NGWC 및 ACS 5.2로 동적 VLAN 할당 구성

목차

소개

이 문서에서는 동적 VLAN 할당 개념에 대해 설명합니다. 또한 특정 VLAN에 무선 LAN(WLAN) 클라이언트를 동적으로 할당하기 위해 WLC(Wireless LAN Controller) 및 RADIUS 서버를 구성하는 방법에 대해 설명합니다. 이 문서에서 RADIUS 서버는 Cisco Secure Access Control System 버전 5.2를 실행하는 ACS(Access Control Server)입니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- WLC 및 LAP(Lightweight Access Point)에 대한 기본 지식
- AAA(Authentication, Authorization, and Accounting) 서버의 기능 지식
- 무선 네트워크 및 무선 보안 문제에 대한 철저한 지식

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco IOS® XE Software 릴리스 3.2.2(Next Generation Wiring Closet 또는 NGWC)가 포함된 Cisco 5760 Wireless LAN Controller
- Cisco Aironet 3602 Series Lightweight Access Point
- Microsoft Windows XP with Intel Proset Supplicant
- Cisco Secure Access Control System 버전 5.2
- Cisco Catalyst 3560 Series 스위치

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

RADIUS 서버를 사용한 동적 VLAN 할당

대부분의 WLAN 시스템에서 각 WLAN에는 컨트롤러 용어에서 SSID(Service Set Identifier) 또는 WLAN과 연결된 모든 클라이언트에 적용되는 정적 정책이 있습니다. 강력하지만 이 방법은 여러 QoS 및 보안 정책을 상속하기 위해 클라이언트가 다른 SSID와 연결해야 하기 때문에 제한이 있습니다.

그러나 Cisco WLAN 솔루션은 ID 네트워킹을 지원합니다. 이를 통해 네트워크에서 단일 SSID를 광고할 수 있지만, 특정 사용자가 사용자 자격 증명을 기반으로 서로 다른 QoS, VLAN 특성 및/또는 보안 정책을 상속할 수 있습니다.

동적 VLAN 할당은 사용자가 제공한 자격 증명을 기반으로 무선 사용자를 특정 VLAN에 넣는 기능입니다. 특정 VLAN에 대한 사용자 할당 작업은 Cisco Secure ACS와 같은 RADIUS 인증 서버에 의해 처리됩니다. 예를 들어, 이 기능을 사용하면 무선 호스트가 캠퍼스 네트워크 내에서 이동하는 것과 동일한 VLAN에 유지되도록 할 수 있습니다.

따라서 클라이언트가 컨트롤러에 등록된 LAP에 연결하려고 하면 LAP는 검증을 위해 사용자의 자격 증명을 RADIUS 서버에 전달합니다. 인증에 성공하면 RADIUS 서버는 특정 IETF(Internet Engineering Task Force) 특성을 사용자에게 전달합니다. 이러한 RADIUS 특성은 무선 클라이언트에 할당해야 하는 VLAN ID를 결정합니다. 사용자가 항상 이 미리 결정된 VLAN ID에 할당되므로 클라이언트의 SSID(WLC의 경우 WLAN)는 중요하지 않습니다.

VLAN ID 할당에 사용되는 RADIUS 사용자 특성은 다음과 같습니다.

- IETF 64(터널 유형) - VLAN으로 설정합니다.
- IETF 65(Tunnel Medium Type) - 802로 설정합니다.
- IETF 81(Tunnel-Private-Group-ID) - VLAN ID로 설정합니다.

VLAN ID는 12비트이며 1과 4094 사이의 값을 포함합니다(포함). Tunnel-Private-Group-ID는 RFC 2868에 정의된 대로 유형 문자열이므로 IEEE 802.1X와 함께 사용할 터널 프로토콜 지원을 위한 RADIUS 특성은 문자열로 인코딩됩니다. 이러한 터널 특성이 전송되면 Tag 필드를 입력해야 합니다.

RFC2868, 섹션 3.1에 설명된 대로:

"Tag 필드는 길이가 18진이며 동일한 터널을 참조하는 동일한 패킷에서 특성을 그룹화하는 방법을

제공합니다."

Tag 필드에 유효한 값은 0x01~0x1F이며, 0x1F입니다. 태그 필드가 사용되지 않으면 0이어야 합니다(0x00). 모든 RADIUS 특성에 대한 자세한 내용은 RFC 2868을 참조하십시오.

구성

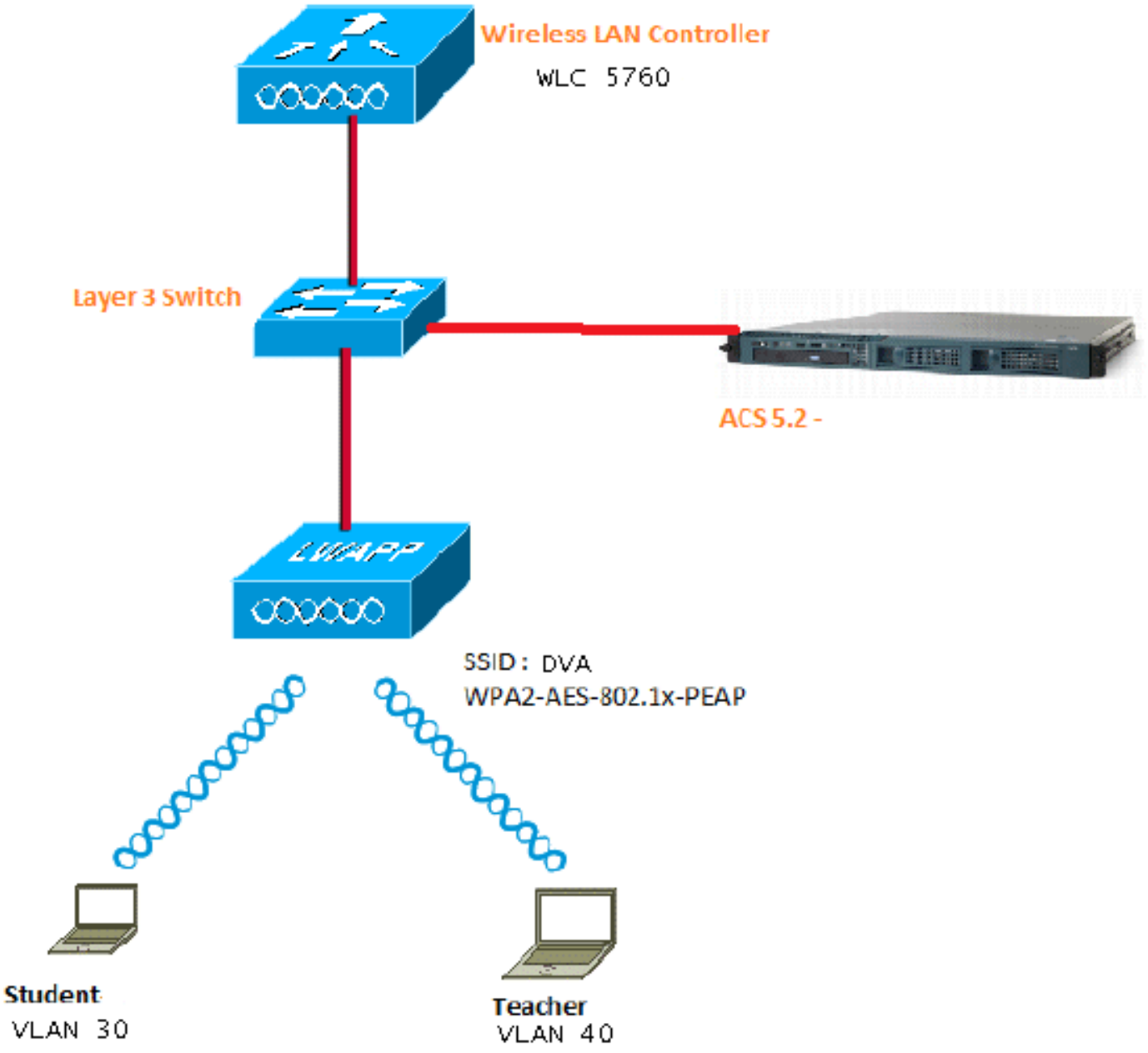
동적 VLAN 할당 구성은 두 가지 단계로 구성됩니다.

1. CLI(Command Line Interface) 또는 GUI를 사용하여 WLC를 구성합니다.
2. RADIUS 서버를 구성합니다.

   참고: 이 섹션에 사용된 명령에 대한 자세한 내용을 보려면 Command Lookup Tool(등록된 고객만 해당)을 사용합니다.

네트워크 다이어그램

이 문서에서는 다음 네트워크 설정을 사용합니다.



이 문서에서는 PEAP(Protected Extensible Authentication Protocol)가 포함된 802.1X를 보안 메커니즘으로 사용합니다.

가정

- 스위치는 모든 레이어 3(L3) VLAN에 대해 구성됩니다.
- DHCP 서버에 DHCP 범위가 할당됩니다.
- 네트워크의 모든 디바이스 간에 L3 연결이 존재합니다.
- LAP가 이미 WLC에 조인되었습니다.
- 각 VLAN에는 /24 마스크가 있습니다.
- ACS 5.2에 자체 서명 인증서가 설치되어 있습니다.

CLI로 WLC 구성

WLAN 구성

다음은 DVA의 SSID로 WLAN을 구성하는 방법의 예입니다.

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

WLC에서 RADIUS 서버 구성

다음은 WLC에서 RADIUS 서버를 구성하는 예입니다.

```
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
```

클라이언트 VLAN에 대한 DHCP 풀 구성

다음은 클라이언트 VLAN 30 및 VLAN 40에 대한 DHCP 풀 컨피그레이션의 예입니다.

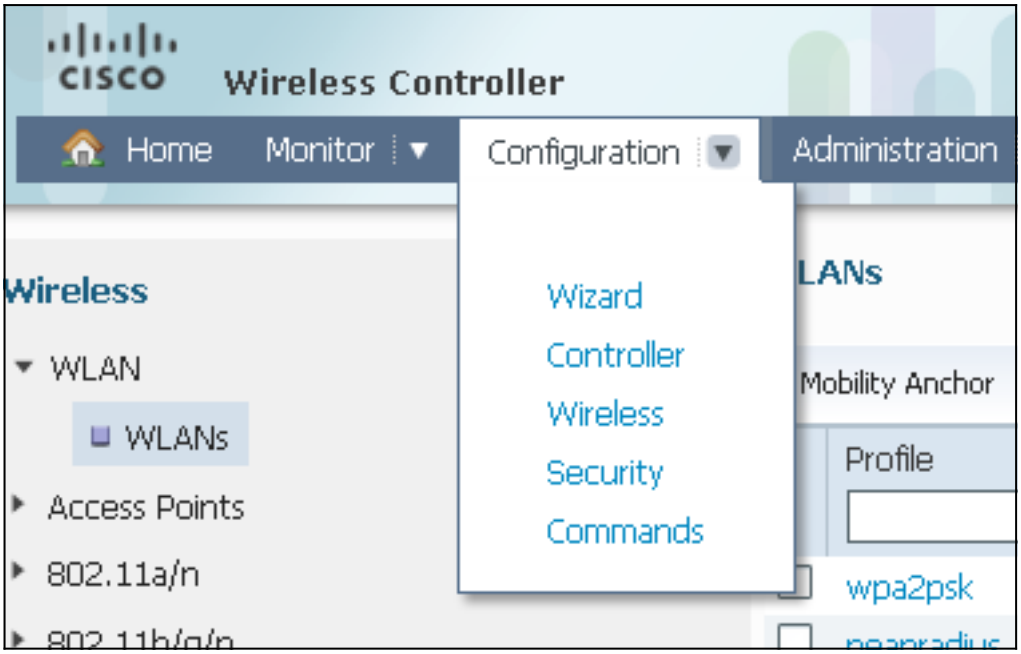
```
interface Vlan30
 ip address 30.30.30.1 255.255.255.0
!
interface Vlan40
 ip address 40.40.40.1 255.255.255.0

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
```

GUI를 사용하여 WLC 구성

WLAN 구성

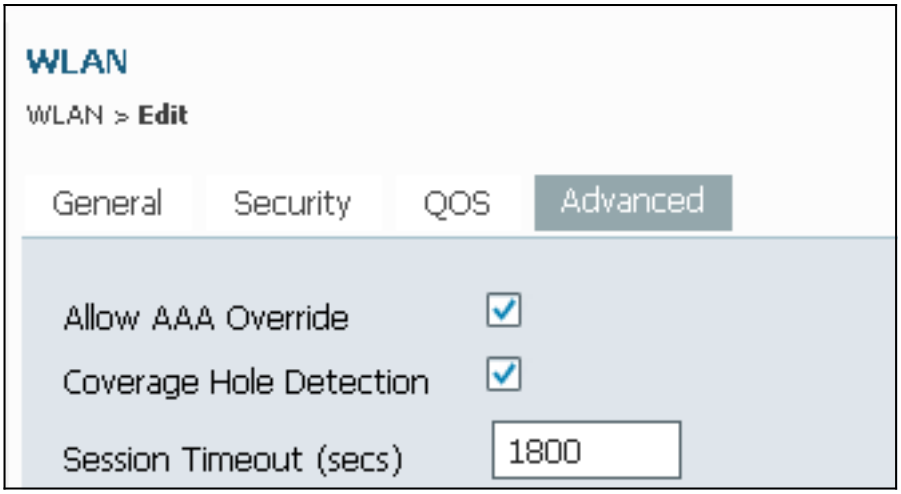
이 절차에서는 WLAN을 구성하는 방법을 설명합니다.

1. Configuration(컨피그레이션) > **Wireless(무선)** > **WLAN** > **NEW** 탭으로 이동합니다.

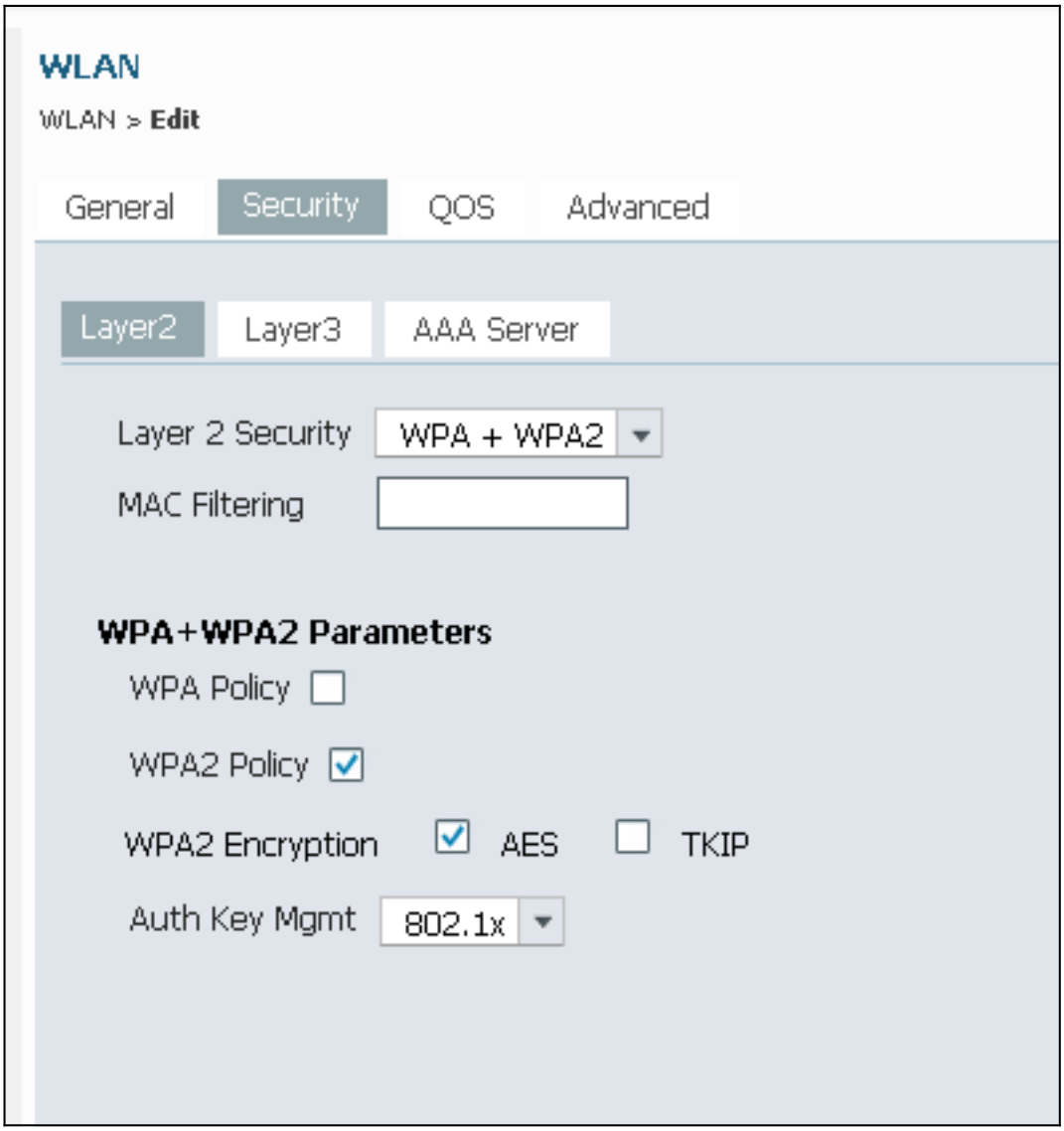


2. WLAN이 WPA2-802.1X에 대해 구성되어 있는지 확인하고 인터페이스/인터페이스 그룹(G)을 VLAN 20(VLAN0020)에 매핑하려면 **일반** 탭을 클릭합니다.

3. Advanced(**고급**) 탭을 클릭하고 Allow **AAA Override(AAA 재정의 허용**) 확인란을 선택합니다. 이 기능이 작동하려면 재지정을 활성화해야 합니다.



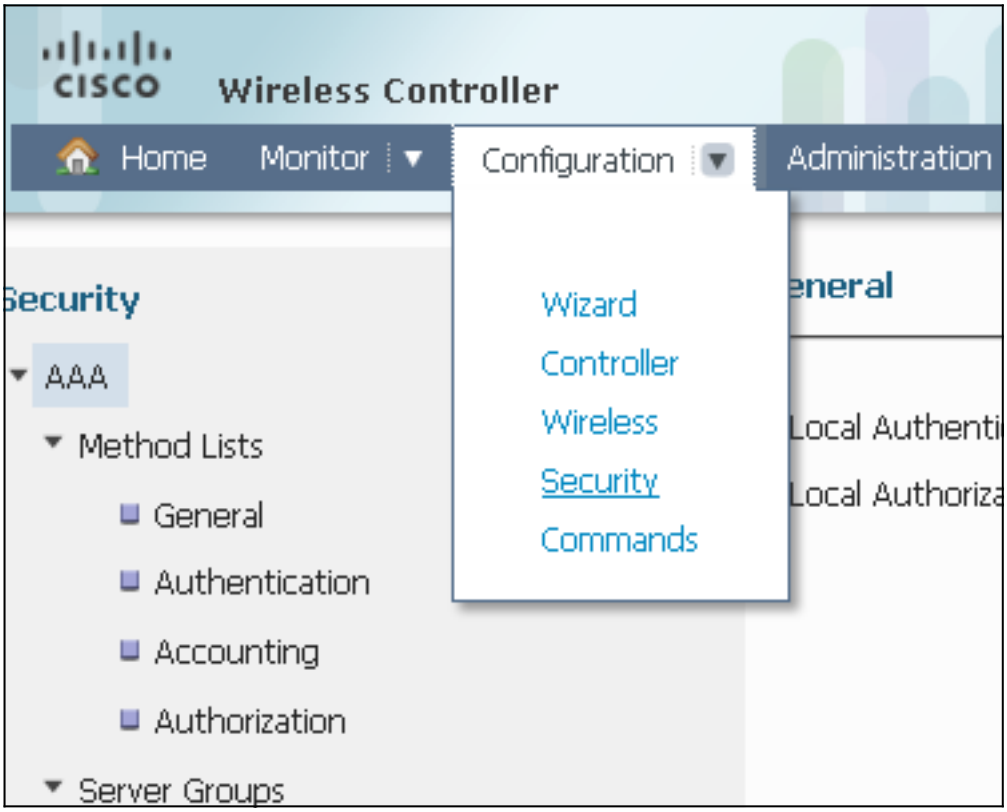
4. Security(**보안**) 탭 및 **Layer2** 탭을 클릭하고 WPA2 Encryption **AES** 확인란을 선택한 다음 Auth Key Mgmt(인증 키 관리) 드롭다운 목록에서 802.1x를 선택합니다.



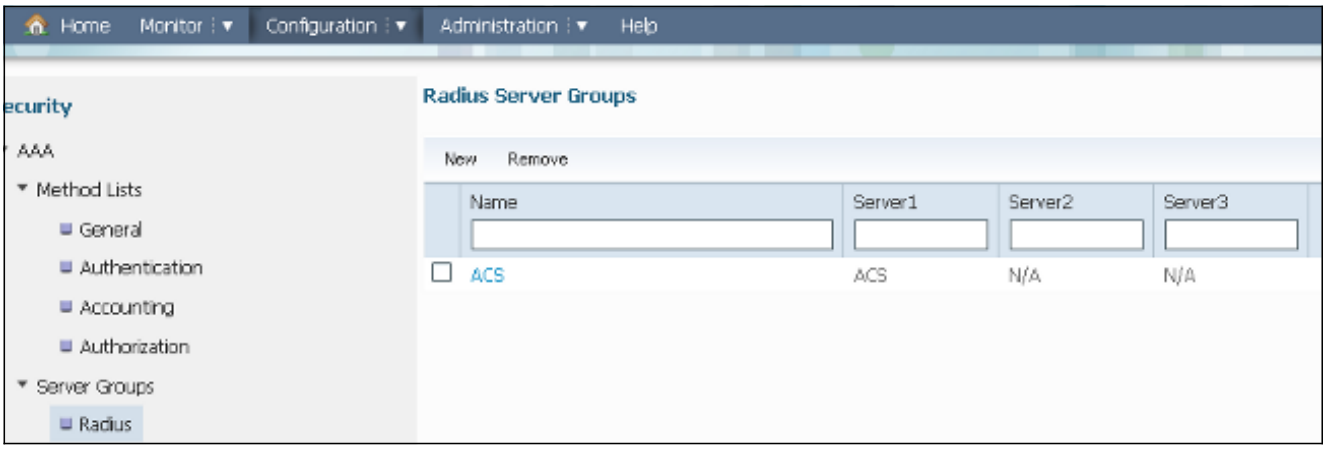
WLC에서 RADIUS 서버 구성

이 절차에서는 WLC에서 RADIUS 서버를 구성하는 방법을 설명합니다.

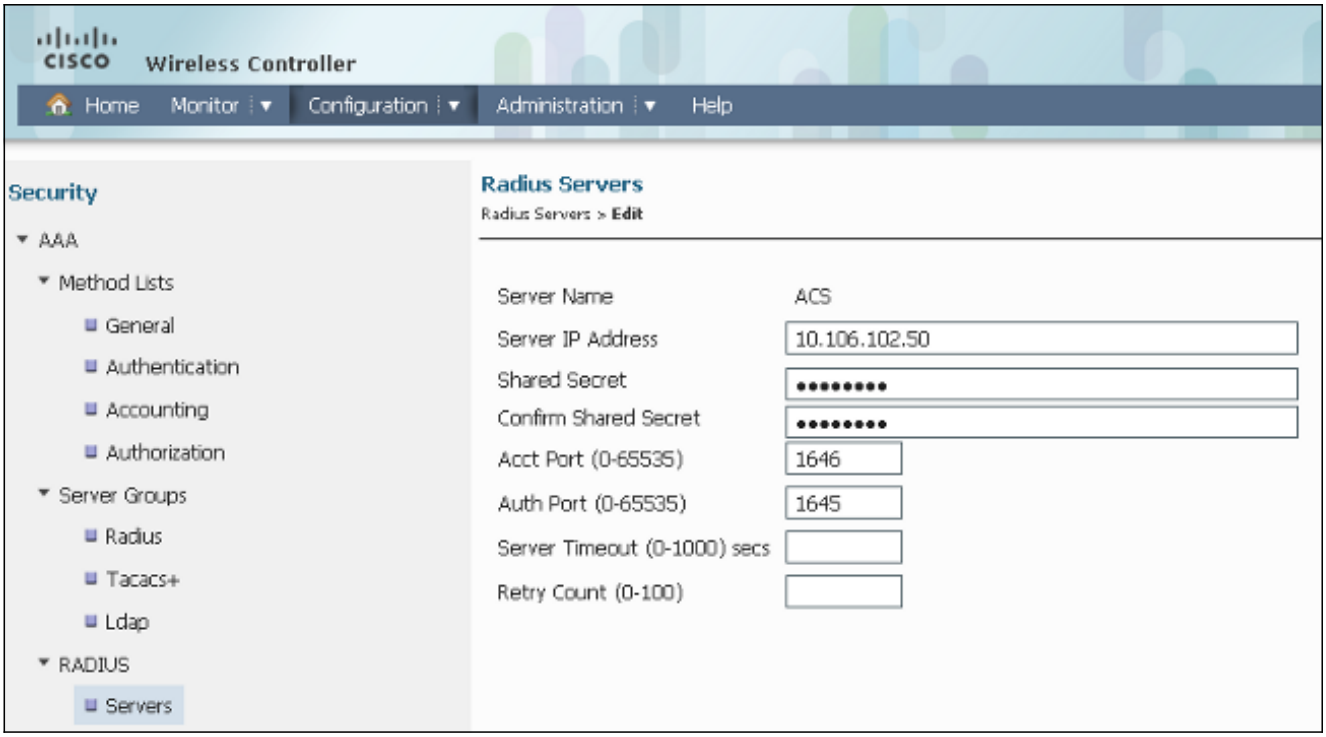
1. Configuration(컨피그레이션) > **Security(보안**) 탭으로 이동합니다.



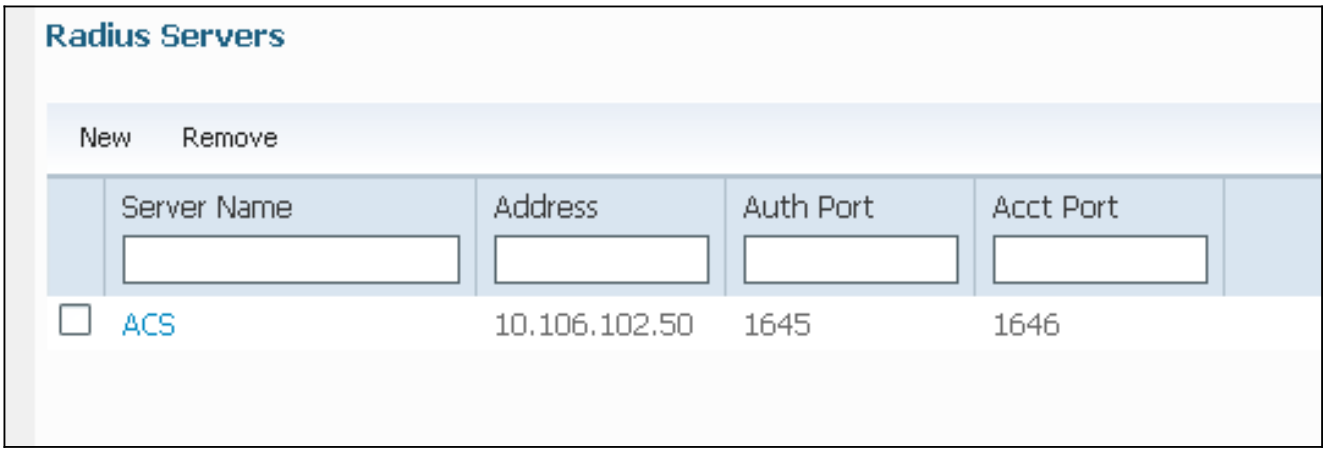
2. Radius 서버 그룹을 생성하려면 **AAA > Server Groups > Radius**로 이동합니다. 이 예에서는 Radius 서버 그룹을 ACS라고 합니다.



3. 서버 IP 주소 및 공유 암호를 추가하려면 Radius 서버 항목을 편집합니다. 이 공유 암호는 WLC 및 RADIUS 서버의 공유 암호와 일치해야 합니다.



다음은 전체 컨피그레이션의 예입니다.

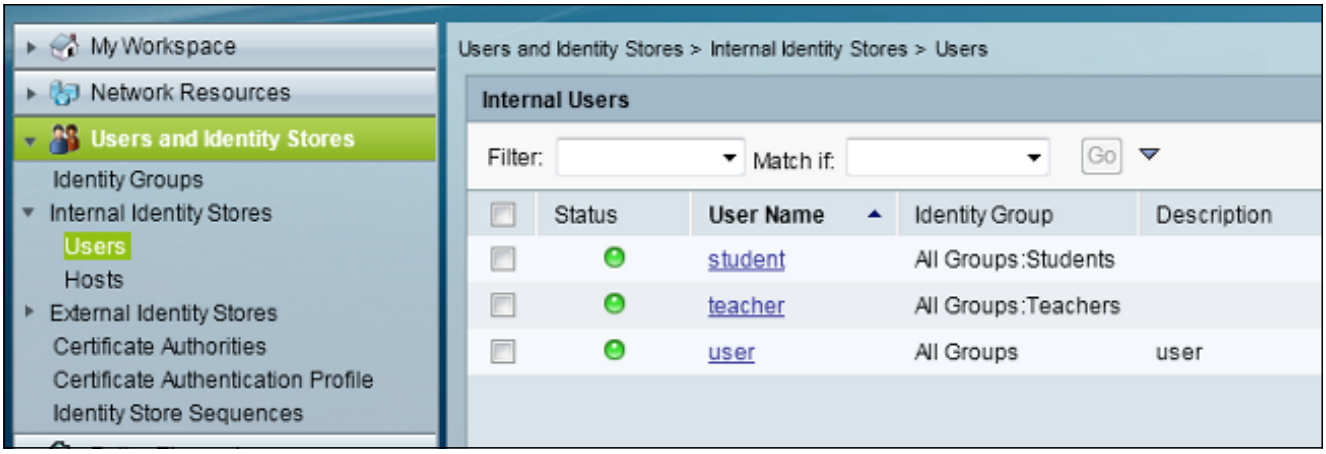


RADIUS 서버 구성

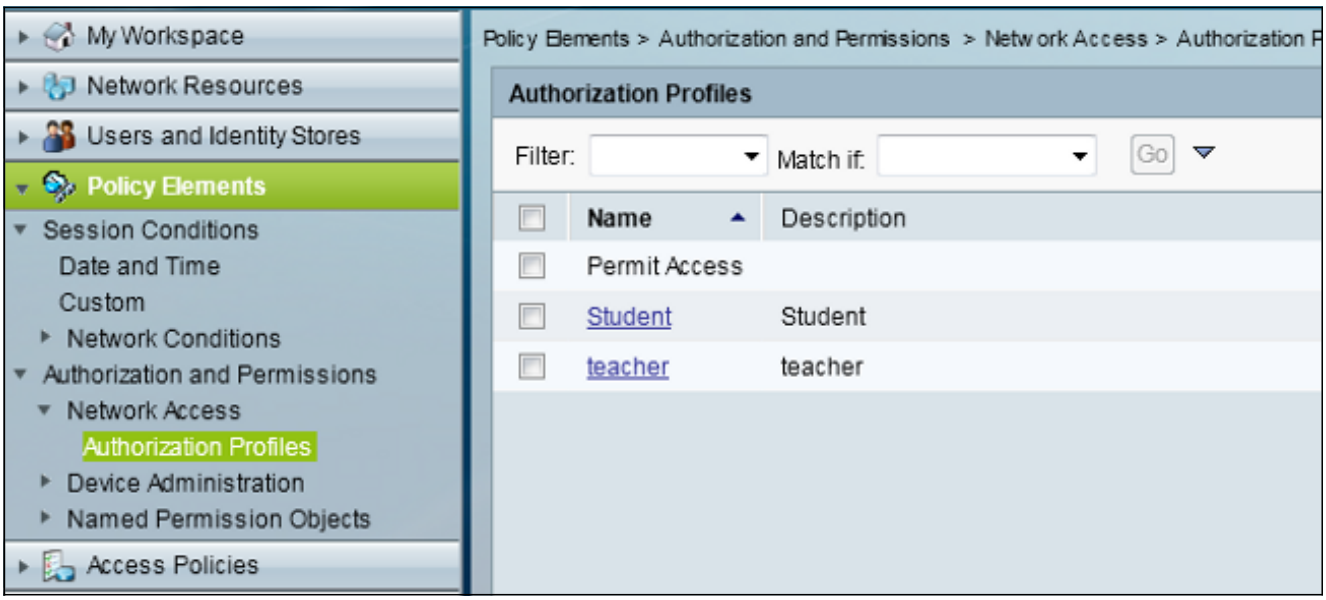
이 절차에서는 RADIUS 서버를 구성하는 방법을 설명합니다.

1. RADIUS 서버에서 Users and **Identity Stores(사용자 및 ID 저장소) > Internal Identity Stores(내부 ID 저장소)** > Users(**사용자)로** 이동합니다.

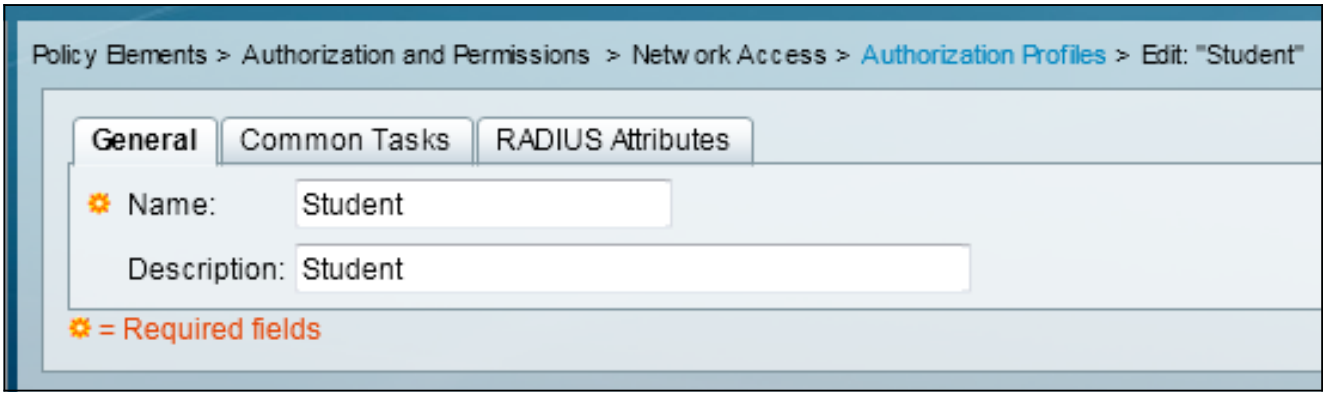
2. 적절한 사용자 이름 및 ID 그룹을 생성합니다. 이 예제에서는 Student 및 All Groups:Students, Teacher 및 AllGroups:Teachers입니다.



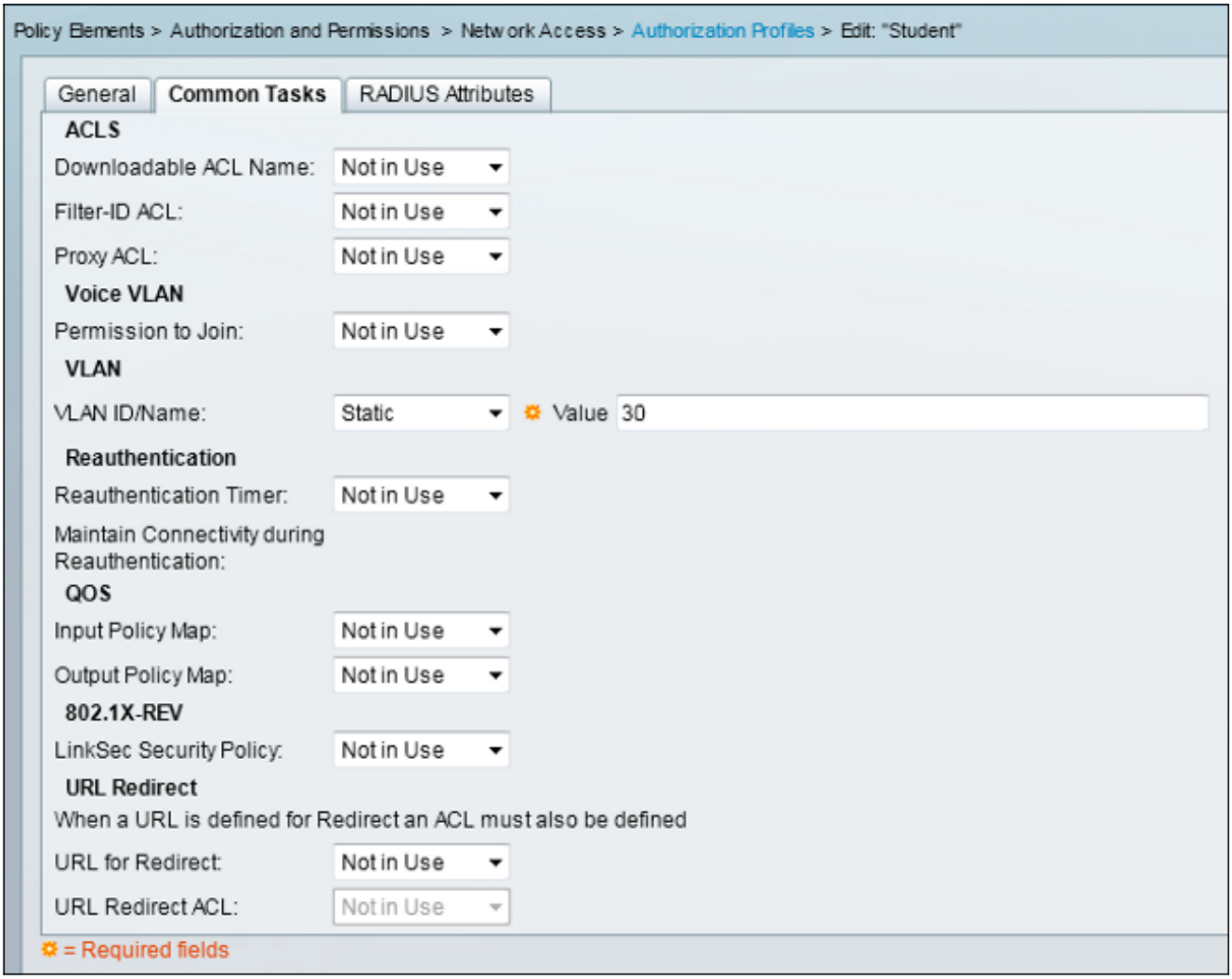
3. Policy Elements(**정책 요소**) > Authorization and **Permissions(권한 부여 및 권한)** > Network Access(네트워크 액세스) > **Authorization Profiles(권한 부여 프로파일**)로 이동하여 AAA 재정의에 대한 권한 부여 프로파일을 생성합니다.



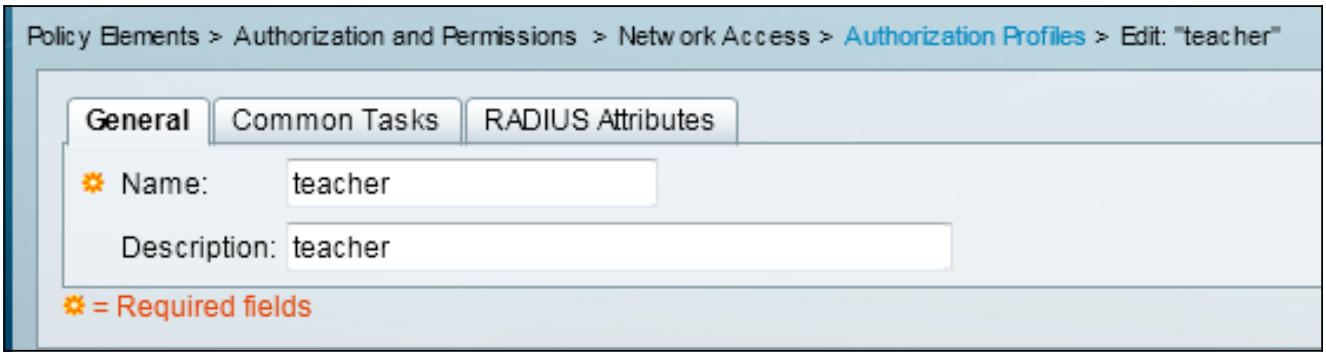
4. Authorization Profile for Student를 수정합니다.



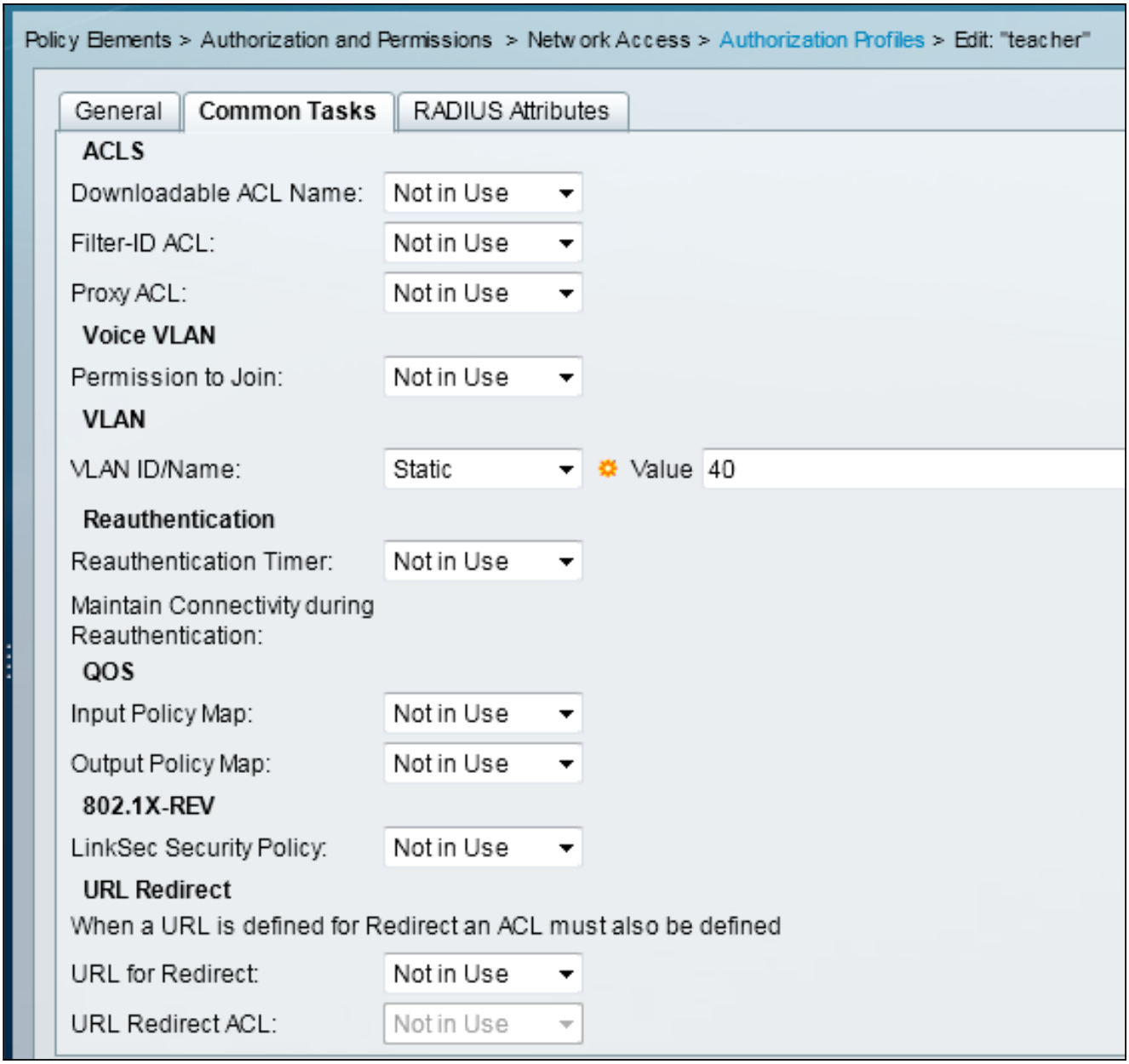
5. VLAN ID/Name을 **30**(VLAN 30) 값으로 **Static**으로 설정합니다.



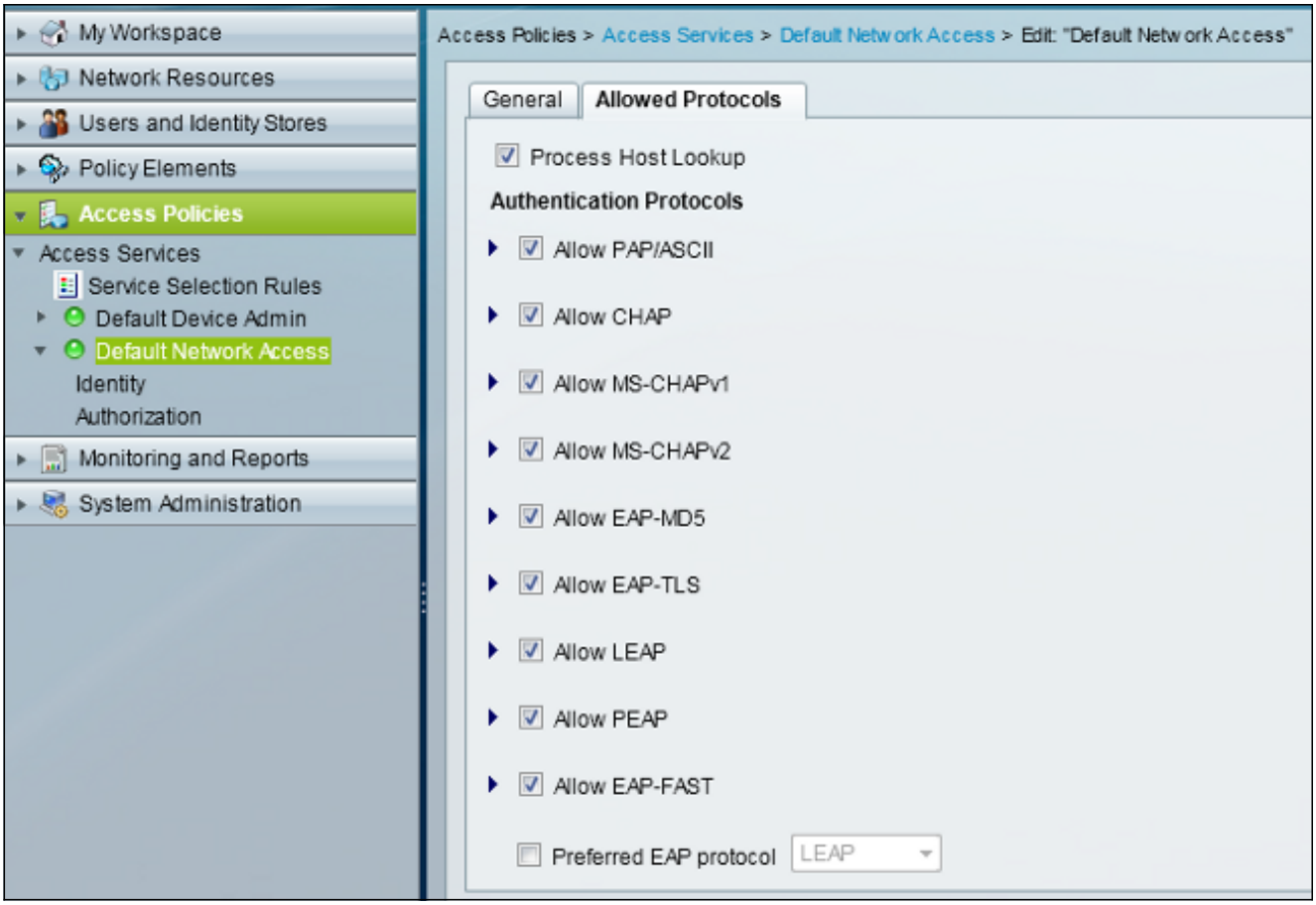
6. 교사의 권한 부여 프로파일을 편집합니다.



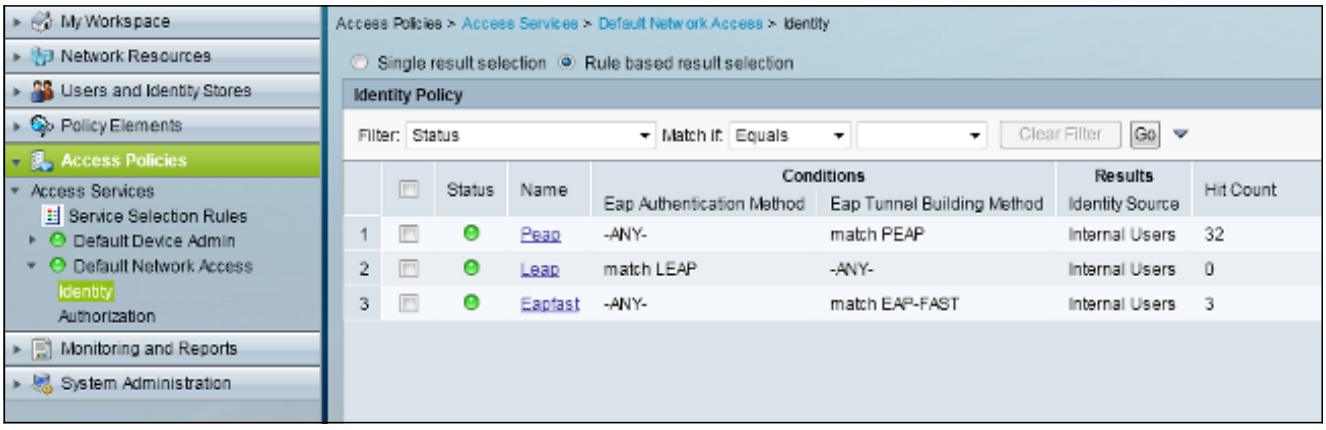
7. VLAN ID/Name을 **40**(VLAN 40) 값으로 **Static**으로 설정합니다.



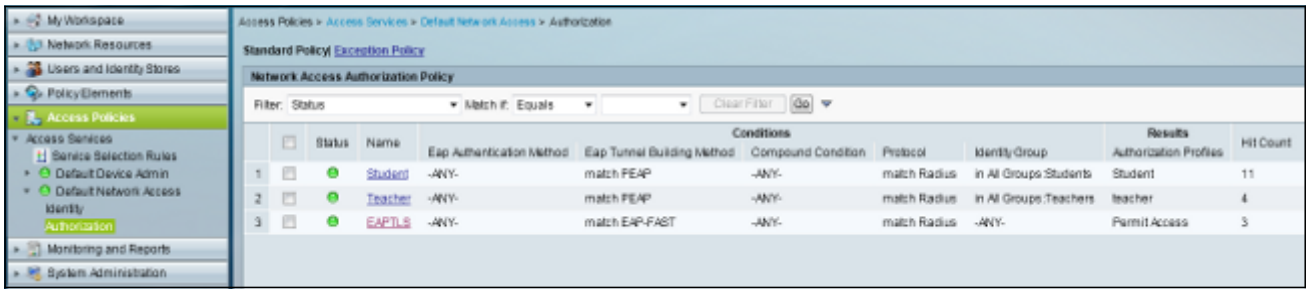
8. Access Policies(**액세스 정책**) > **Access Services(액세스 서비스)** > **Default Network Access(기본 네트워크 액세스)**로 이동하고 **Allowed Protocols(허용되는 프로토콜)** 탭을 클릭합니다. Allow PEAP(**PEAP 허용)** 확인란을 선택합니다.



9. PEAP 사용자를 허용하기 위해 Identity로 이동하고 규칙을 정의합니다.



10. Authorization(권한 **부여)**으로 이동하고 Student and Teacher(학생 및 교사)를 권한 부여 정책에 매핑합니다. 이 예에서 매핑은 VLAN 30의 Student와 VLAN 40의 Teacher여야 합니다.

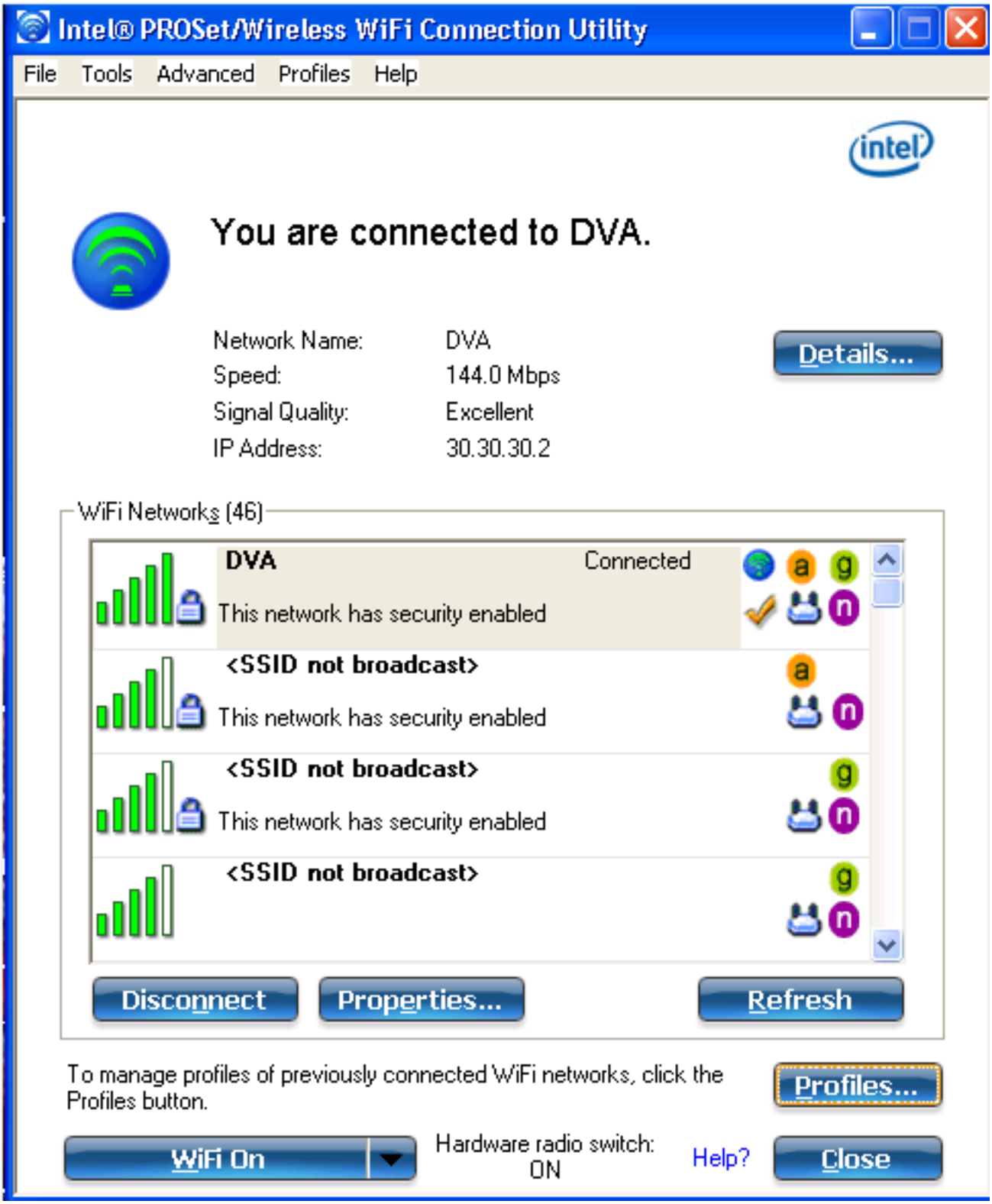


다음을 확인합니다.

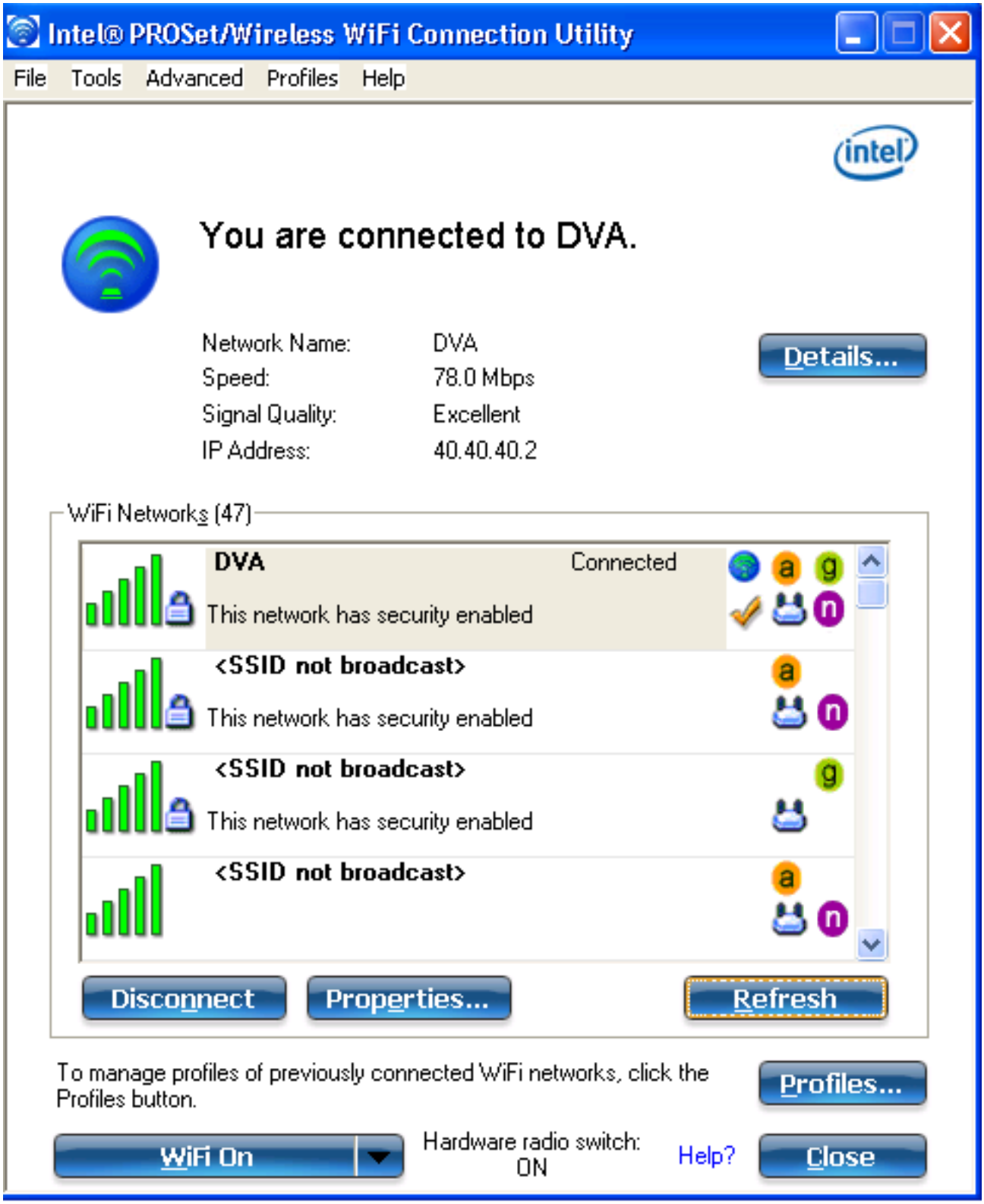
이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다. 다음은 확인 프로세스입니다.

- ACS에서 인증된 클라이언트를 보여 주는 페이지를 모니터링합니다.

- 학생 그룹을 사용하여 DVA WLAN에 연결하고 클라이언트 WiFi 연결 유틸리티를 검토합니다.



- 교사 그룹을 사용하여 DVA WLAN에 연결하고 클라이언트 WiFi 연결 유틸리티를 검토합니다.



문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

참고:

이 섹션에 사용된 명령에 대한 자세한 내용을 보려면 Command Lookup Tool(등록된 고객만 해당)을 사용합니다.

Output Interpreter 도구(등록된 고객만 해당)는 특정 **show** 명령을 지원합니다. **show** 명령 출력의 분석을 보려면 [출력 인터프리터 도구]를 사용합니다.

debug 명령을 사용하기 전에 디버그 명령에 대한 중요 정보를 참조하십시오.

유용한 디버깅에는 **debug client mac-address** *mac*과 다음 NGWC trace 명령이 포함됩니다.

- **trace group-wireless-client level debug 설정**
- **trace group-wireless-client filter mac 설정** *xxxx.xxxx.xxxx*
- **show trace sys 필터링된 추적**

NGWC 추적에는 dot1x/AAA가 포함되지 않으므로 dot1x/AAA에 대해 결합된 전체 추적 목록을 사용합니다.

- **trace group-wireless-client level debug 설정**
- **trace wcm-dot1x 이벤트 수준 디버그 설정**
- **trace wcm-dot1x aaa 레벨 디버그 설정**
- **trace aaa 무선 이벤트 수준 디버그**
- **trace access-session core sm level debug 설정**
- **trace access-session method dot1x level debug 설정**
- **trace group-wireless-client filter mac 설정** *xxxx.xxxx.xxxx*
- **trace wcm-dot1x 이벤트 필터 mac 설정** *xxxx.xxxx.xxxx*
- **trace wcm-dot1x aaa 필터 mac 설정** *xxxx.xxxx.xxxx*
- **trace aaa 무선 이벤트 필터 mac 설정** *xxxx.xxxx.xxxx*
- **trace access-session core sm 필터 mac 설정** *xxxx.xxxx.xxxx*
- **trace access-session method dot1x filter mac 설정** *xxxx.xxxx.xxxx*
- **show trace sys 필터링된 추적**

동적 VLAN 할당이 올바르게 작동하는 경우 디버그의 출력 유형을 확인해야 합니다.

```
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)