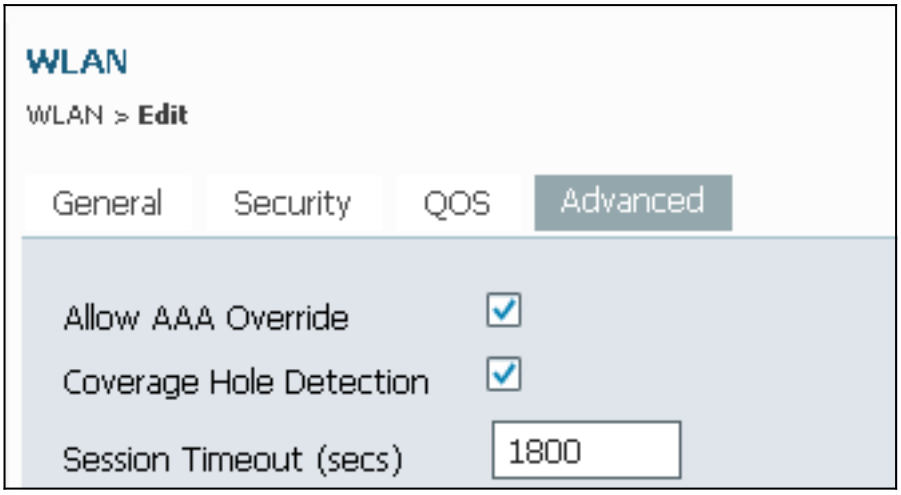
此过程描述如何配置WLAN。

1. 导航至**Configuration > Wireless > WLAN > NEW** 选项卡。

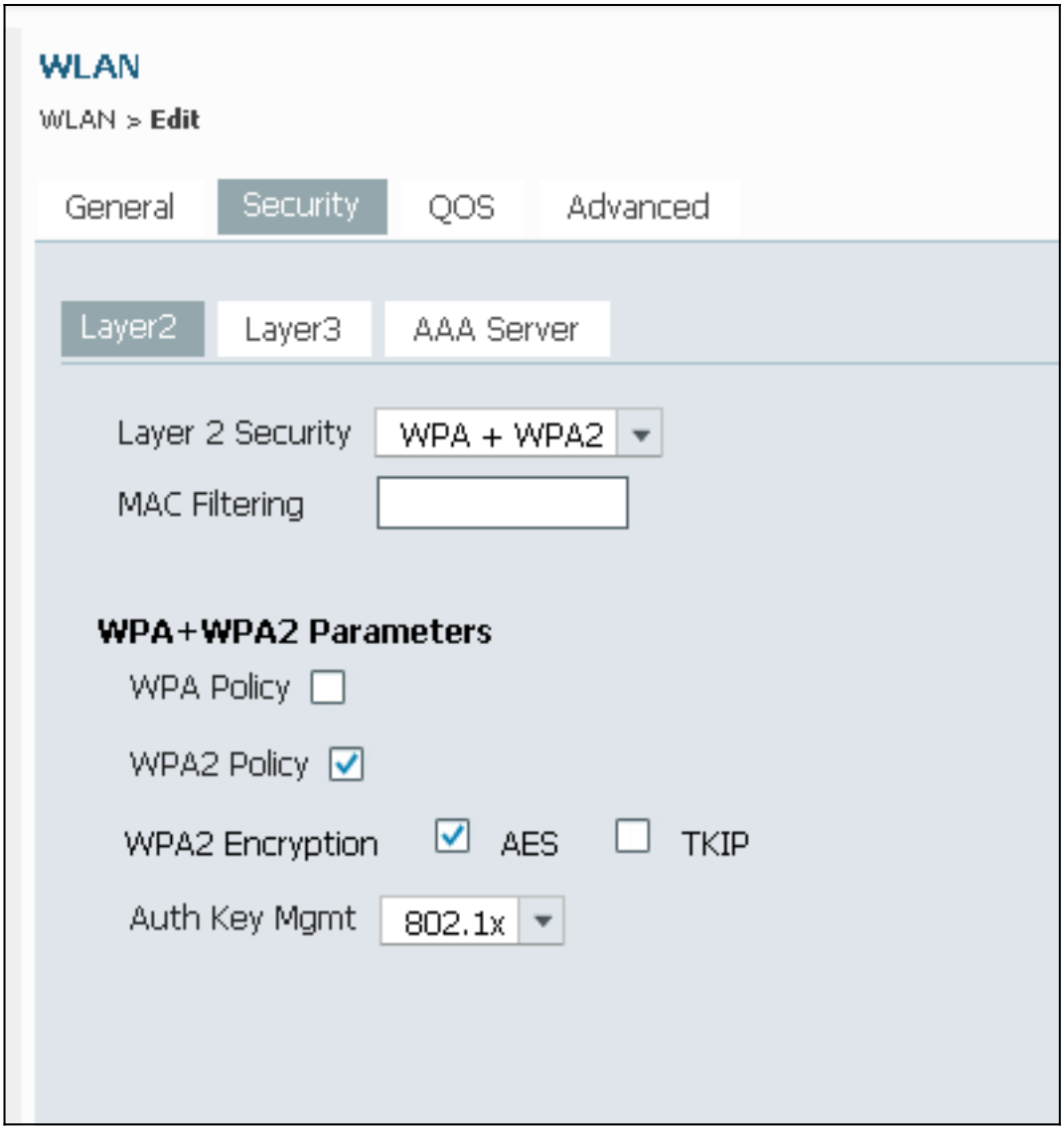


2. 单击**General**选项卡，查看WLAN是否配置为WPA2-802.1X，并将接口/接口组(G)映射到VLAN 20(**VLAN0020**)。

3. 单击“高级”选项卡，然后选中“允许AAA覆盖”复选框。必须启用覆盖才能使此功能正常工作。



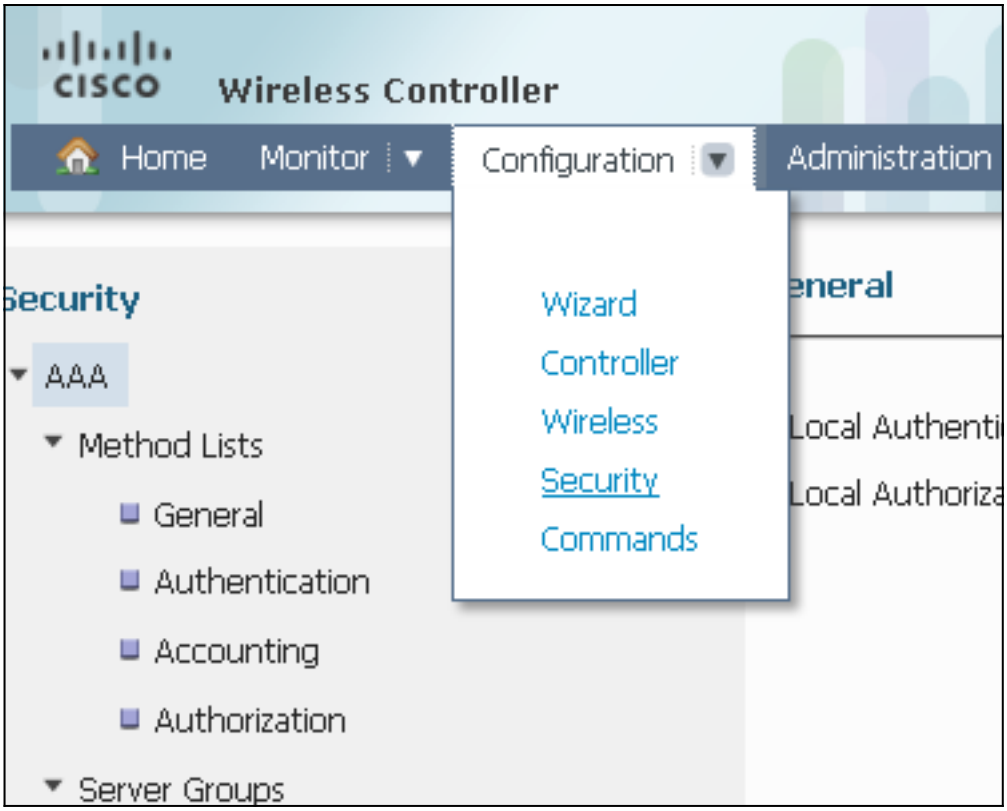
4. 单击Security选项卡和Layer2选项卡，选中WPA2 Encryption AES复选框，然后从Auth Key Mgmt下拉列表中选择802.1x。



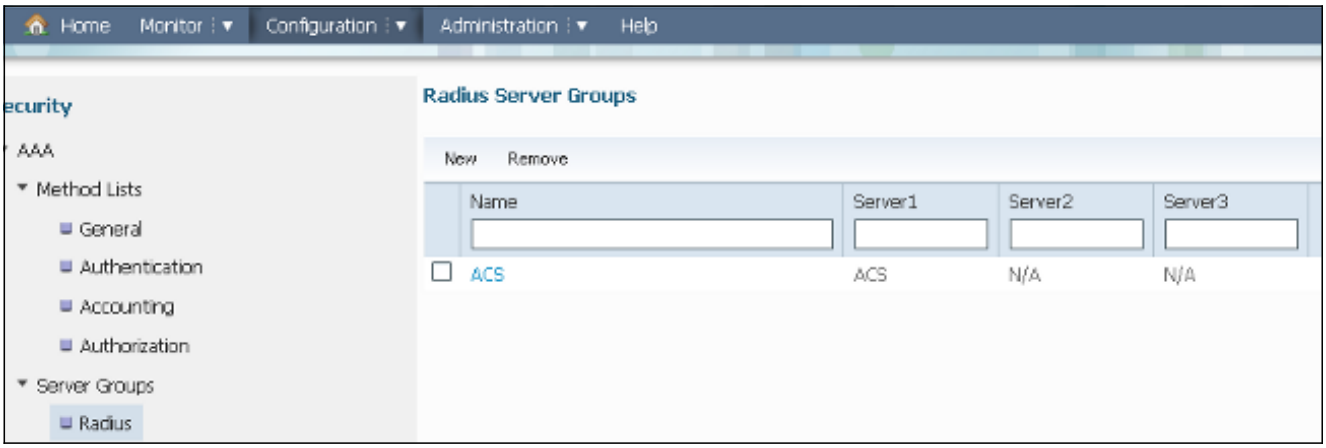
在WLC上配置RADIUS服务器

此过程介绍如何在WLC上配置RADIUS服务器。

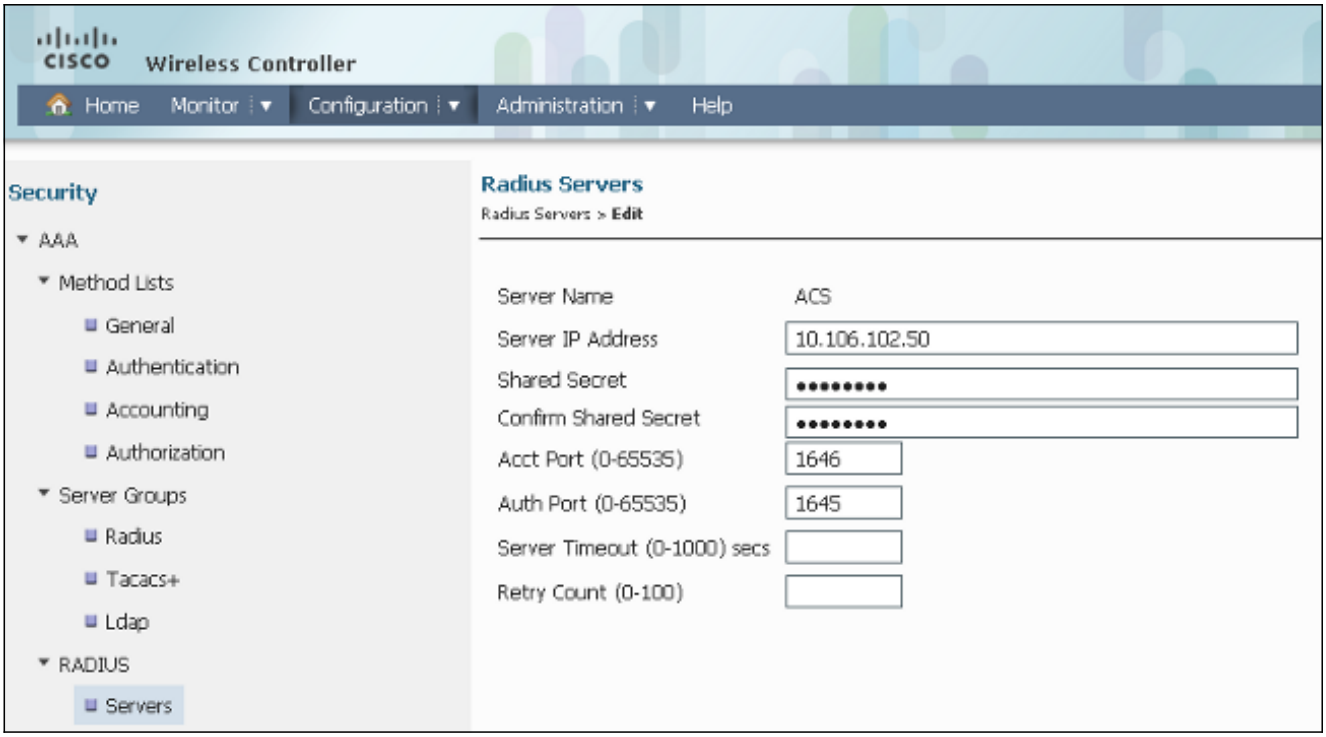
1. 导航至**配置>安全选**项卡。



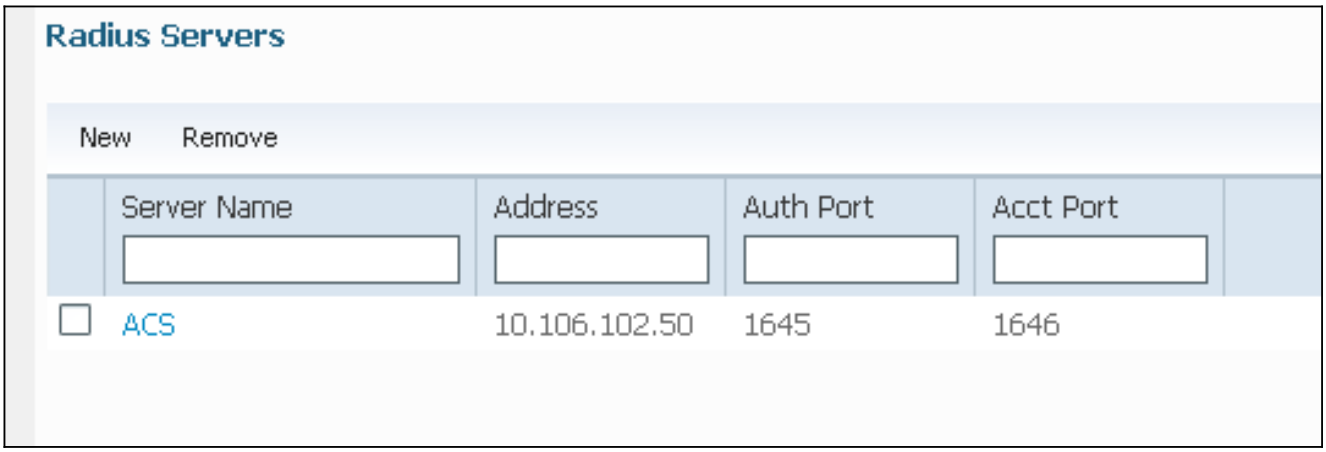
2. 导航到**AAA > Server Groups > Radius**以创建Radius服务器组。在本例中，Radius服务器组称为ACS。



3. 编辑Radius服务器条目以添加服务器IP地址和共享密钥。此共享密钥必须与WLC和RADIUS服务器上的共享密钥匹配。



以下是完整配置的示例：

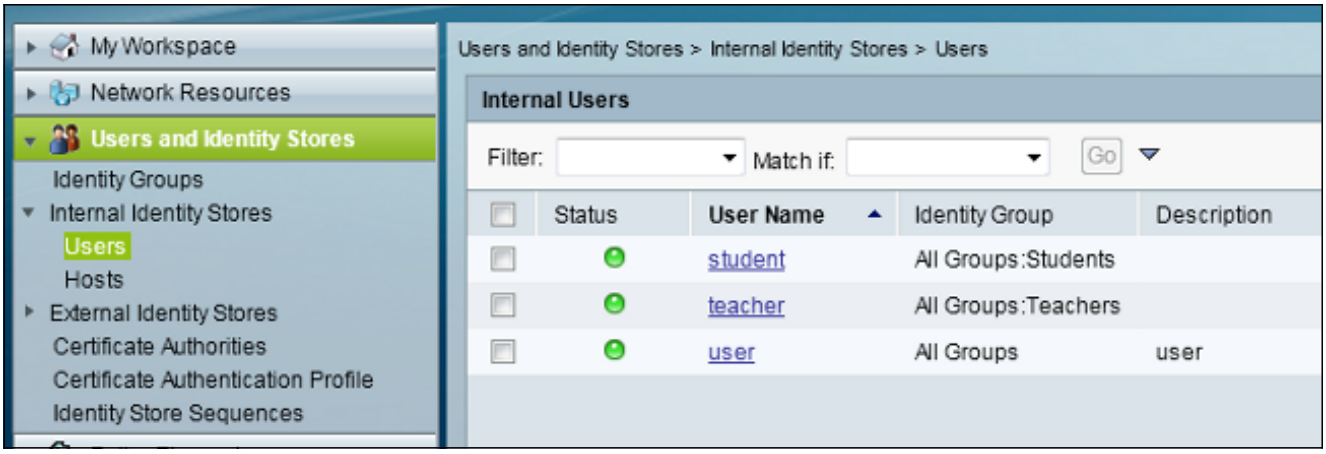


配置RADIUS服务器

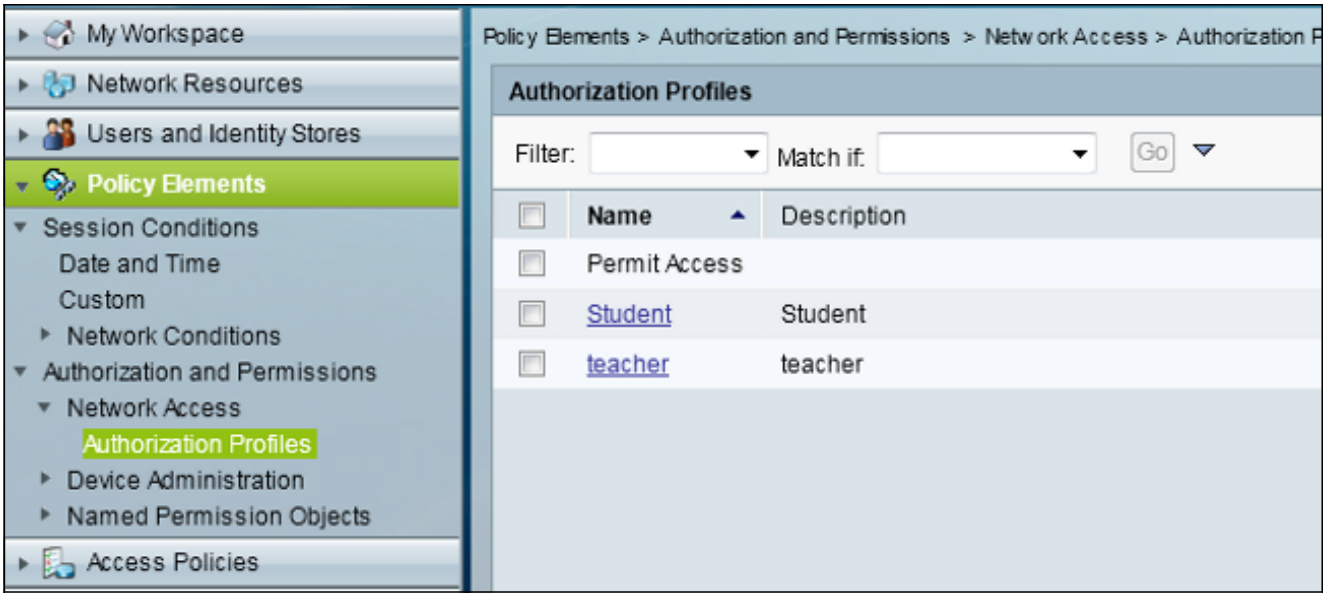
此过程介绍如何配置RADIUS服务器。

1. 在RADIUS服务器上，导航**到用户和身份**库**>内部身份**库**>用户**。

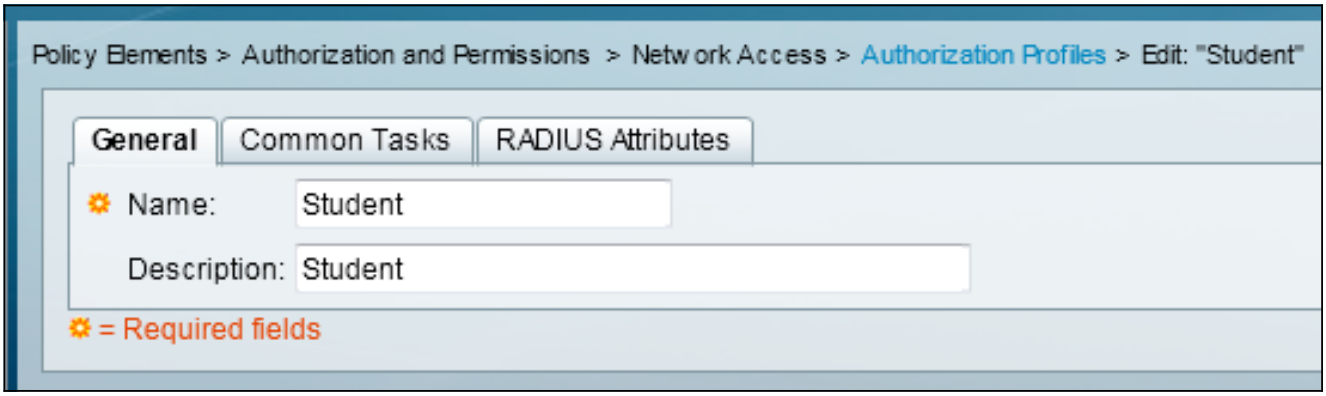
2. 创建适当的用户名和身份组。在本例中，它是“学生”和“所有组：学生”和“教师”和“所有组：教师”。



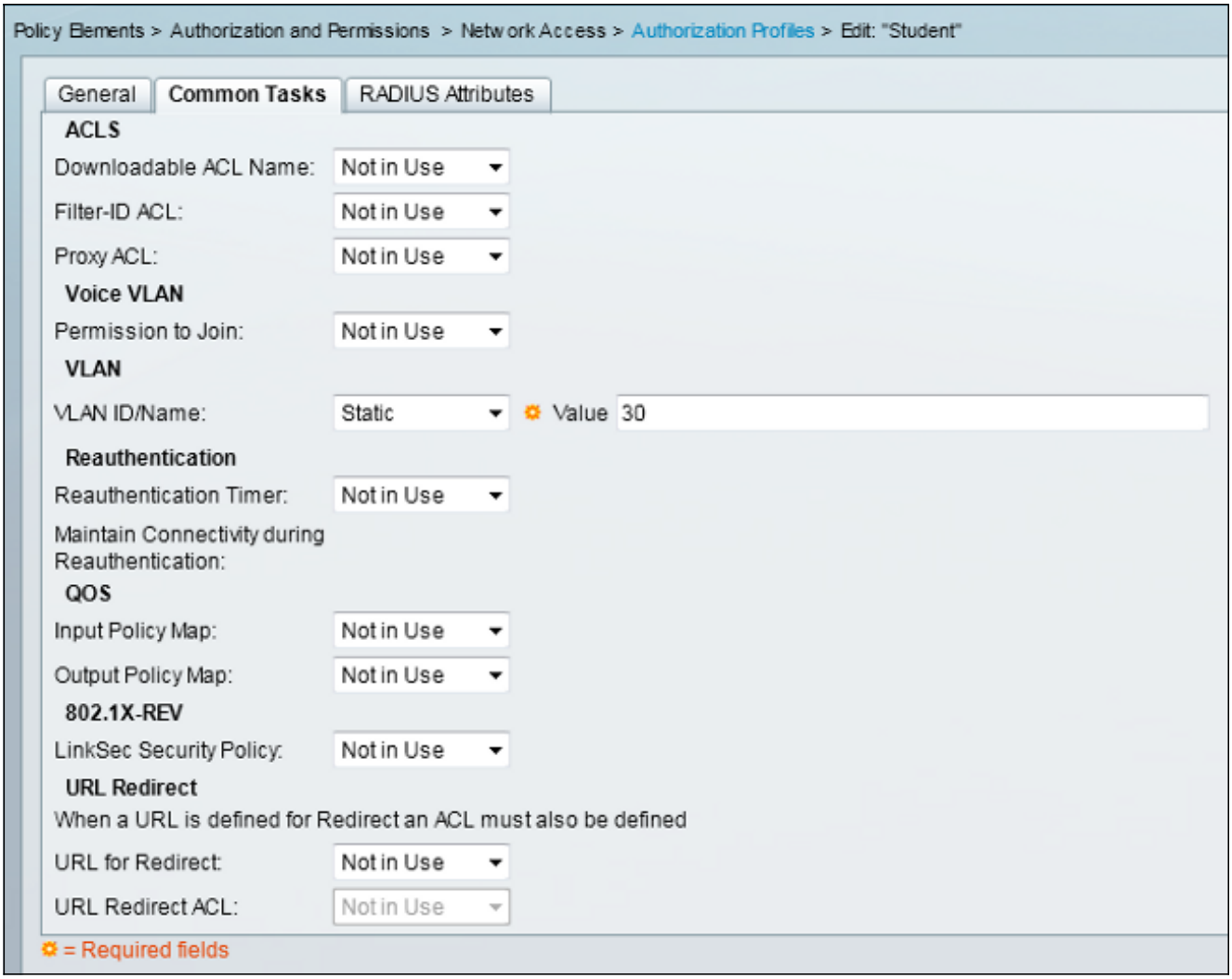
3. 导航至**策略元素 > 授权和权限 > 网络访问 > 授权配置文件**，并为AAA覆盖创建授权配置文件。



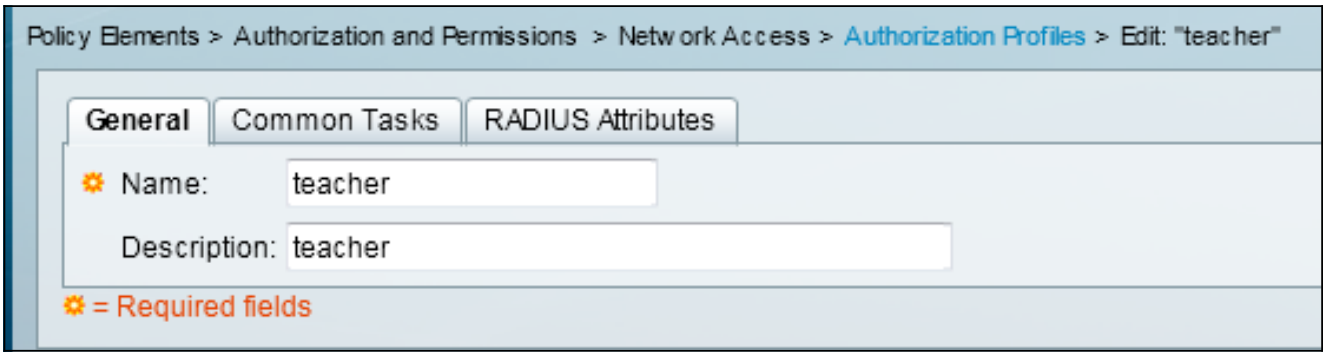
4. 编辑学生的授权配置文件。



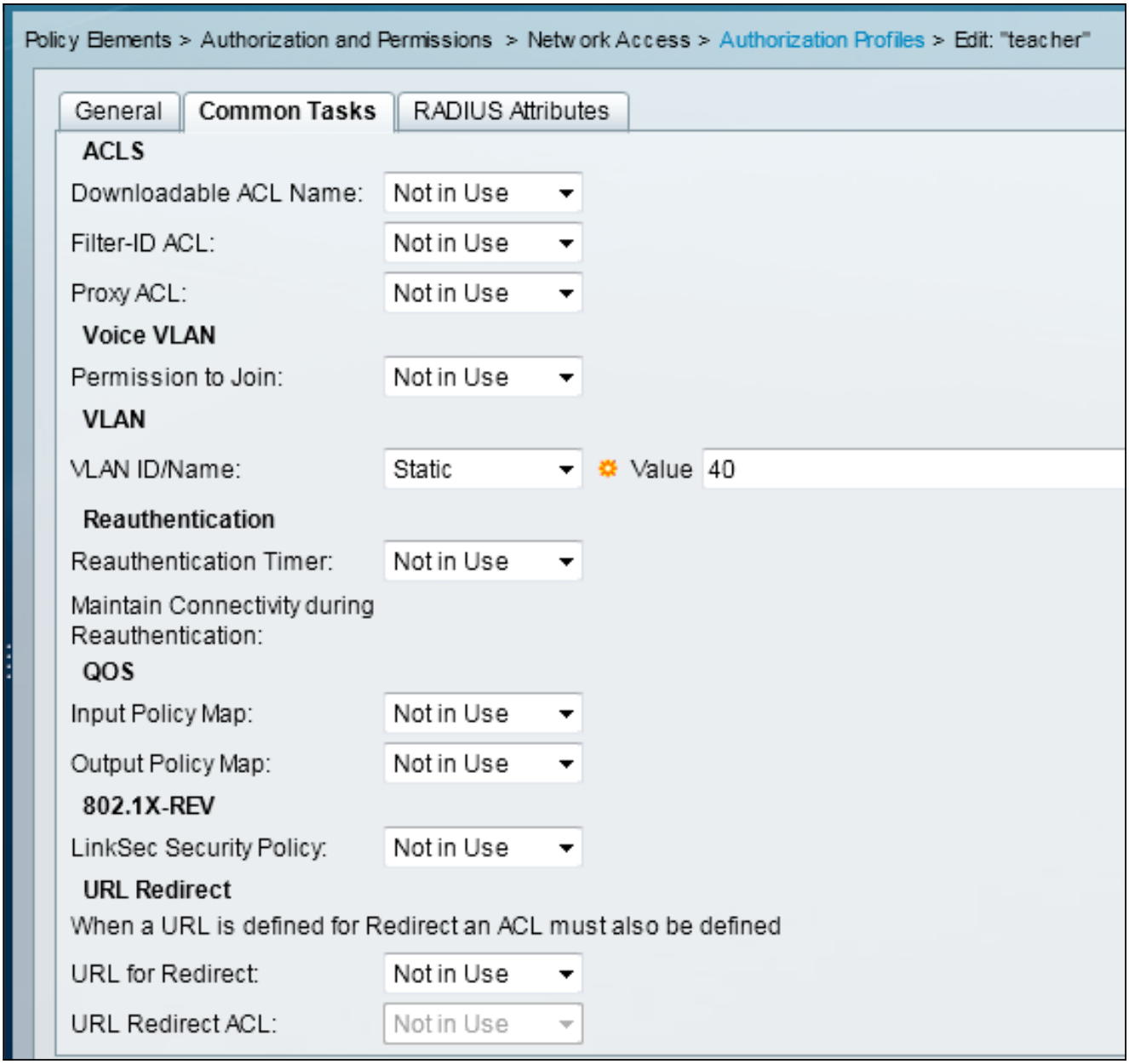
5. 将VLAN ID/Name设置为**Static**，值为**30**(VLAN 30)。



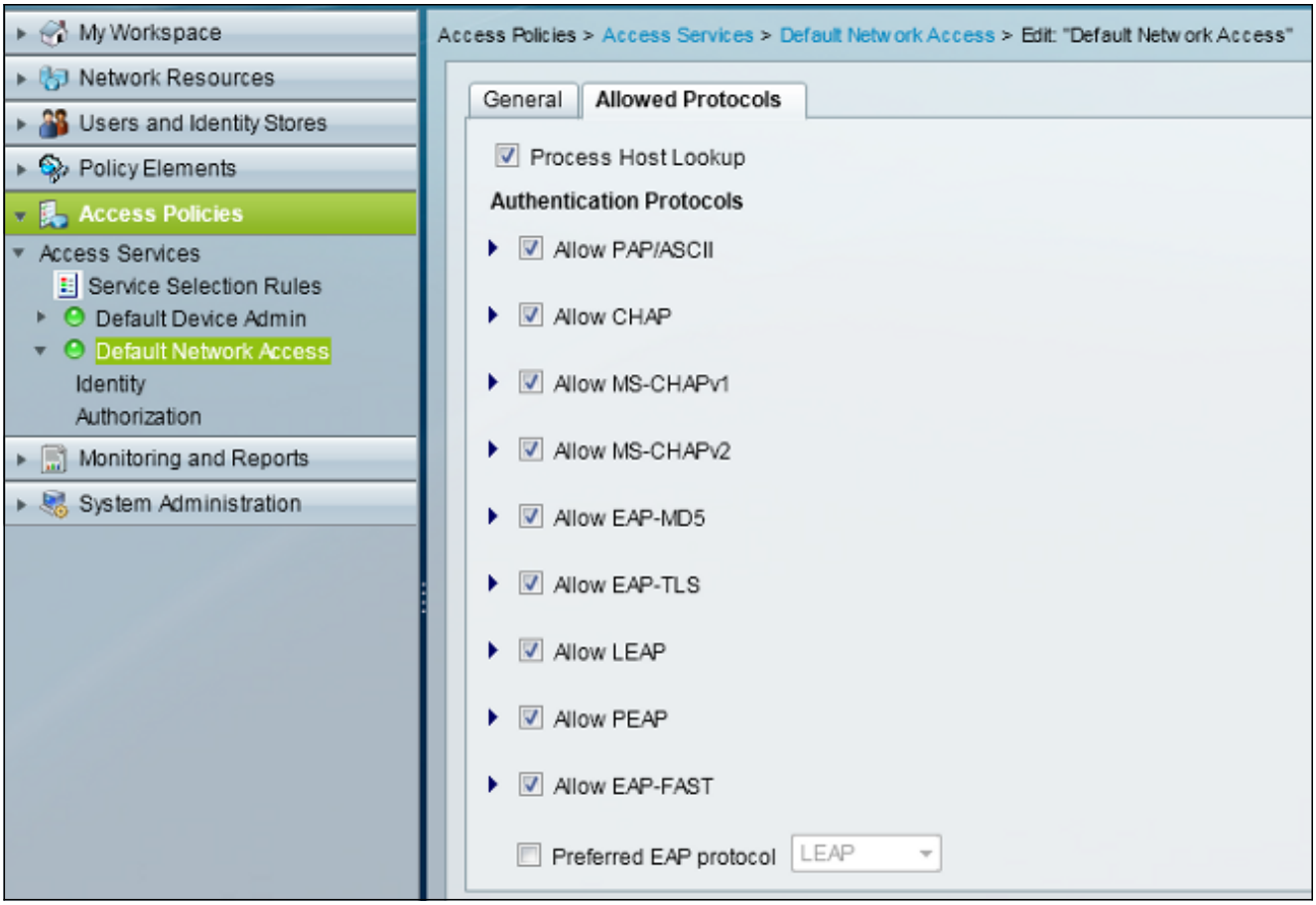
6. 编辑教师的授权配置文件。



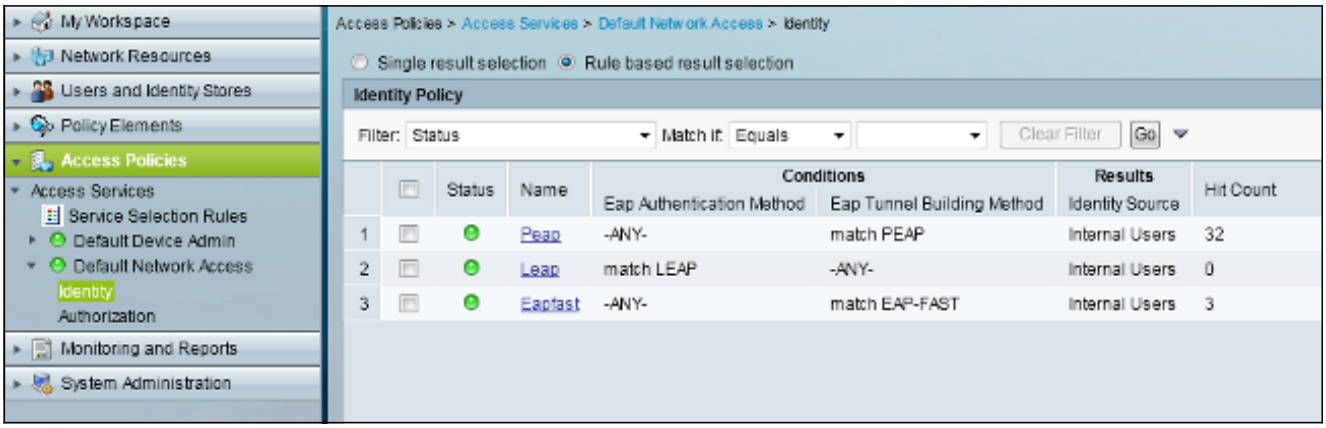
7. 将VLAN ID/Name设置为**Static**，值为40(**VLAN** 40)。



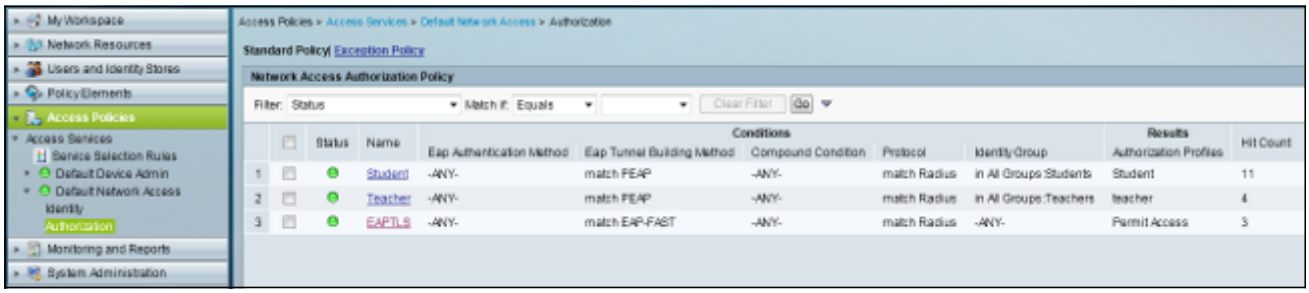
8. 导航至**Access Policies > Access Services > Default Network Access**，然后单击**Allowed Protocols**选项卡。选中“**允许PEAP**”复选框。



9. 导航至**Identity**，并定义规则以允许PEAP用户。



10. 导航至**授权**，并将学生和教师映射到授权策略；在本例中，映射应为VLAN 30的Student和VLAN 40的Teacher。

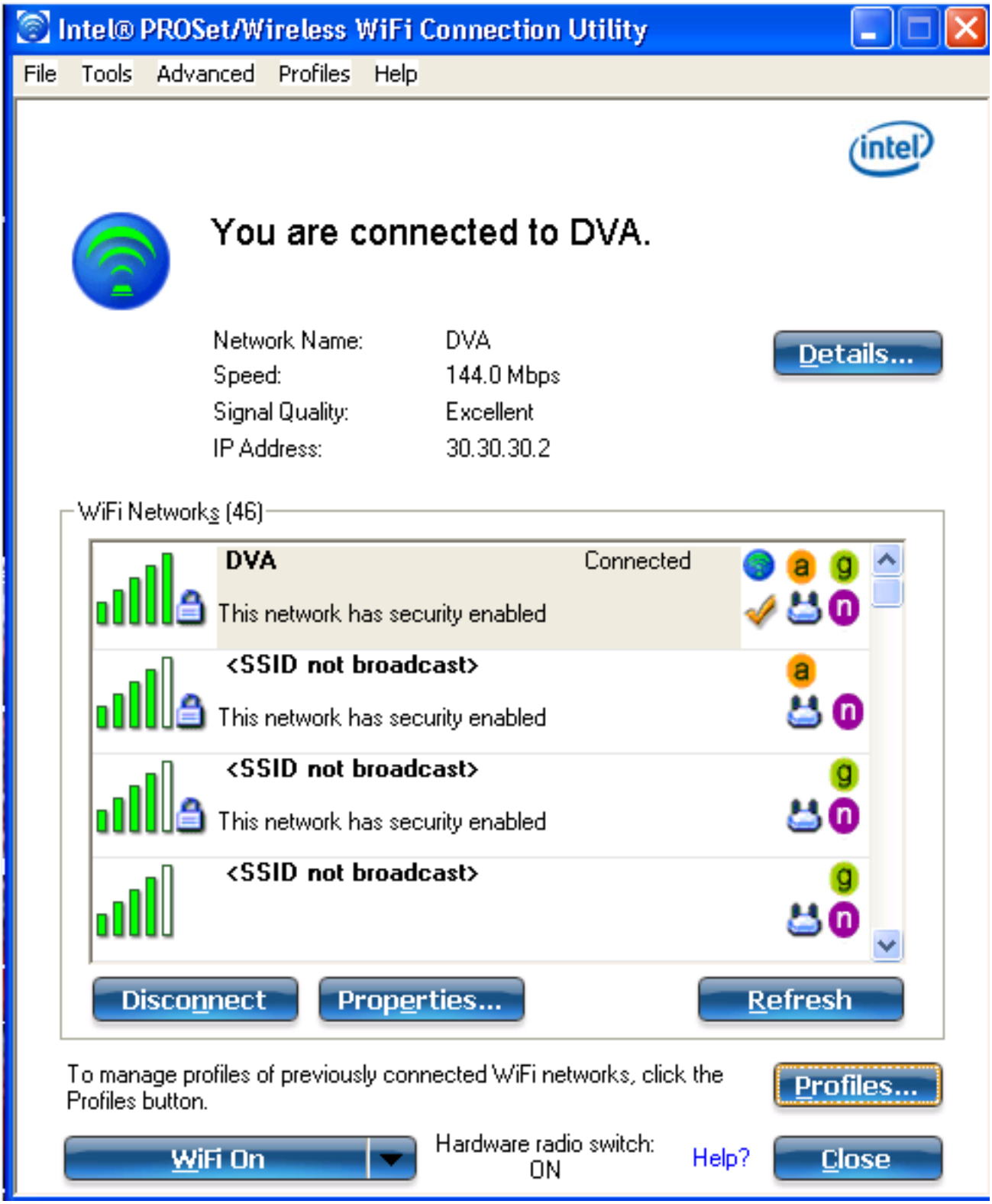


验证

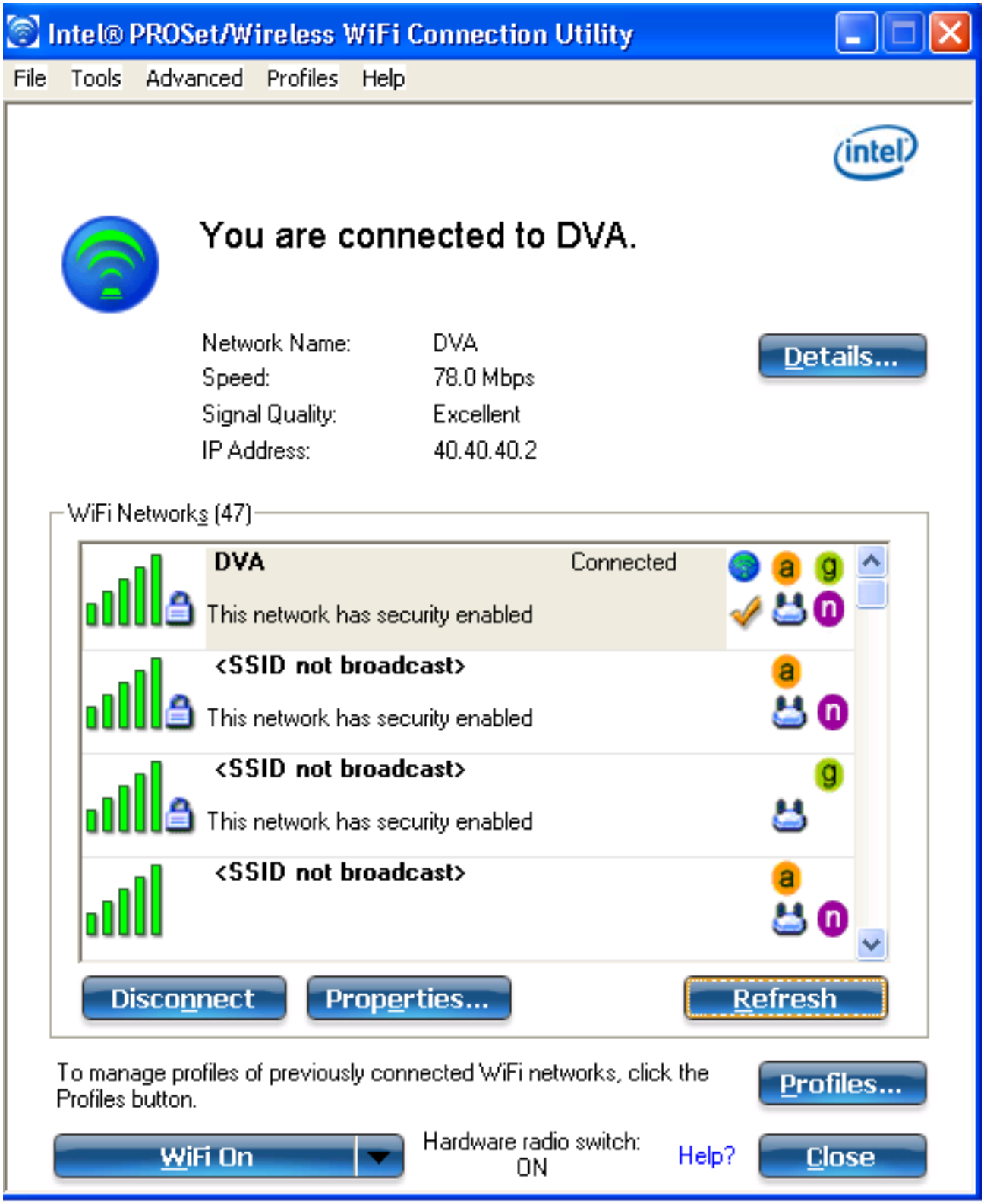
使用本部分可确认配置能否正常运行。以下是验证过程：

- 监控ACS上显示哪些客户端经过身份验证的页面。

- 使用学生组连接到DVA WLAN，并查看客户端WiFi连接实用程序。



- 使用教师组连接到DVA WLAN，并查看客户端WiFi连接实用程序。



故障排除

本部分提供的信息可用于对配置进行故障排除。

注意：

使用命令查找工具（仅限注册用户）可获取有关本部分所使用命令的详细信息。

命令输出解释程序工具（仅限注册用户）支持某些 **show 命令。**使用输出解释器工具来查看

show 命令输出的分析。

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

有用的调试包**括debug client mac-address** *mac*，以及以下NGWC跟踪命令：

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

NGWC跟踪不包括dot1x/AAA，因此请对dot1x/AAA使用以下整个组合跟踪列表：

- **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**
- **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-filtered-traces**

当动态VLAN分配正常工作时，您应该会从调试中看到以下类型的输出：

```
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)
```