Dynamic VLAN Assignment with NGWC and ACS 5.2 Configuration Example

Document ID: 116494

Contributed by Surendra BG, Cisco TAC Engineer.
Oct 03, 2013

Contents

Introduction

This document describes the concept of dynamic VLAN assignment. It also describes how to configure the wireless LAN controller (WLC) and a RADIUS server in order to assign wireless LAN (WLAN) clients to a specific VLAN dynamically. In this document, the RADIUS server is an Access Control Server (ACS) that runs Cisco Secure Access Control System Version 5.2.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Basic knowledge of the WLC and Lightweight Access Points (LAPs)
- Functional knowledge of the authentication, authorization, and accounting (AAA) server
- Thorough knowledge of wireless networks and wireless security issues

Components Used

The information in this document is based on these software and hardware versions:

- Cisco 5760 Wireless LAN Controller with Cisco IOS® XE Software Release 3.2.2 (Next Generation Wiring Closet, or NGWC)
- Cisco Aironet 3602 Series Lightweight Access Point
- Microsoft Windows XP with Intel Proset Supplicant
- Cisco Secure Access Control System Version 5.2
- Cisco Catalyst 3560 Series Switch

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.

Dynamic VLAN Assignment with RADIUS Server

In most WLAN systems, each WLAN has a static policy that applies to all clients associated with a Service Set Identifier (SSID), or WLAN in the controller terminology. Although powerful, this method has limitations because it requires clients to associate with different SSIDs in order to inherit different QoS and security policies.

However, the Cisco WLAN solution supports identity networking. This allows the network to advertise a single SSID, but allows specific users to inherit different QoS, VLAN attributes, and/or security policies based on the user credentials.

Dynamic VLAN assignment is one such feature that places a wireless user into a specific VLAN based on the credentials supplied by the user. This task of user assignment to a specific VLAN is handled by a RADIUS authentication server, such as a Cisco Secure ACS. This feature can be used, for example, in order to allow the wireless host to remain on the same VLAN as it moves within a campus network.

As a result, when a client attempts to associate to a LAP registered with a controller, the LAP passes the credentials of the user to the RADIUS server for validation. Once the authentication is successful, the RADIUS server passes certain Internet Engineering Task Force (IETF) attributes to the user. These RADIUS attributes decide the VLAN ID that should be assigned to the wireless client. The SSID of the client (the WLAN, in terms of the WLC) does not matter because the user is always assigned to this predetermined VLAN ID.

The RADIUS user attributes used for the VLAN ID assignment are:

- IETF 64 (Tunnel Type) − Set to VLAN.
- IETF 65 (Tunnel Medium Type) − Set to 802.
- IETF 81 (Tunnel−Private−Group−ID) − Set to the VLAN ID.

The VLAN ID is 12 bits and takes a value between 1 and 4094, inclusive. Because the Tunnel−Private−Group−ID is of type string, as defined in RFC 2868, RADIUS Attributes for Tunnel Protocol Support for use with IEEE 802.1X, the VLAN ID integer value is encoded as a string. When these tunnel attributes are sent, it is necessary to fill in the Tag field.

As noted in RFC2868, section 3.1:

"The Tag field is one octet in length and is intended to provide a means of grouping attributes in the same packet which refer to the same tunnel."

Valid values for the Tag field are 0x01 through 0x1F, inclusive. If the Tag field is unused, it must be zero (0x00). Refer to RFC 2868 for more information on all RADIUS attributes.

Configure

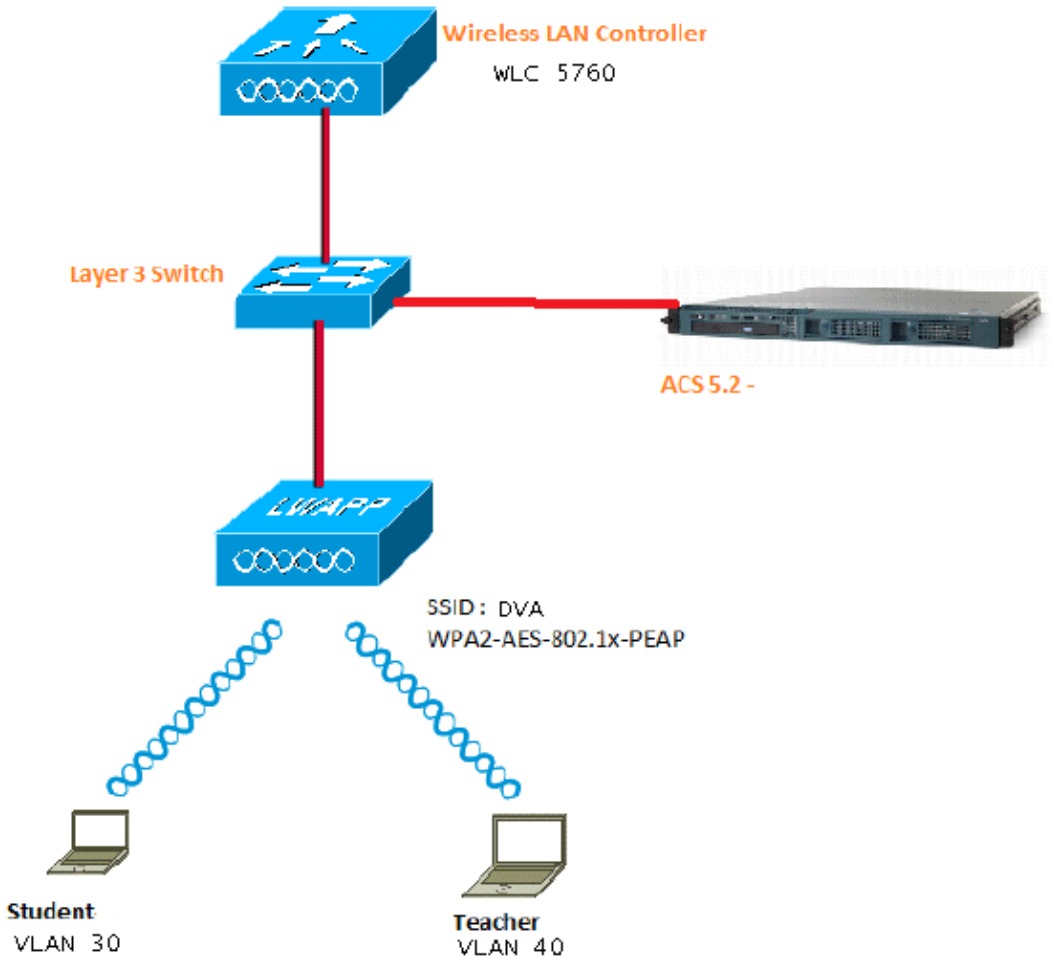
Configuration of a dynamic VLAN assignment consists of two distinct steps:

1. Configure the WLC with the command−line interface (CLI) or with the GUI.
2. Configure the RADIUS server.

Note: Use the Command Lookup Tool (registered customers only) in order to obtain more information on the commands used in this section.

Network Diagram

This document uses this network setup:



This document uses 802.1X with Protected Extensible Authentication Protocol (PEAP) as the security mechanism.

Assumptions

- Switches are configured for all Layer 3 (L3) VLANs.
- The DHCP server is assigned a DHCP scope.
- L3 connectivity exists between all devices in the network.
- The LAP is already joined to the WLC.
- Each VLAN has a /24 mask.

- ACS 5.2 has a self−signed certificate installed.

Configure WLC with CLI

Configure WLAN

This is an example of how to configure a WLAN with the SSID of DVA:

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

Configure RADIUS Server on WLC

This is an example of the configuration of the RADIUS server on the 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
```

Configure DHCP Pool for Client VLAN

This is an example of the configuration of the DHCP pool for the client VLAN 30 and VLAN 40:

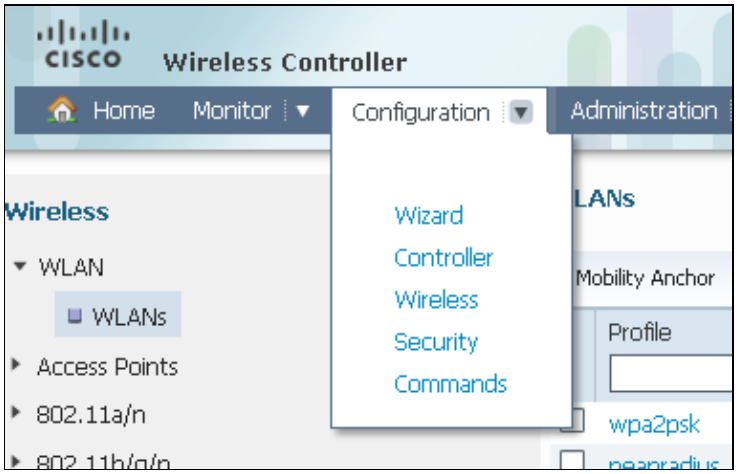
```
interface Vlan30
 ip address 30.30.30.1 255.255.255.0
!
interface Vlan40
 ip address 40.40.40.1 255.255.255.0

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
```

Configure WLC with GUI

Configure WLAN

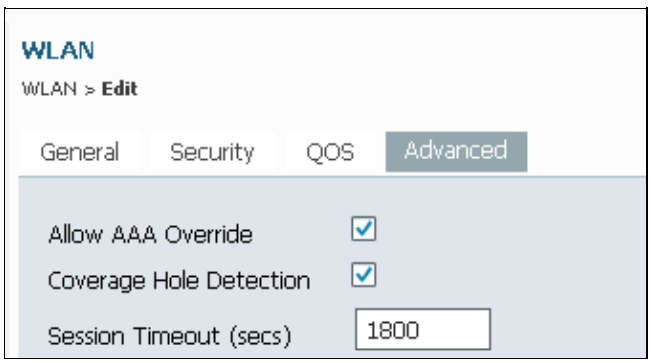
This procedure describes how to configure the WLAN.

1. Navigate to ***Configuration*** > ***Wireless*** > ***WLAN*** > ***NEW*** tab.

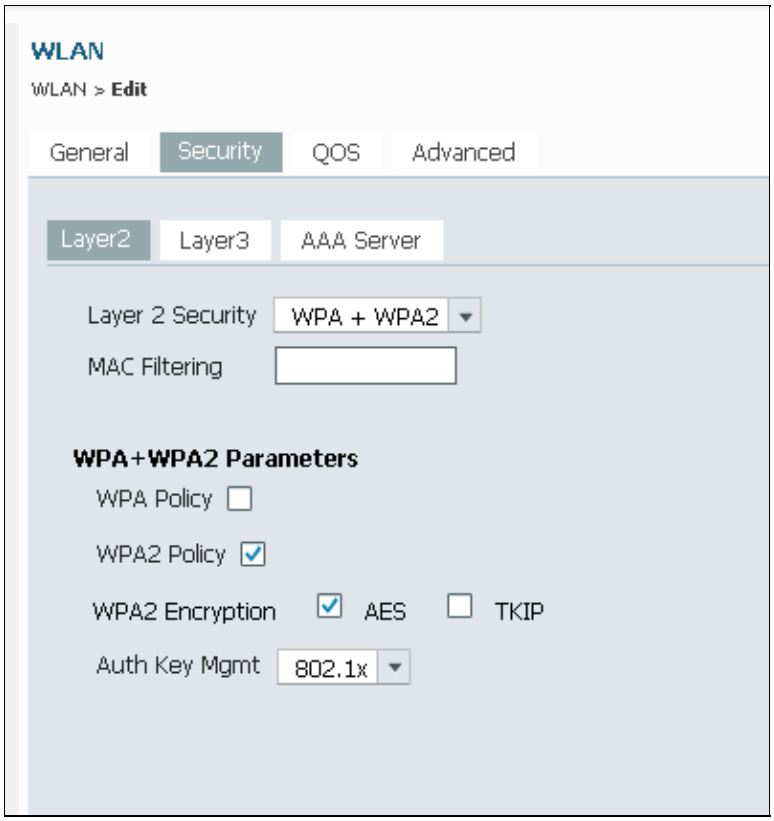


2. Click the ***General*** tab in order to see that the WLAN is configured for WPA2−802.1X, and map the Interface/Interfrace Group(G) to VLAN 20 (***VLAN0020***).

3. Click the ***Advanced*** tab, and check the ***Allow AAA Override*** check box. Override must be enabled for this feature to work.



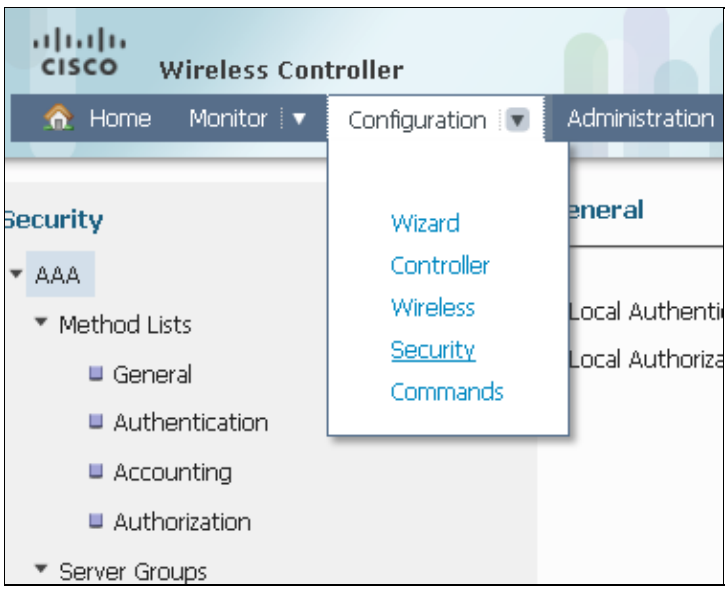
4. Click the ***Security*** tab and the ***Layer2*** tab, check the WPA2 Encryption ***AES*** check box, and select ***802.1x*** from the Auth Key Mgmt drop−down list.



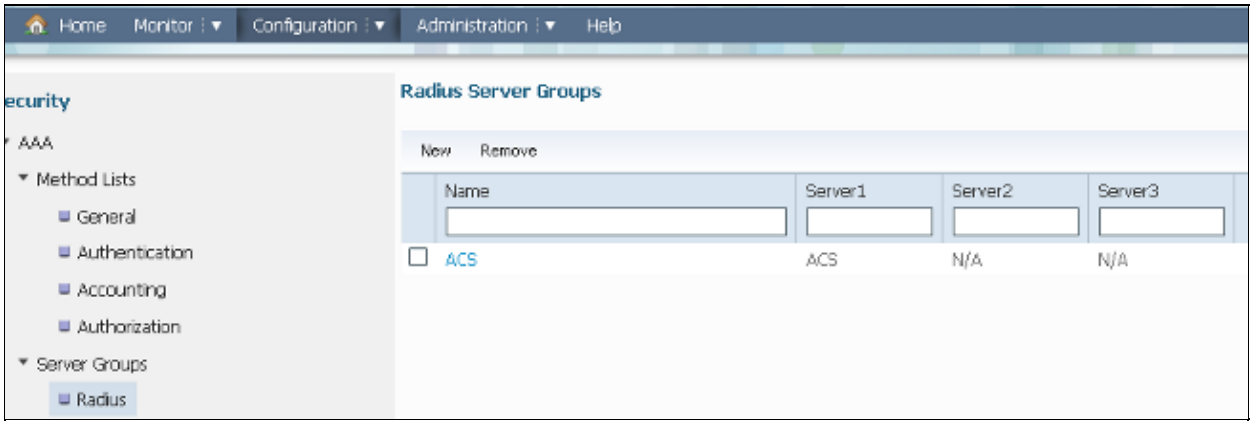
Configure RADIUS Server on WLC

This procedure describes how to configure the RADIUS server on the WLC.

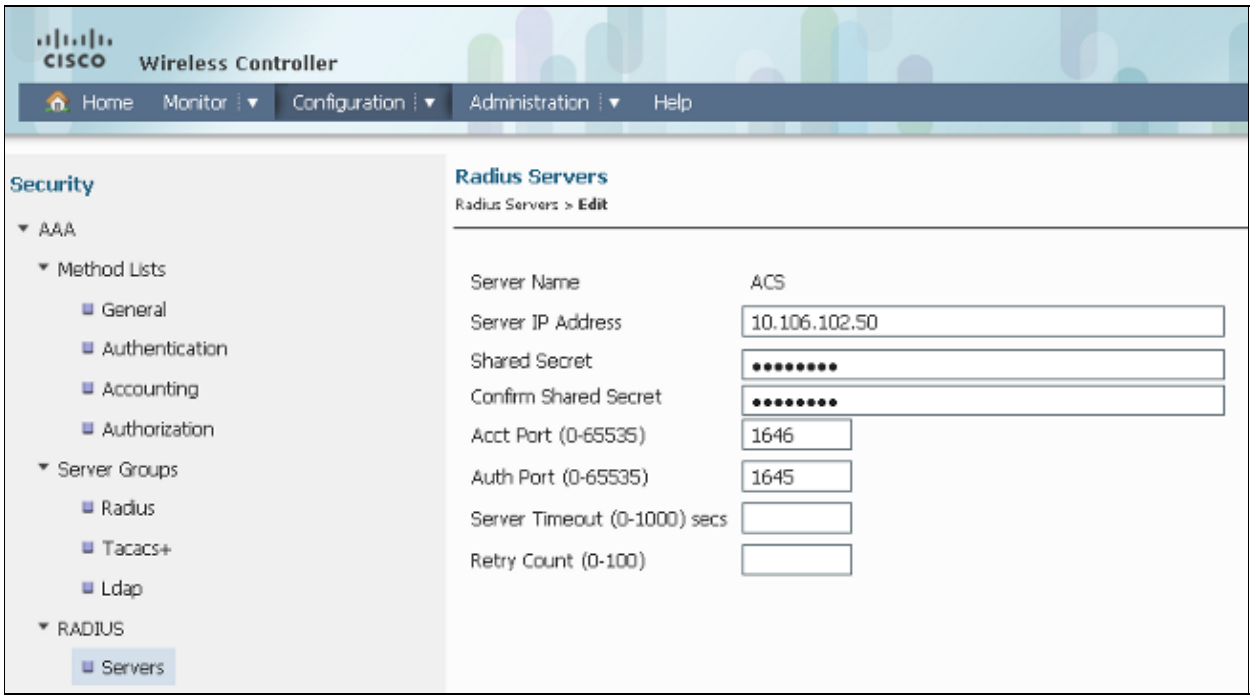
1. Navigate to ***Configuration*** > ***Security*** tab.



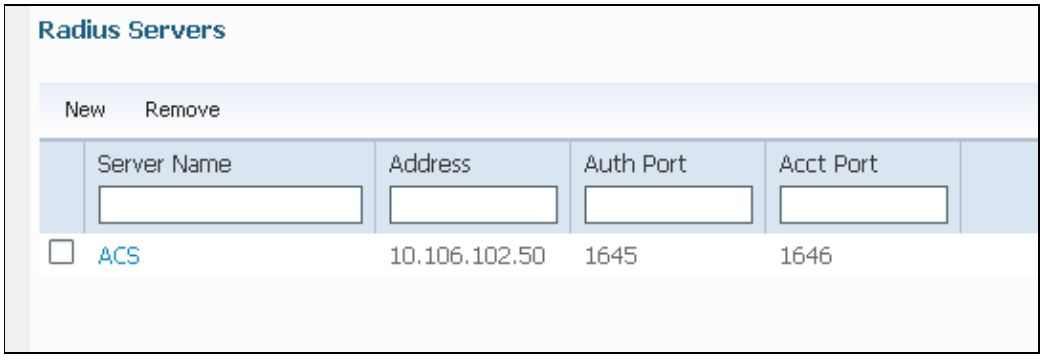
2. Navigate to ***AAA*** > ***Server Groups*** > ***Radius*** in order to create the Radius Server Groups. In this example, the Radius Server Group is called ACS.



3. Edit the Radius Server entry in order to add the Server IP Address and the Shared Secret. This Shared Secret must match the Shared Secret on the WLC and the RADIUS server.



This is an example of a complete configuration:

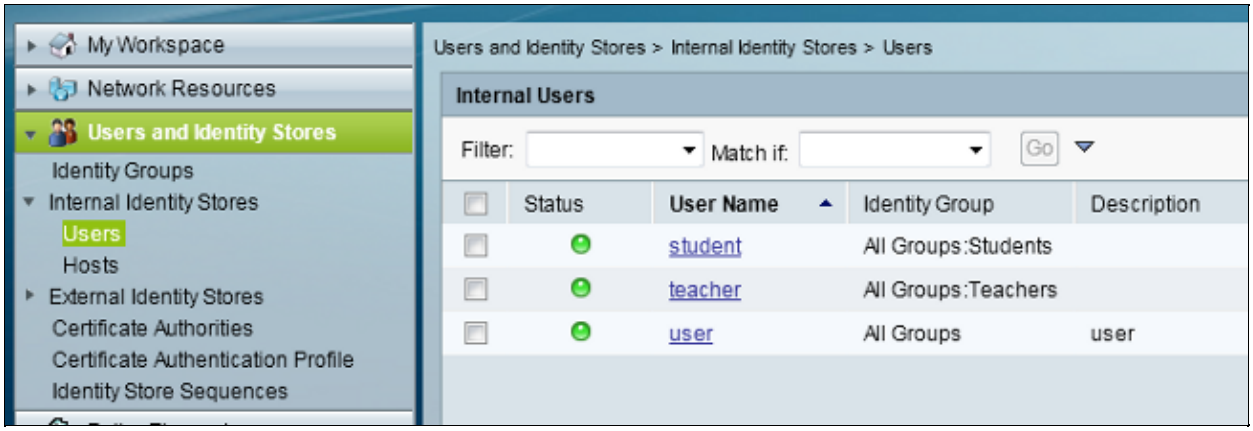


Configure RADIUS Server

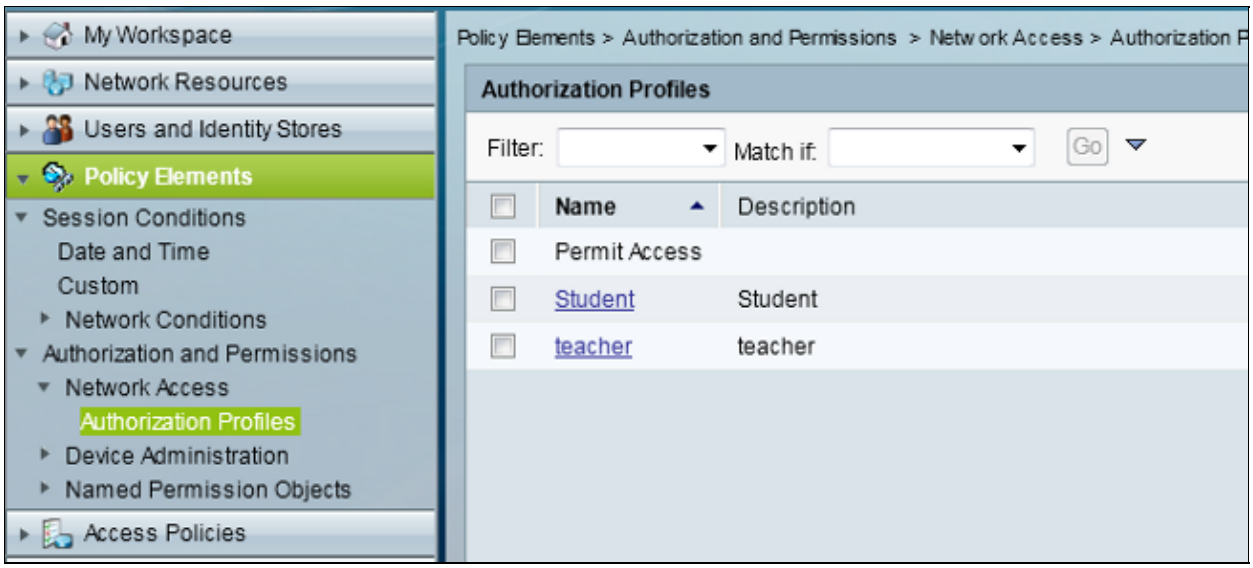
This procedure describes how to configure the RADIUS server.

1. On the RADIUS server, navigate to ***Users and Identity Stores*** > ***Internal Identity Stores*** > ***Users***.

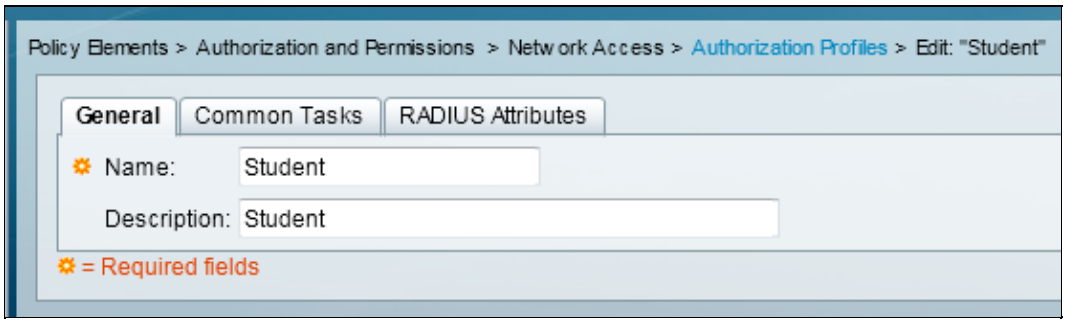
2. Create the appropriate User Names and Identity Groups. In this example, it is Student and All Groups:Students, and Teacher and AllGroups:Teachers.



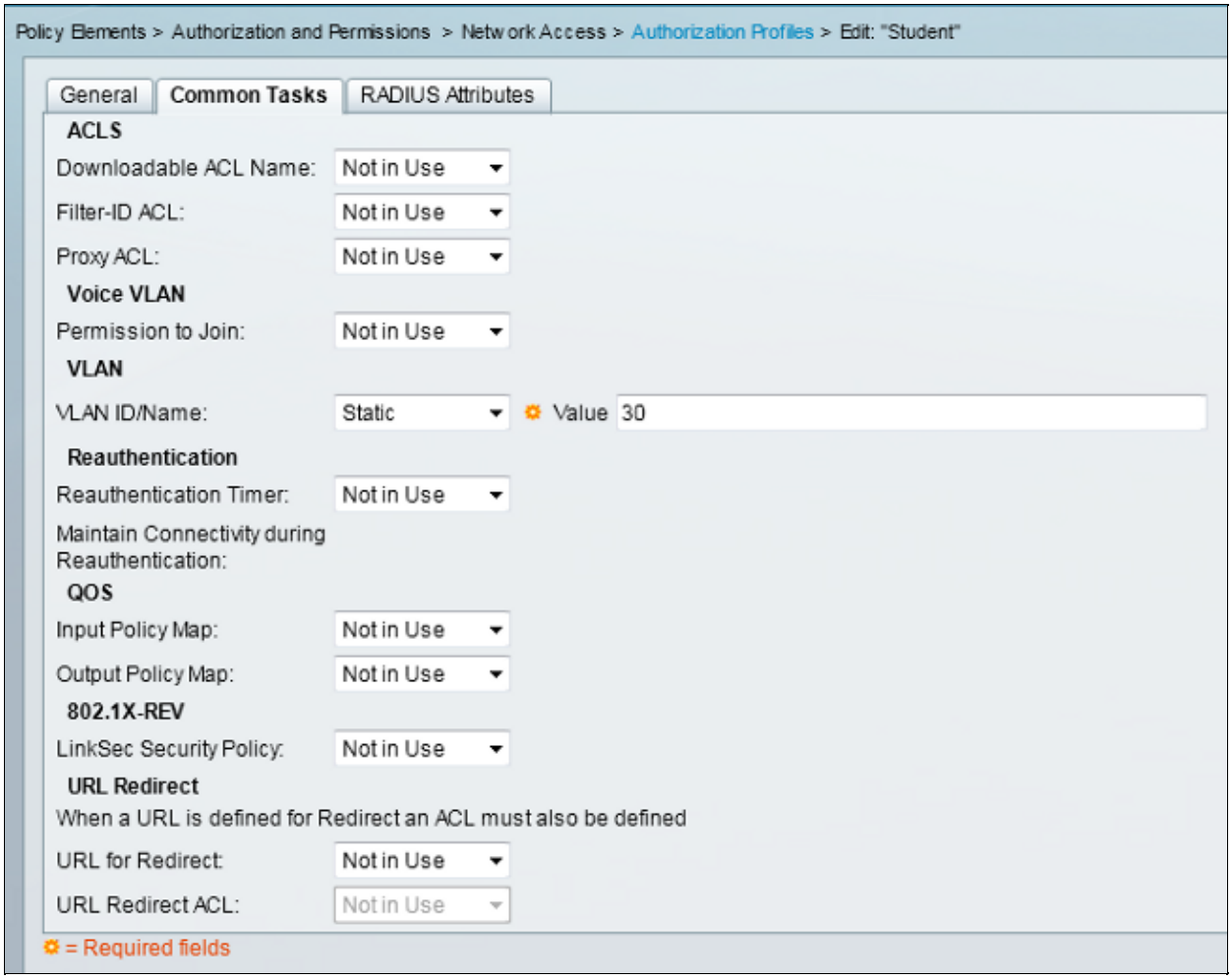
3. Navigate to ***Policy Elements*** > ***Authorization and Permissions*** > ***Network Access*** > ***Authorization Profiles***, and create the Authorization Profiles for AAA override.



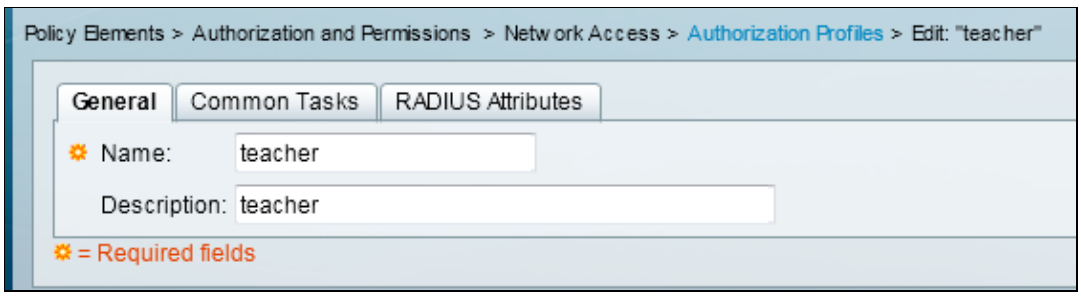
4. Edit the Authorization Profile for Student.



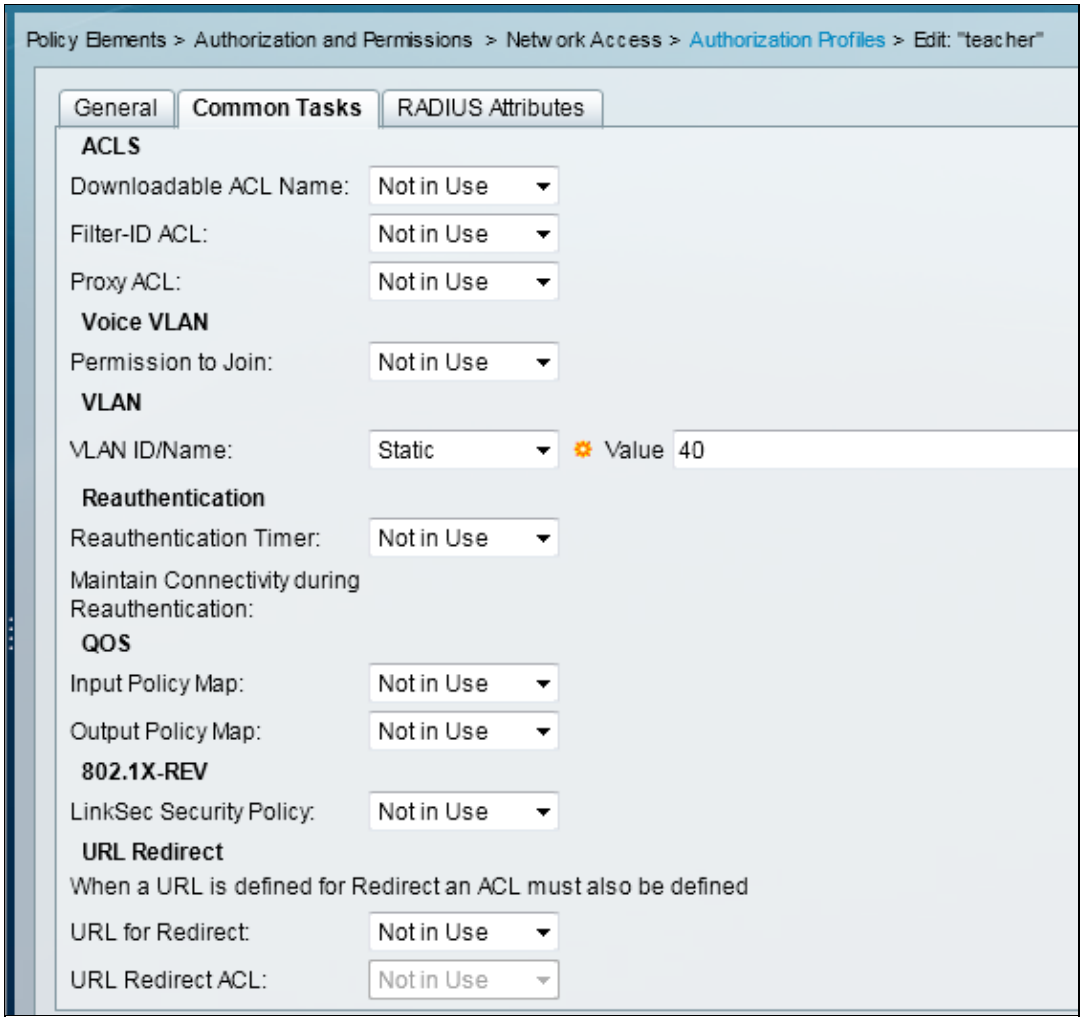
5. Set the VLAN ID/Name as ***Static*** with a Value of ***30*** (VLAN 30).



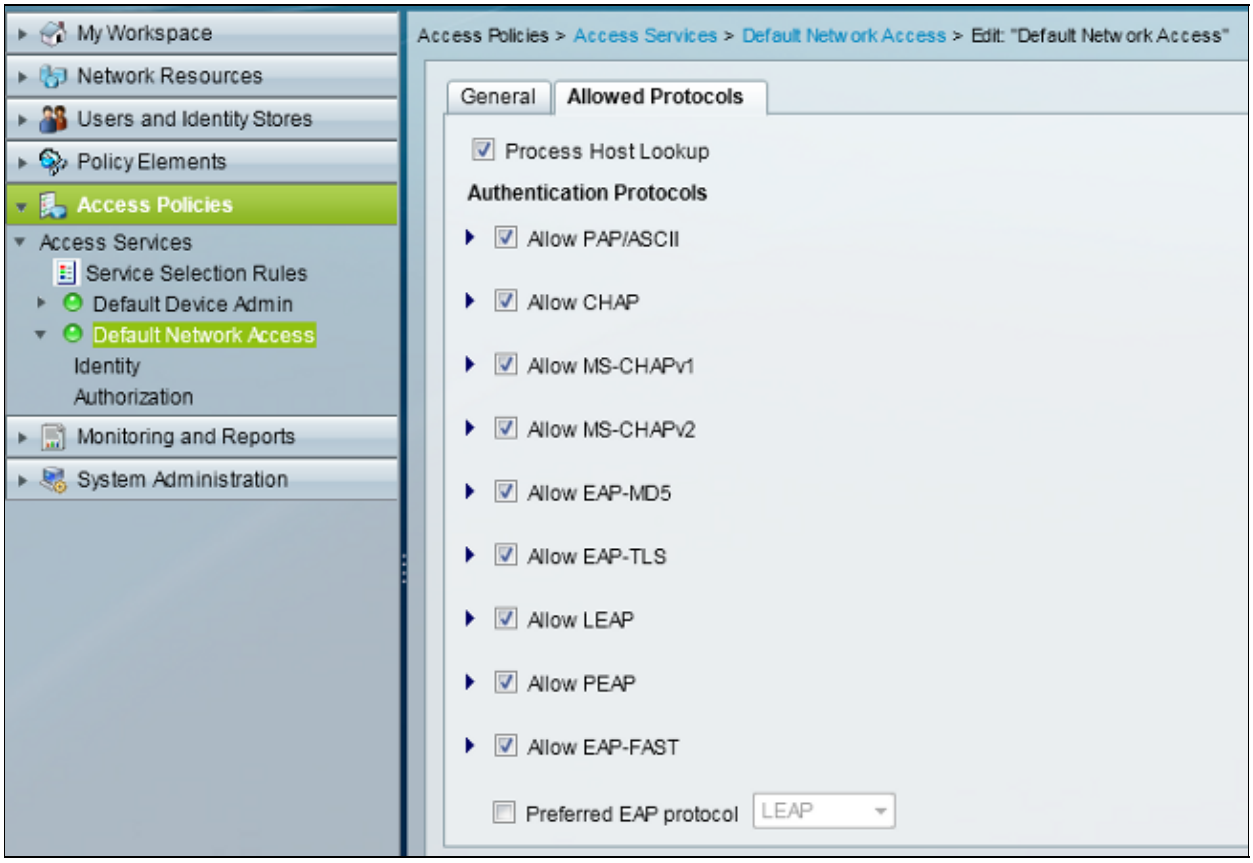
6. Edit the Authorization Profile for Teacher.



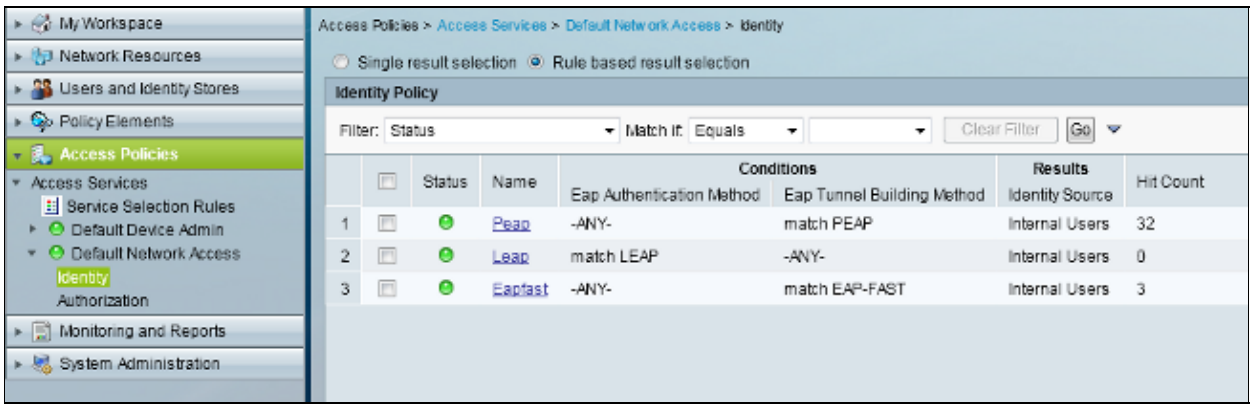
7. Set the VLAN ID/Name as ***Static*** with a Value of ***40*** (VLAN 40).



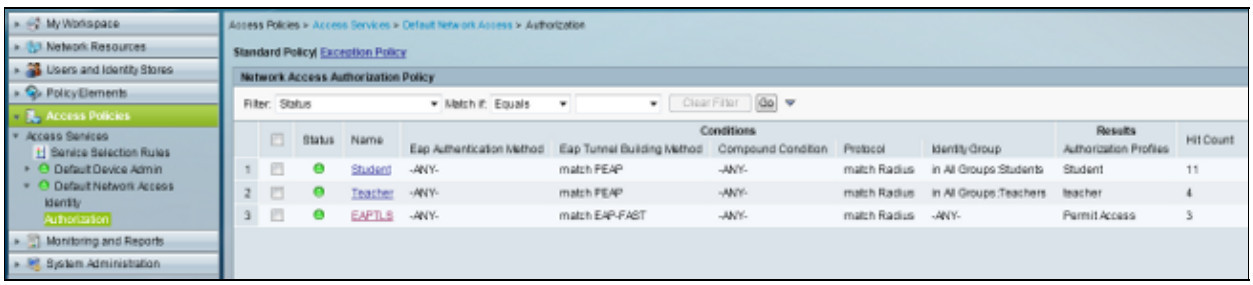
8. Navigate to ***Access Policies*** > ***Access Services*** > ***Default Network Access***, and click the ***Allowed Protocols*** tab. Check the ***Allow PEAP*** checkbox.



9. Navigate to ***Identity***, and define the rules in order to allow PEAP users.



10. Navigate to ***Authorization***, and map Student and Teacher to the Authorization Policy; in this example, the mapping should be Student for VLAN 30 and Teacher for VLAN 40.

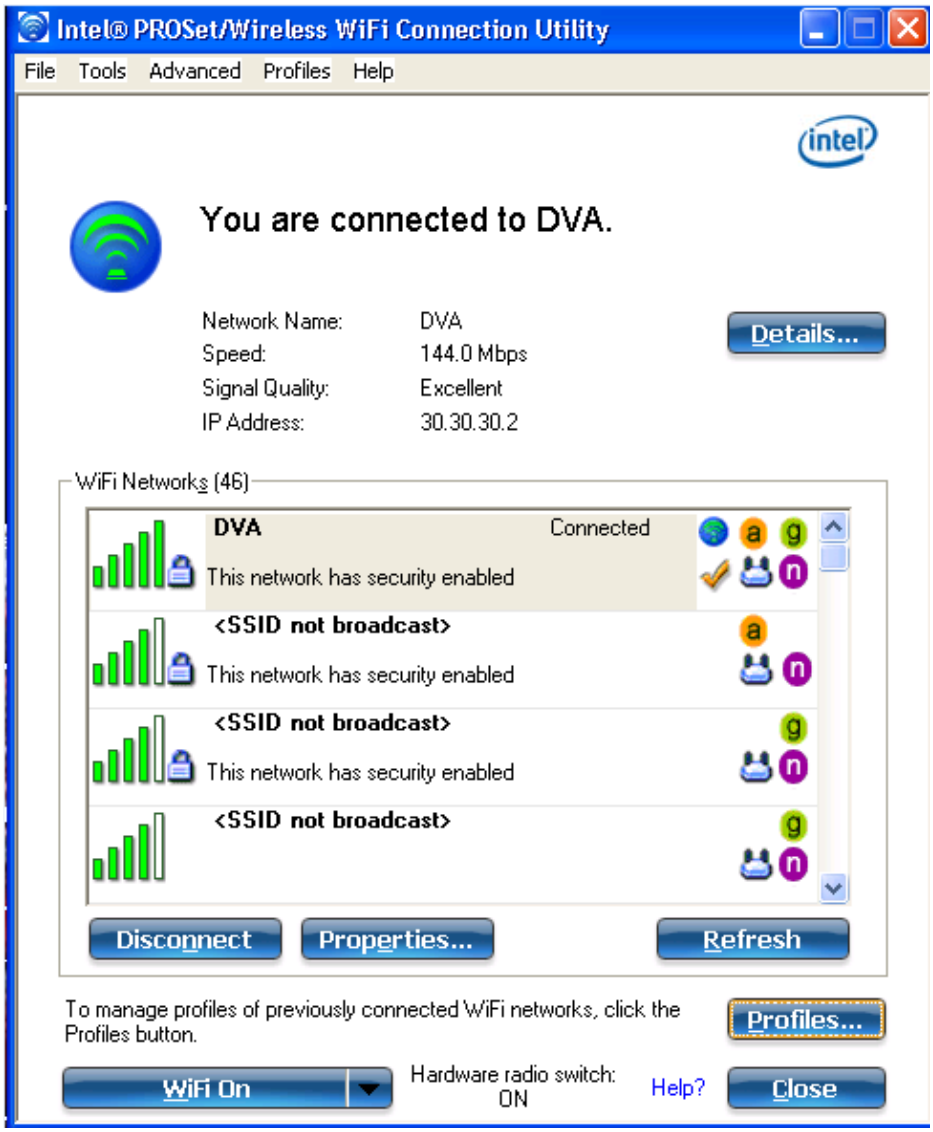


Verify

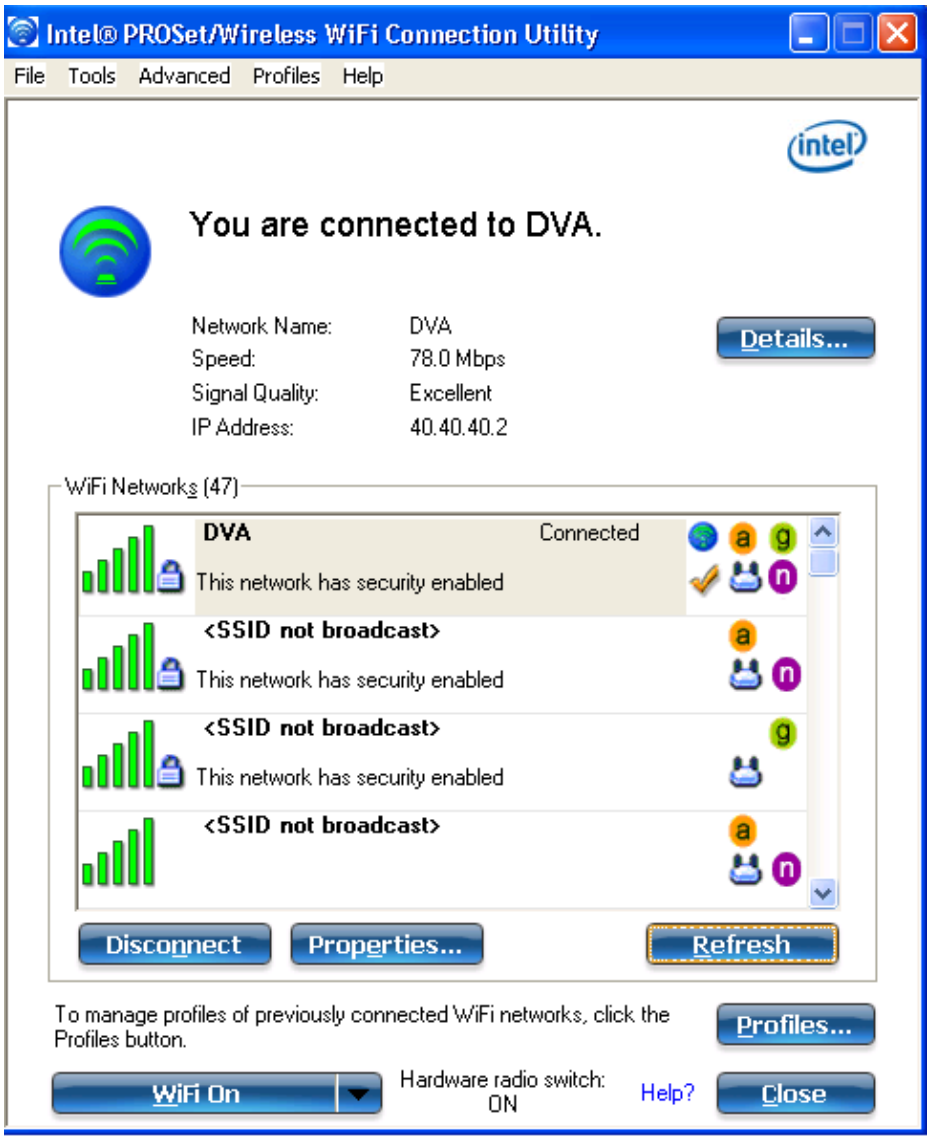
Use this section to confirm that your configuration works properly. These are the verification processes:

- Monitor the page on the ACS that shows which clients are authenticated.

- Connect to the DVA WLAN with Student Group, and review the client WiFi Connection Utility.



- Connect to the DVA WLAN with the Teacher Group, and review the client WiFi Connection Utility.



Troubleshoot

This section provides information you can use to troubleshoot your configuration.

Notes:

Use the Command Lookup Tool (registered customers only) in order to obtain more information on the commands used in this section.

The Output Interpreter Tool (registered customers only) supports certain ***show*** commands. Use the Output Interpreter Tool in order to view an analysis of ***show*** command output.

Refer to Important Information on Debug Commands before you use ***debug*** commands.

Useful debugs include ***debug client mac-address*** *mac*, as well as these NGWC trace commands:

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

The NGWC trace does not include dot1x/AAA, so use this entire list of combined traces for 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−filtered−traces***

When dynamic VLAN assignment is working correctly, you should see this type of output from the 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)
```