使用NGWC和ACS 5.2配置動態VLAN分配

目錄

簡介

本檔案介紹動態VLAN分配的概念。其中也說明如何設定無線LAN控制器(WLC)和RADIUS伺服器，以動態地將無線LAN(WLAN)使用者端指派給特定VLAN。在本文檔中，RADIUS伺服器是運行思科安全訪問控制系統5.2版的訪問控制伺服器(ACS)。

必要條件

需求

思科建議您瞭解以下主題：

- WLC和輕量型存取點(LAP)的基本知識
- 身份驗證、授權和記帳(AAA)伺服器的功能知識
- 全面瞭解無線網路和無線安全問題

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 採用Cisco IOS® XE軟體版本3.2.2的Cisco 5760無線LAN控制器（下一代配線間，或NGWC）
- Cisco Aironet 3602系列輕量型存取點
- 採用Intel Proset Supplicant客戶端的Microsoft Windows XP
- 思科安全存取控制系統版本5.2
- Cisco Catalyst 3560系列交換器

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

使用RADIUS伺服器進行動態VLAN指派

在大多數WLAN系統中，每個WLAN都有一個靜態策略，該策略適用於與服務集識別符號(SSID)或控制器術語中的WLAN相關聯的所有客戶端。此方法雖然功能強大，但也有侷限性，因為它要求客戶端與不同的SSID關聯以繼承不同的QoS和安全策略。

但是，Cisco WLAN解決方案支援身份網路。這允許網路通告單個SSID，但允許特定使用者根據使用者憑證繼承不同的QoS、VLAN屬性和/或安全策略。

動態VLAN分配是一種功能，可根據使用者提供的憑證將無線使用者置於特定VLAN中。使用者分配到特定VLAN的任務由RADIUS身份驗證伺服器（例如Cisco Secure ACS）處理。例如，此功能可用於允許無線主機在園區網路中移動時保持在同一個VLAN上。

因此，當客戶端嘗試與註冊到控制器的LAP關聯時，LAP會將使用者的憑證傳遞到RADIUS伺服器進行驗證。驗證成功後，RADIUS伺服器會將某些Internet工程工作小組(IETF)屬性傳遞給使用者。這些RADIUS屬性決定應分配給無線客戶端的VLAN ID。使用者端的SSID（WLAN，從WLC的角度而言）並不重要，因為系統總是將使用者指派給此預先確定的VLAN ID。

用於VLAN ID分配的RADIUS使用者屬性包括：

- IETF 64（隧道型別） — 設定為VLAN。
- IETF 65（隧道介質型別） — 設定為802。
- IETF 81(Tunnel-Private-Group-ID) — 設定為VLAN ID。

VLAN ID為12位，取值範圍為1到4094（含1）。由於Tunnel-Private-Group-ID是字串型別(如RFC 2868，隧道協定支援的RADIUS屬性中所定義)，用於與IEEE 802.1X一起使用，因此VLAN ID整數值被編碼為字串。傳送這些隧道屬性時，需要填寫Tag欄位。

如RFC2868第3.1節所述：

「Tag（標籤）欄位的長度是一個二進位制八位數，它旨在提供一種方法，用於將引用同一隧道的同一資料包中的屬性分組。」

「標籤」欄位的有效值為0x01到0x1F（包括0x1F）。如果「標籤」欄位未使用，則該欄位必須為零(0x00)。 如需所有RADIUS屬性的詳細資訊，請參閱RFC 2868。

設定

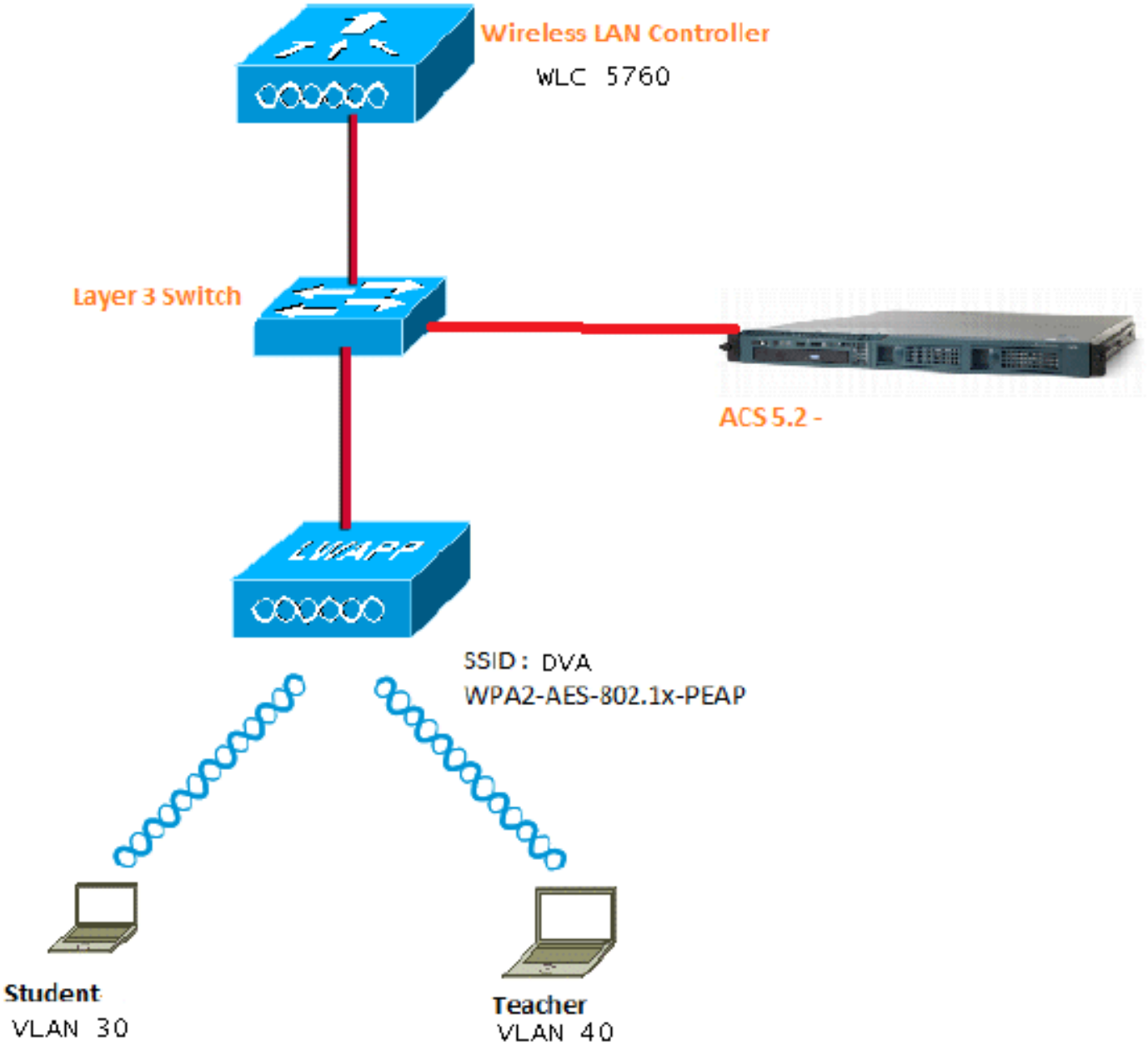
動態VLAN分配的配置包括兩個不同的步驟：

1. 使用命令列介面(CLI)或GUI配置WLC。
2. 設定RADIUS伺服器。

附註：使用命令查詢工具(僅供已註冊客戶使用)可獲取本節中使用的命令的更多資訊。

網路圖表

本檔案會使用以下網路設定：



本文使用具有受保護的可擴充驗證通訊協定(PEAP)的802.1X作為安全機制。

假設

- 交換器設定為所有第3層(L3)VLAN。
- 為DHCP伺服器分配DHCP作用域。
- 網路中所有裝置之間都存在L3連線。
- LAP已連線到WLC。
- 每個VLAN都有一個/24掩碼。
- ACS 5.2已安裝自簽名證書。

使用CLI設定WLC

設定WLAN

以下示例說明如何使用SSID DVA配置WLAN:

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

設定WLC上的RADIUS伺服器

以下是在WLC上設定RADIUS伺服器的範例：

```
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
```

配置客戶端VLAN的DHCP池

以下是客戶端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
```

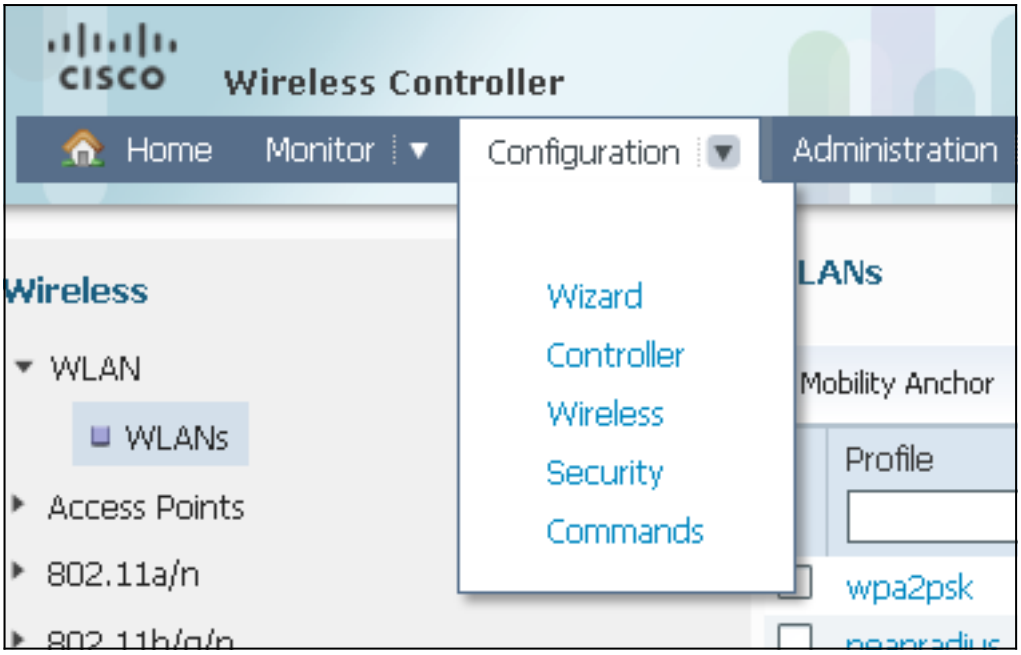
```
!
ip dhcp pool vlan40
 network 40.40.40.0 255.255.255.0
 default-router 40.40.40.1

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

使用GUI設定WLC

設定WLAN

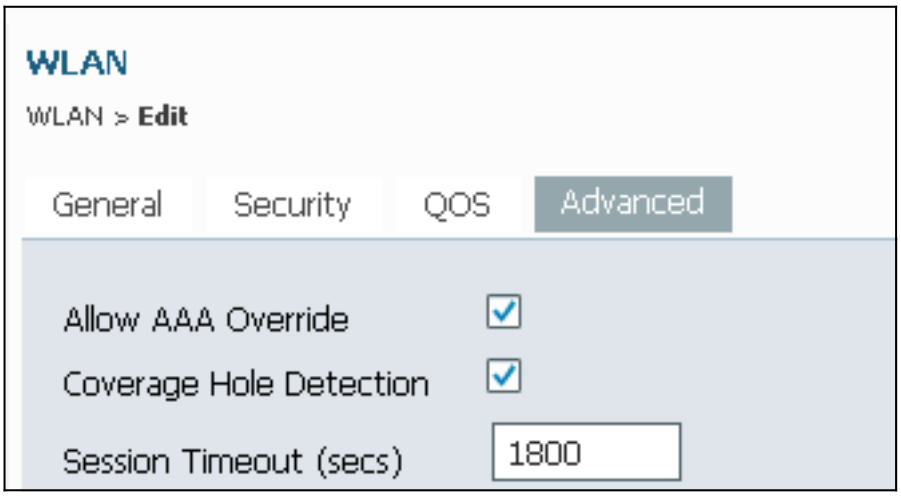
以下步驟說明如何配置WLAN。

1. 導覽至**Configuration > Wireless > WLAN > NEW**索引標籤。

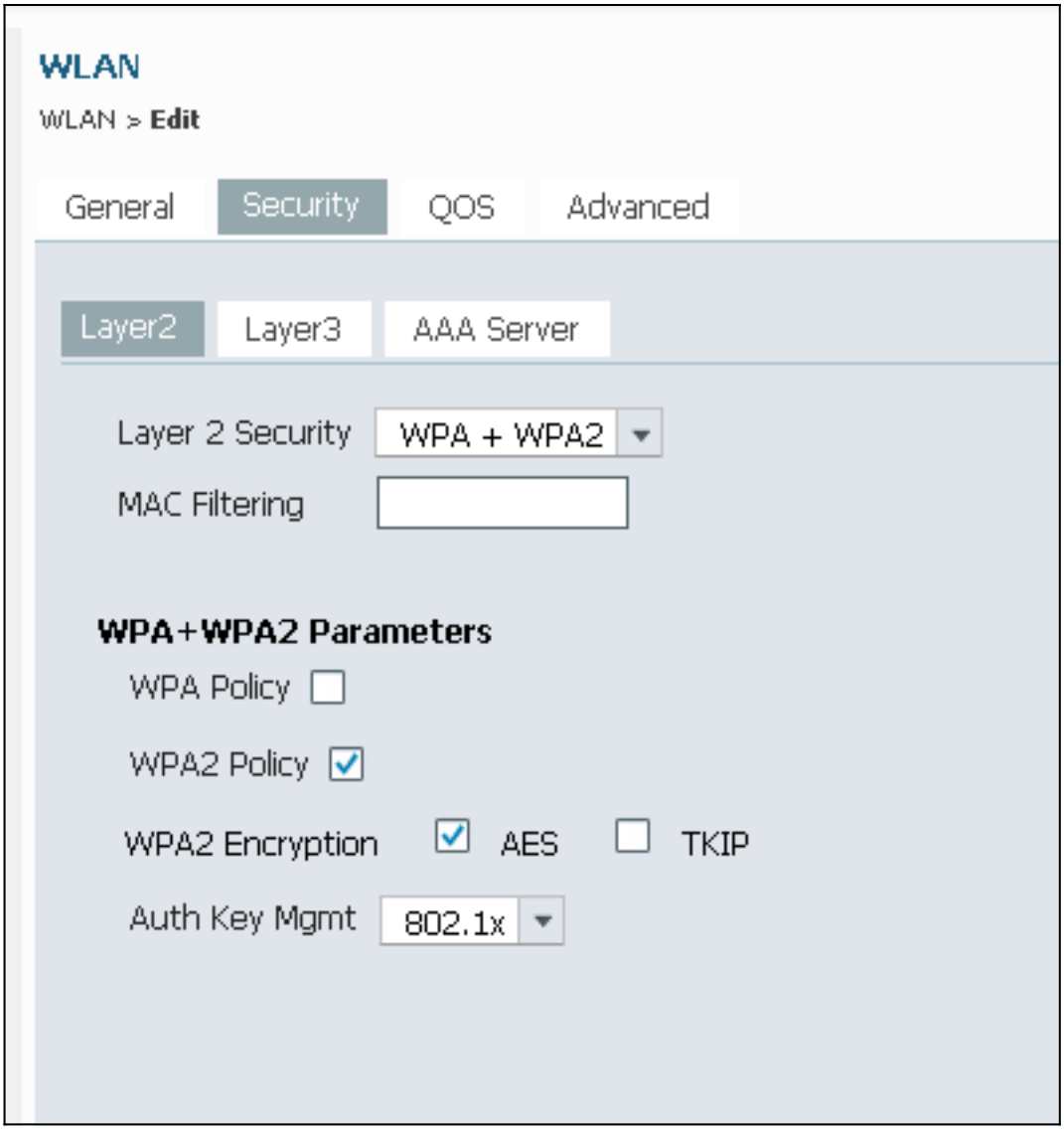


2. 按一下**General**頁籤，檢視WLAN已配置為WPA2-802.1X，並將介面/介面組(G)對映到VLAN 20(**VLAN0020**)。

3. 按一下**Advanced**頁籤，然後選中**Allow AAA Override**覈取方塊。必須啟用覆蓋才能使用此功能。



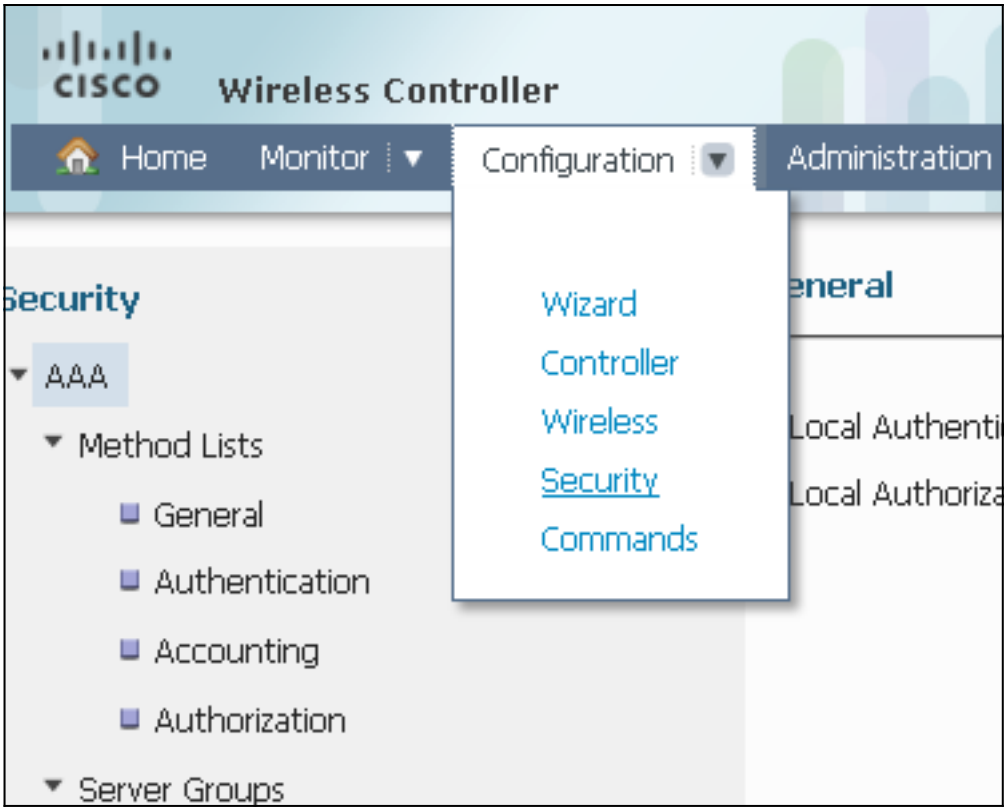
4. 按一下**Security**頁籤和**Layer2**頁籤，選中WPA2加密**AES**覈取方塊，然後從Auth Key Mgmt下拉選單中選擇**802.1x**。



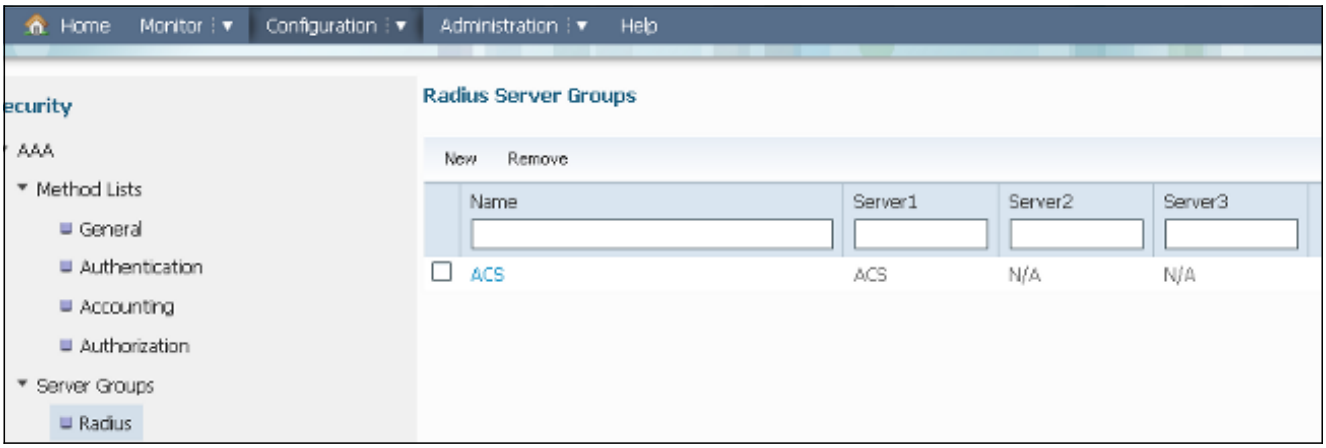
設定WLC上的RADIUS伺服器

以下程式介紹如何在WLC上設定RADIUS伺服器。

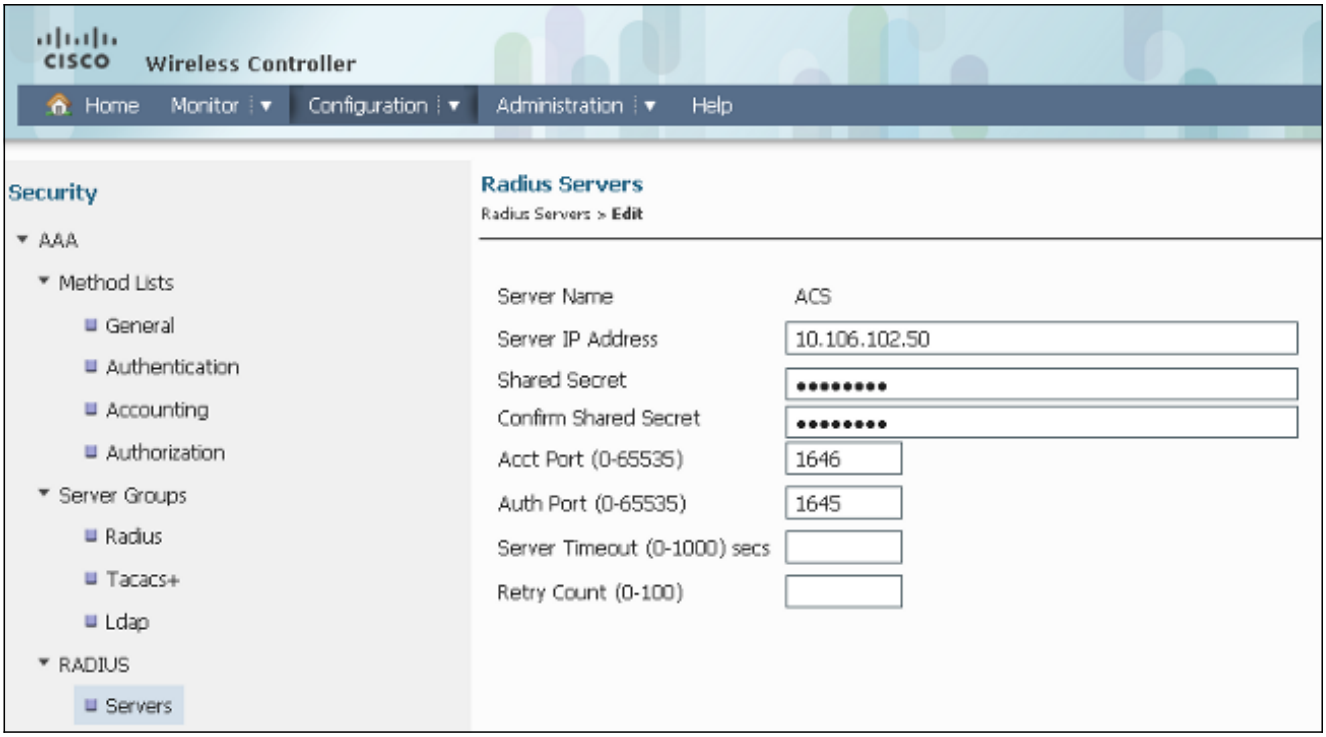
1. 導覽至**Configuration > Security**索引標籤。



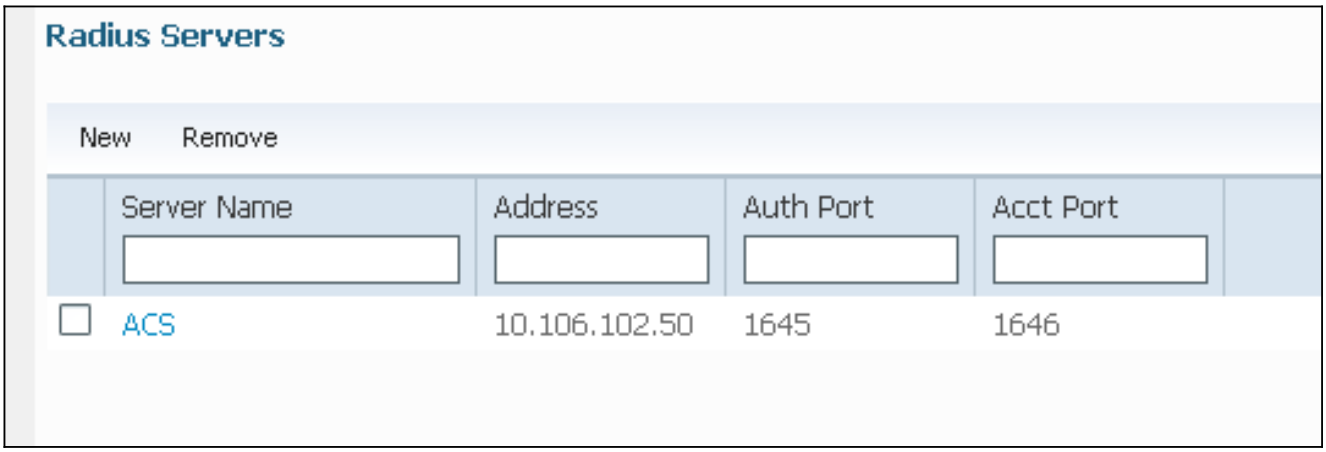
2. 導覽至**AAA > Server Groups > Radius**，以建立Radius伺服器群組。在本示例中，Radius伺服器組稱為ACS。



3. 編輯Radius伺服器條目，以新增伺服器IP地址和共用金鑰。此共用金鑰必須與WLC和RADIUS伺服器上的共用金鑰匹配。



以下是完整組態範例：

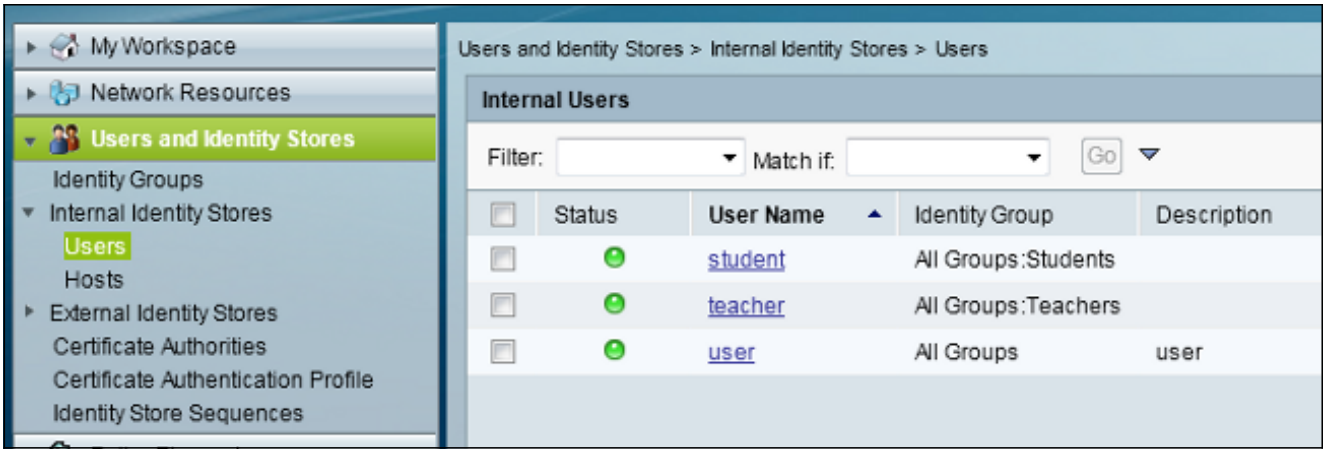


設定RADIUS伺服器

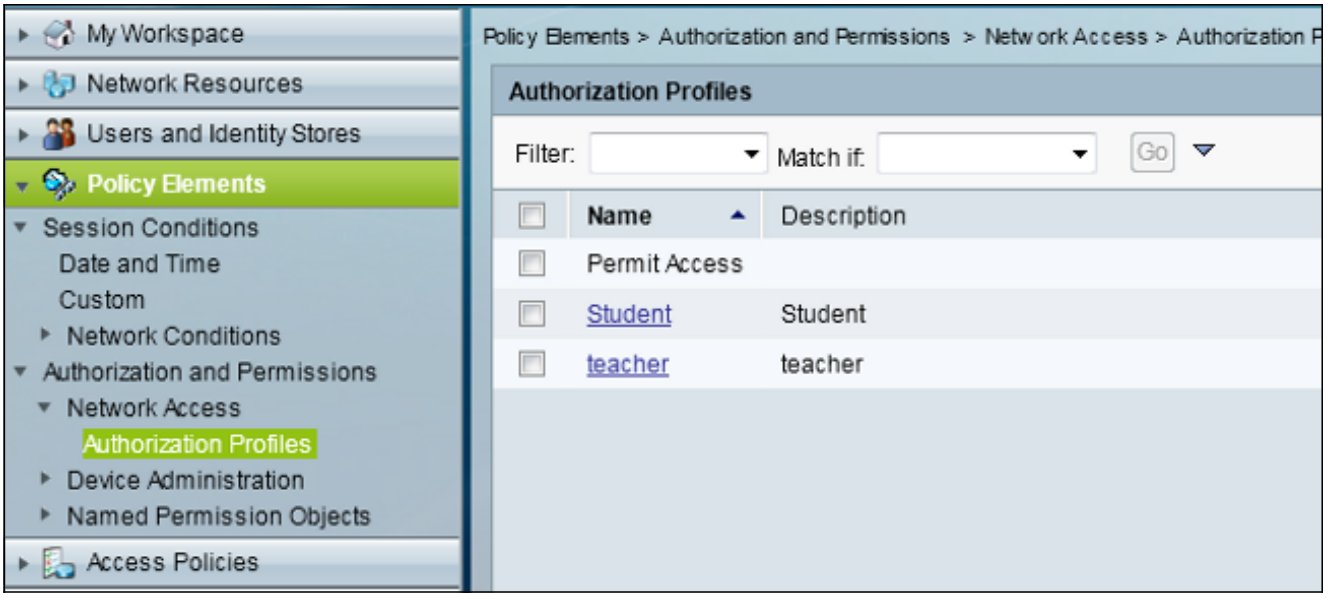
以下程式介紹如何設定RADIUS伺服器。

1. 在RADIUS伺服器上，導覽至**Users and Identity Stores > Internal Identity Stores > Users**。

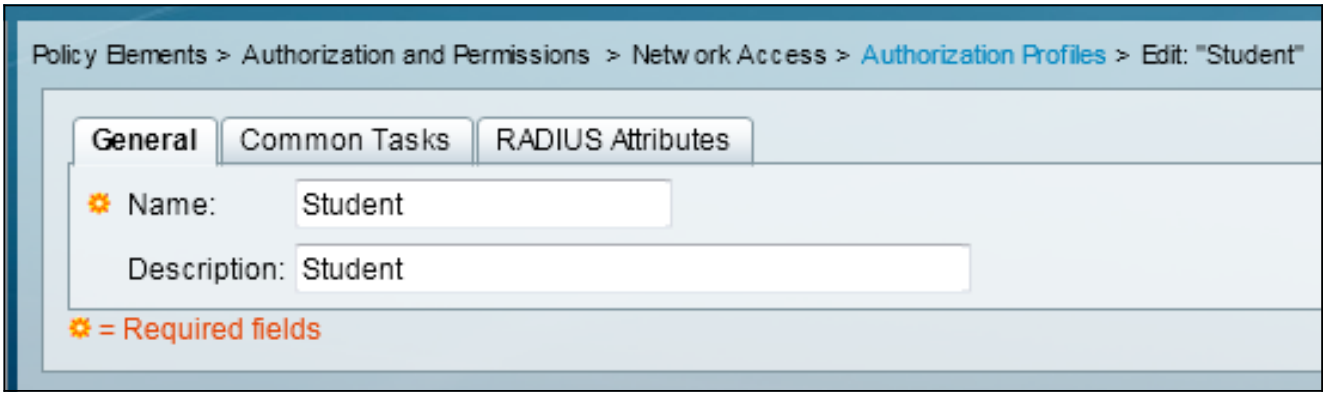
2. 建立相應的使用者名稱和身份組。在本示例中，它是Student and All Groups:Students和Teacher and AllGroups:Teachers。



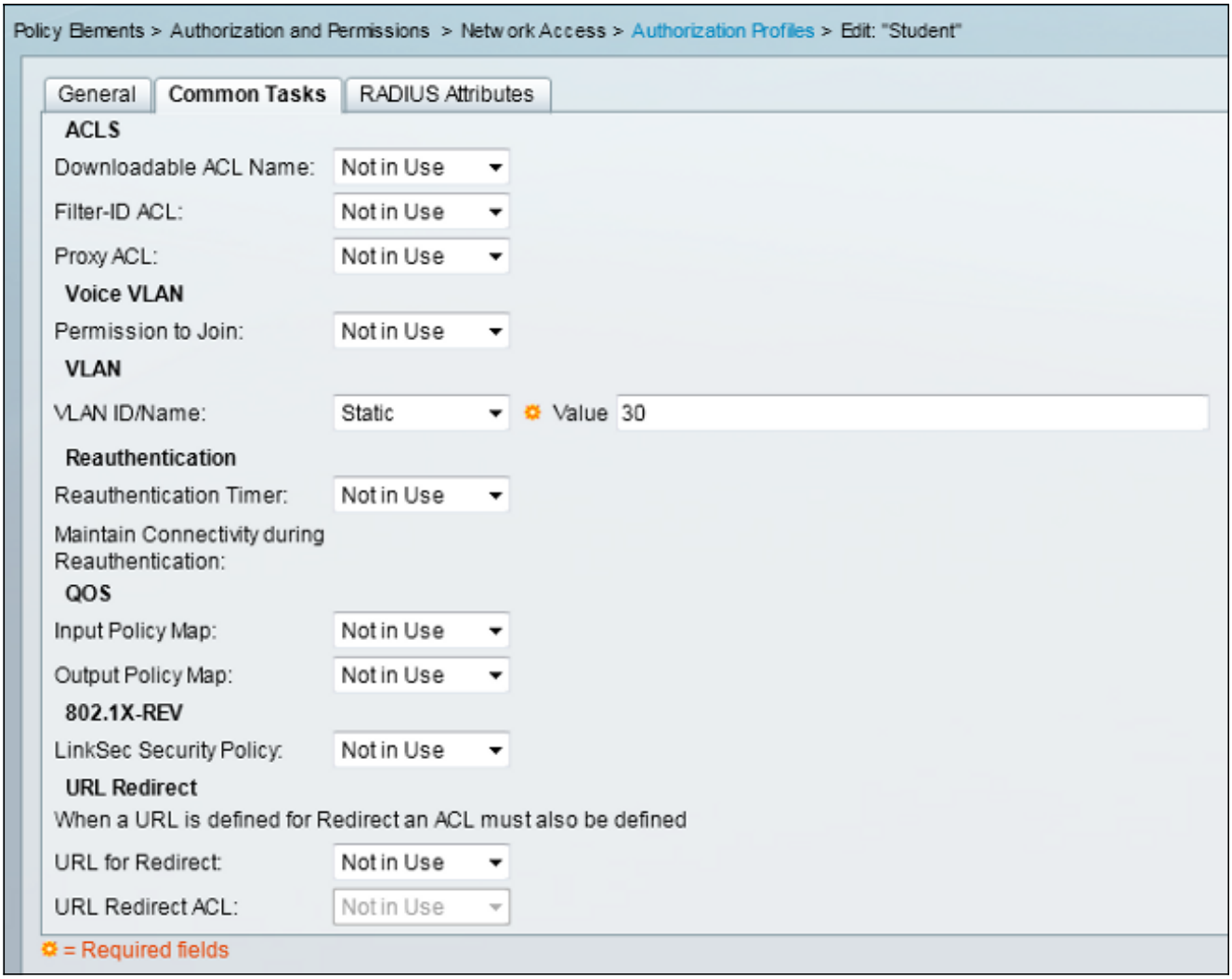
3. 導覽至**Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles**，然後為AAA覆蓋建立授權配置檔案。



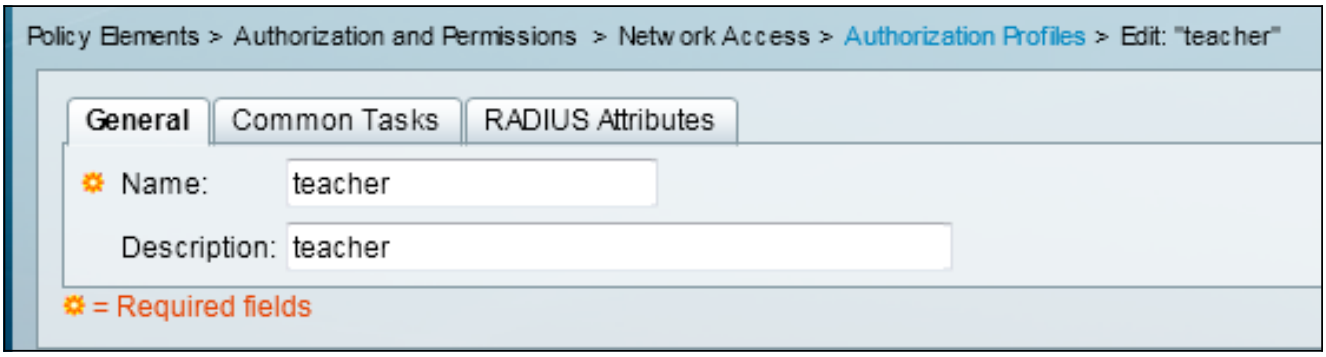
4. 編輯學生的授權配置檔案。



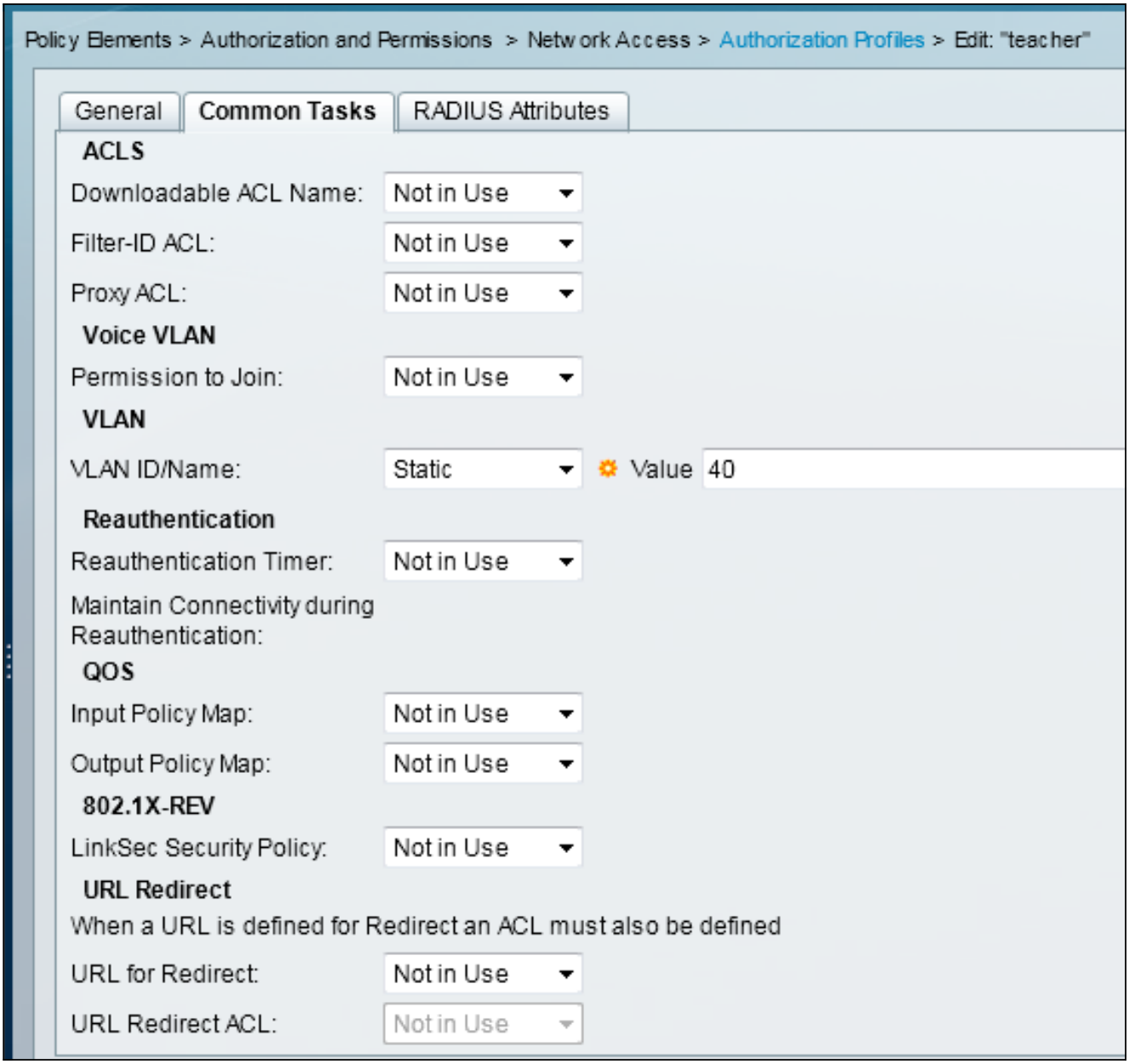
5. 將VLAN ID/名稱設定為**Static**，值為**30**(VLAN 30)。



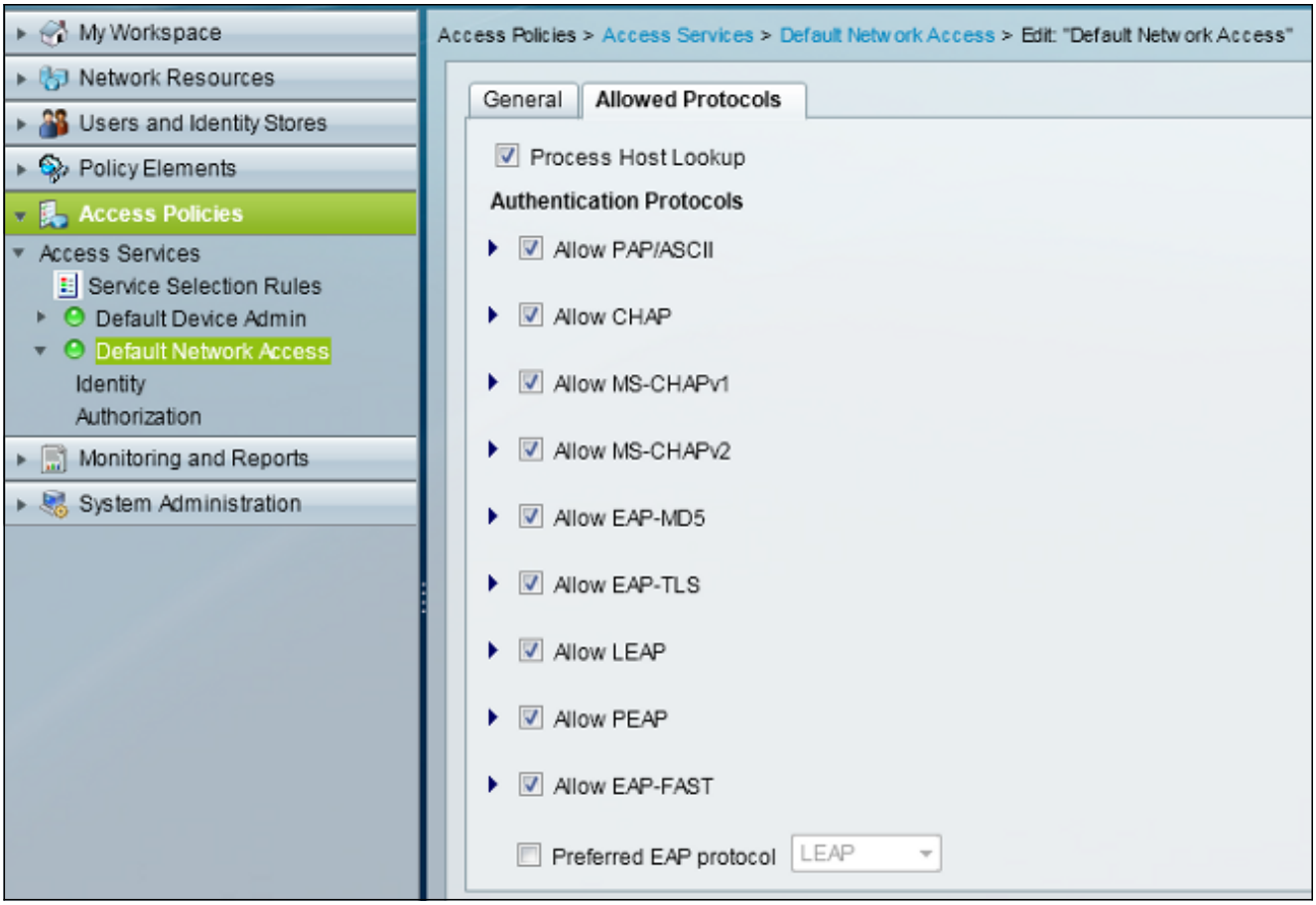
6. 編輯教師的授權配置檔案。



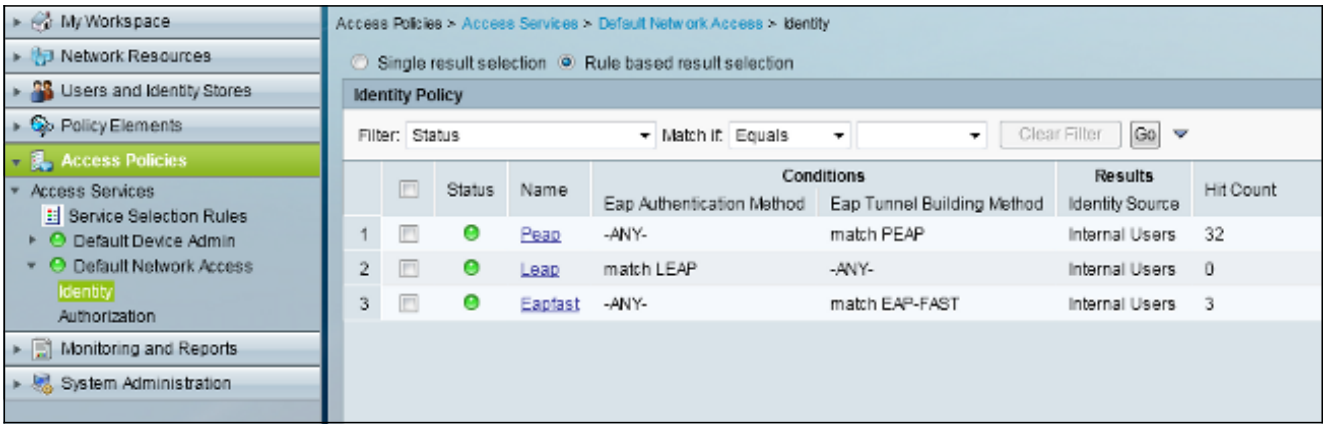
7. 將VLAN ID/Name設定為**Static**，值為**40**(VLAN 40)。



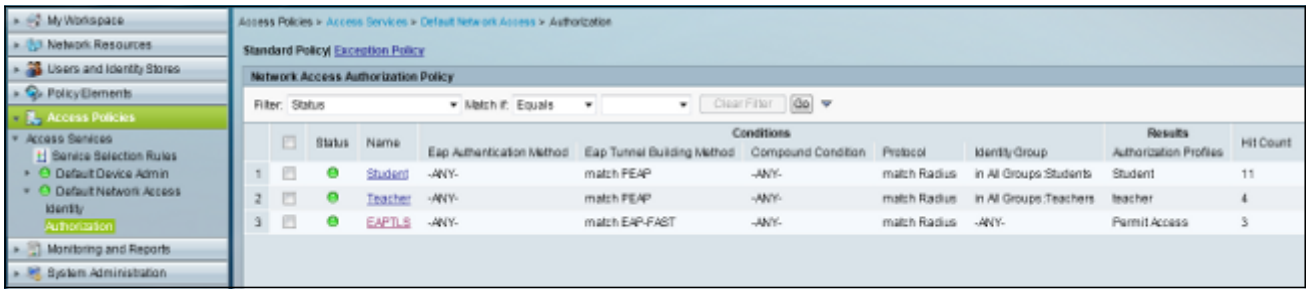
8. 導覽至**Access Policies > Access Services > Default Network Access**，然後按一下**Allowed Protocols**索引標籤。選中**Allow PEAP**覈取方塊。



9. 導航到**Identity**，然後定義規則以允許PEAP使用者。



10. 導航到**Authorization**，並將學生和教師對映到授權策略；在本例中，對映應為VLAN 30的Student和VLAN 40的Teacher。

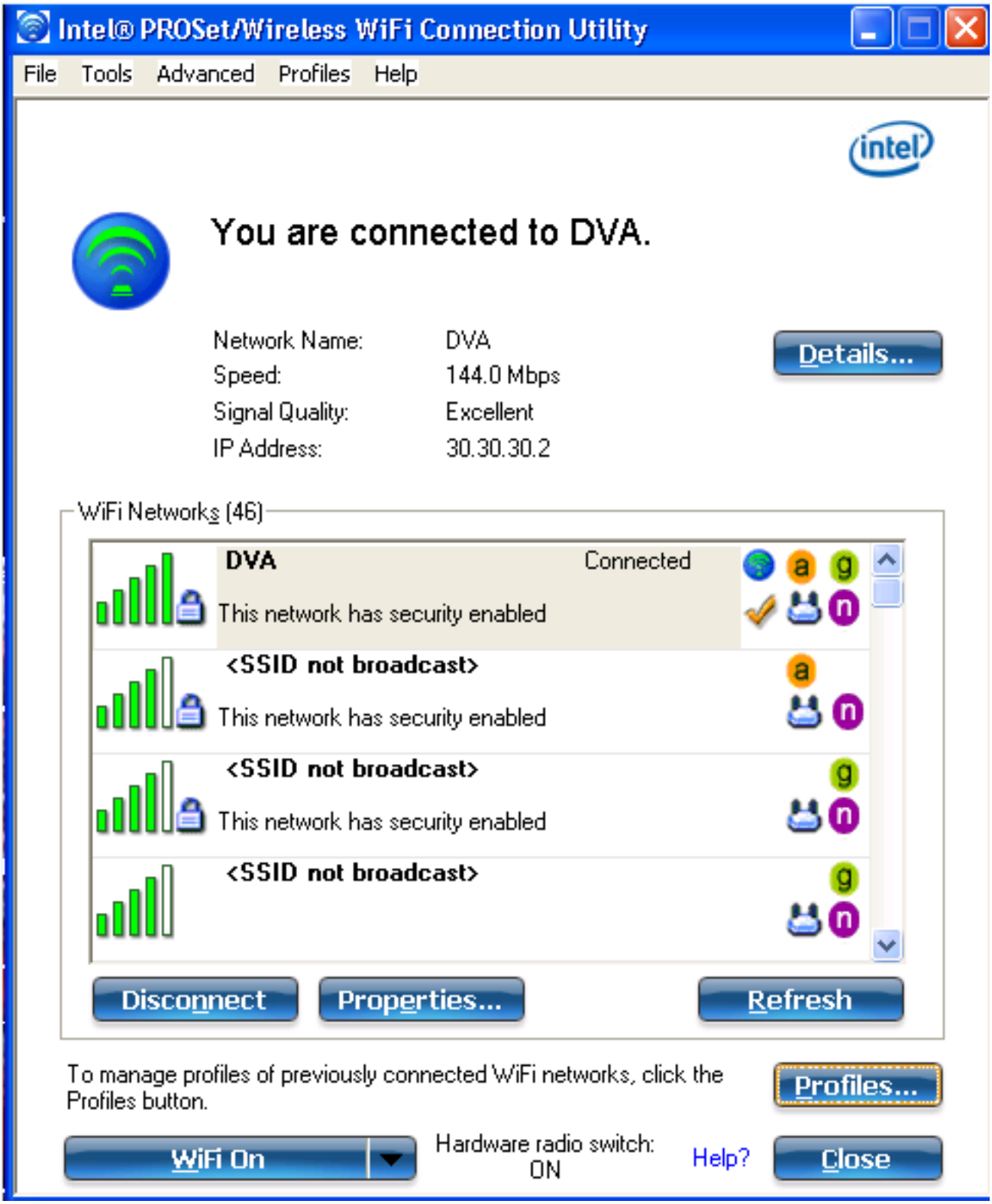


驗證

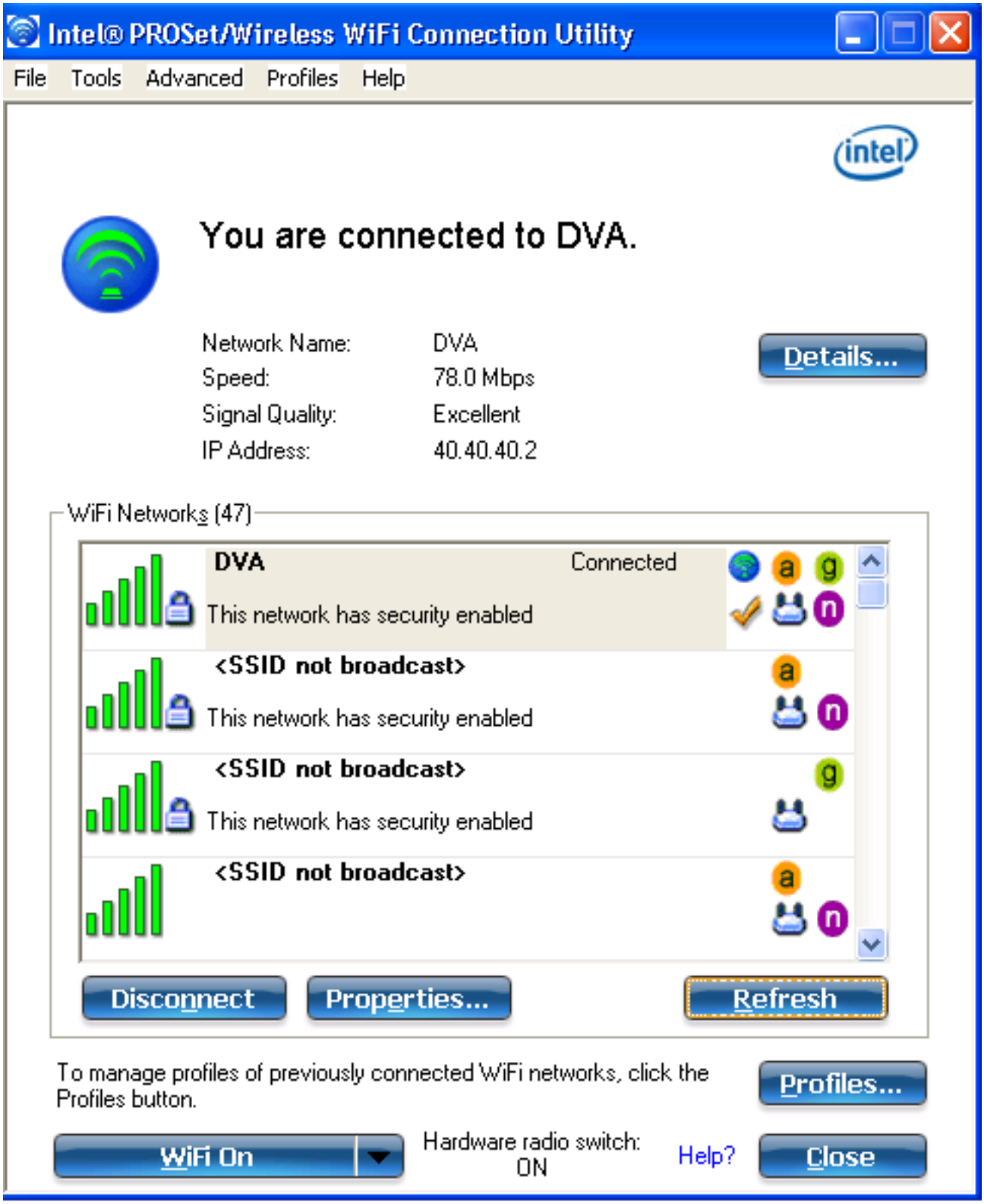
使用本節內容，確認您的組態是否正常運作。以下是驗證程式：

- 監控ACS上顯示哪些客戶端經過身份驗證的頁面。

- 使用學生組連線到DVA WLAN，然後檢視客戶端WiFi連線實用程式。



- 使用教師組連線到DVA WLAN，然後檢視客戶端WiFi連線實用程式。



疑難排解

本節提供的資訊可用於對組態進行疑難排解。

附註：

使用命令查詢工具(僅供已註冊客戶使用)可獲取本節中使用的命令的更多資訊。

輸出直譯器工具(僅供已註冊客戶使用)支援某些**show**命令。使用輸出直譯器工具來檢視

show命令輸出的分析。

使用 **debug 指令之前，請先參閱**有關 Debug 指令的重要資訊。

有用的調試**包括debug client mac-address** *mac*，以及以下NGWC trace命令：

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

NGWC跟蹤不包括dot1x/AAA，因此請對dot1x/AAA使用以下合併跟蹤的完整清單：

- **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-filtered-trace**

當動態VLAN分配正確工作時，您應該從調試中看到以下型別的輸出：

```
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)
```