# Dynamic VLAN Assignment with Converged Access and ACS 5.2 Configuration Example

This document describes the concept of dynamic VLAN assignment and how to configure wireless LAN controller (WLC) and a RADIUS server to assign a 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.oduction

# Prerequisites

We recommend that you have basic and functional knowledge on following topics:

- WLC and Lightweight Access Points (LAPs)
- Authentication, Authorization and Accounting (AAA) server
- Wireless networks and wireless security issues

## Supported Platforms and Releases

The information in this document is based on the following:

- Cisco Catalyst 3850 series Switches Wireless LAN Controller with Cisco IOS® XE Software Release 3.2.2
- Cisco Aironet 3600 Series Lightweight Access Point
- Microsoft Windows XP with Intel Proset Supplicant

- Cisco Secure Access Control System Version 5.2
- Cisco Catalyst 3500 Series Switches

**Note** 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

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 this static policy is powerful, it has some limitations since it requires clients to associate with different SSIDs in order to inherit different QoS and security policies.

Cisco WLAN solution supports identity networking that allows the network to advertise a single SSID, only for 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, i.e. 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 of both 1 and 4094). The Tunnel-Private-Group-ID is of type string for use with IEEE 802.1X. Therefore, 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.

# Configuring Dynamic VLAN Assignment

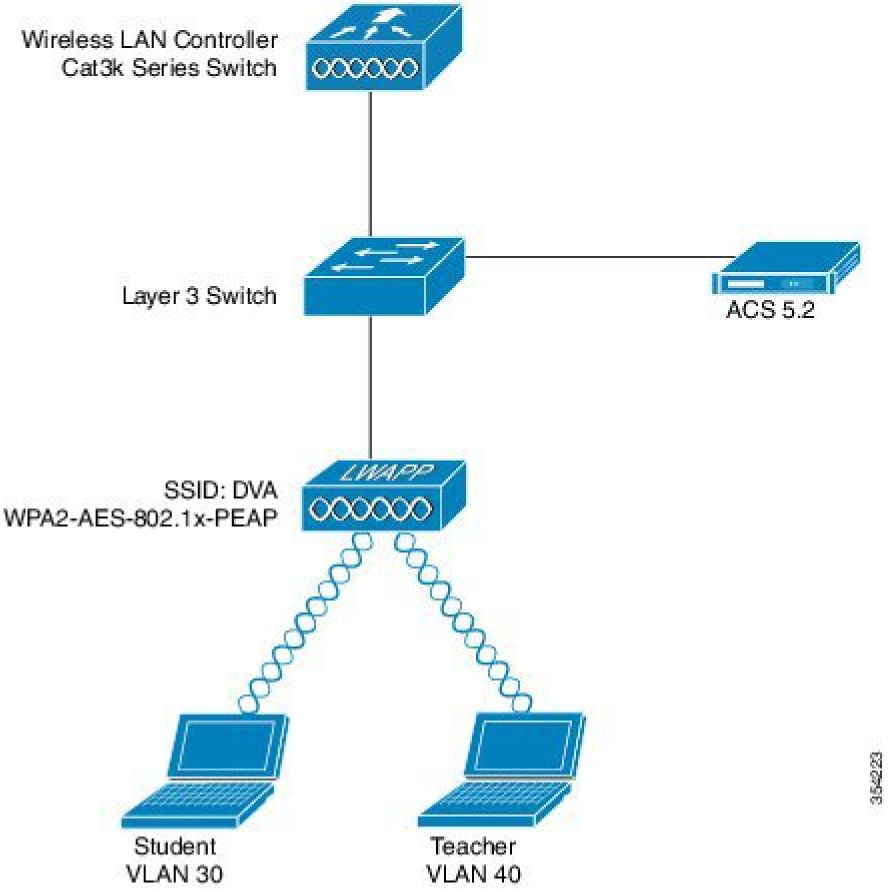
Configuring dynamic VLAN assignment is a two-step process which includes:

- Configuring WLC with the Command-Line Interface (CLI) or with the Graphical User Interface (GUI).
- Configuring RADIUS server.

## Network Diagram of Dynamic VLAN Assignment

The following figure shows the network setup of Dynamic VLAN Assignment with Converged Access and ACS 5.2

*Figure 1: Network setup of Dynamic VLAN Assignment with Converged Access*



Security mechanism used in this document is 802.1X with Protected Extensible Authentication Protocol (PEAP).

Make sure the following tasks are completed before you starts with configuration:

- 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.

# Configuring WLC (CLI)

This section shows configuring WLAN, RADIUS Server and DHCP Pool for Client VLAN.

### Configuring WLAN

The following example shows how WLAN is configured with the SSID of DVA:

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

### Configuring RADIUS Server on WLC

Configuring the RADIUS server on WLC is shown in the below example:

```
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
```

### Configuring DHCP Pool for Client VLAN

This is an example to configure DHCP pool for the client VLAN 30 and VLAN 40:

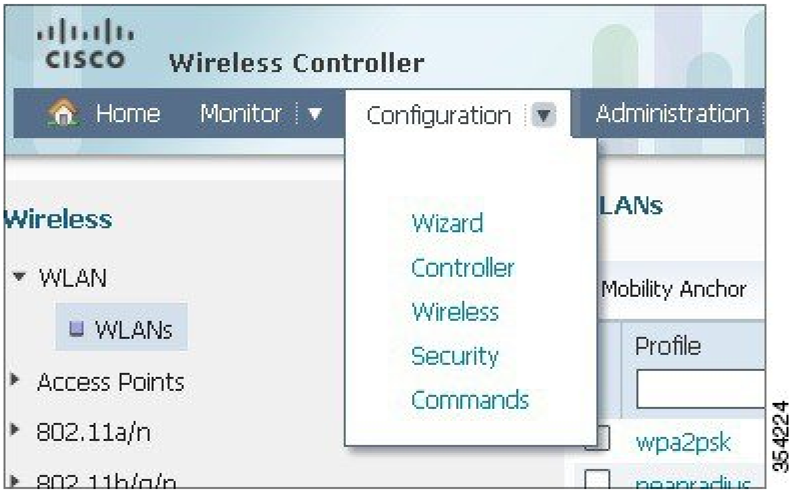
```
interface Vlan30
ip address 30.30.30.1 255.255.255.0
!
interface Vlan40
ip address 40.40.40.1 255.255.255.0

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
```

# Configuring WLAN (GUI)

Perform the following tasks to configure WLAN.

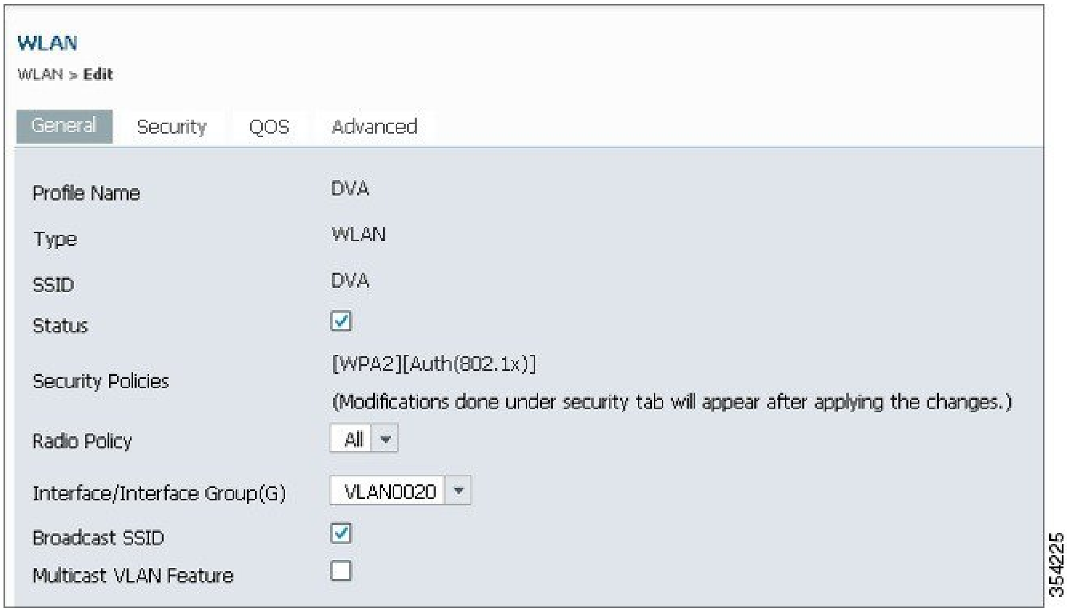
**Step 1** Navigate to **Configuration** > **Wireless** > **WLAN** > **NEW.**

*Figure 2: Configuring WLAN window*



**Step 2** Click the **General** tab to verify that the WLAN is configured for WPA2-802.1X, and Interface / Interface Group (G) is mapping to *VLAN 20* (*VLAN0020*).

*Figure 3: Verifying the WLAN configuration*



WLAN

WLAN > Edit

Profile Name DVA

Type WLAN

SSID DVA

Status ☑

Security Policies [WPA2][Auth(802.1x)]
(Modifications done under security tab will appear after applying the changes.)

Radio Policy All

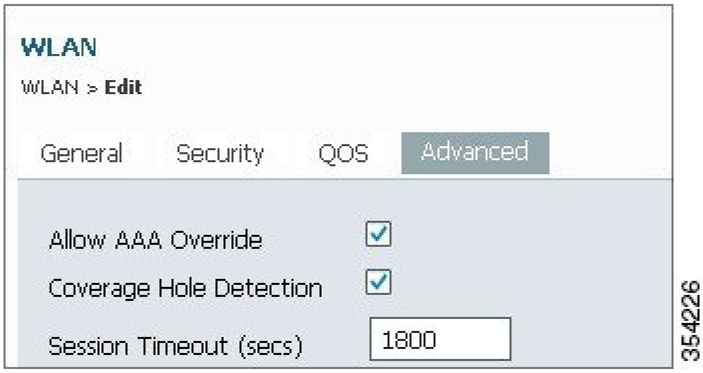
Interface/Interface Group(G) VLAN0020

Broadcast SSID ☑

Multicast VLAN Feature □

**Step 3** To enable the AAA Override, click the **Advanced** tab and check **Allow AAA Override** check box.

*Figure 4: Enabling the AAA Override*



WLAN

WLAN > Edit

Allow AAA Override ☑

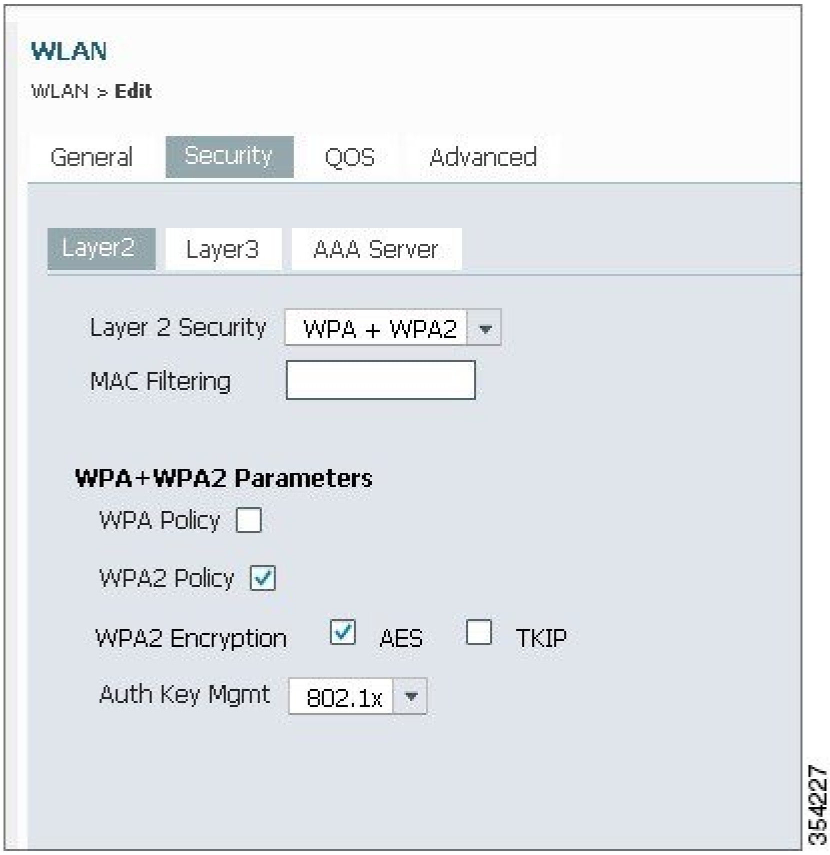
Coverage Hole Detection ☑

Session Timeout (secs) 1800

**Step 4** Click the **Layer2** tab under the **Security** tab, and check **AES** check box as WPA2 Encryption.

**Step 5** Choose *802.1x* as **Auth Key Mgmt** from drop-down list.

***Figure 5: Selecting the Auth Key Management***



WLAN

WLAN > **Edit**

Layer 2 Security: WPA + WPA2

MAC Filtering:

**WPA+WPA2 Parameters**

WPA Policy □

WPA2 Policy ☑

WPA2 Encryption ☑ AES □ TKIP

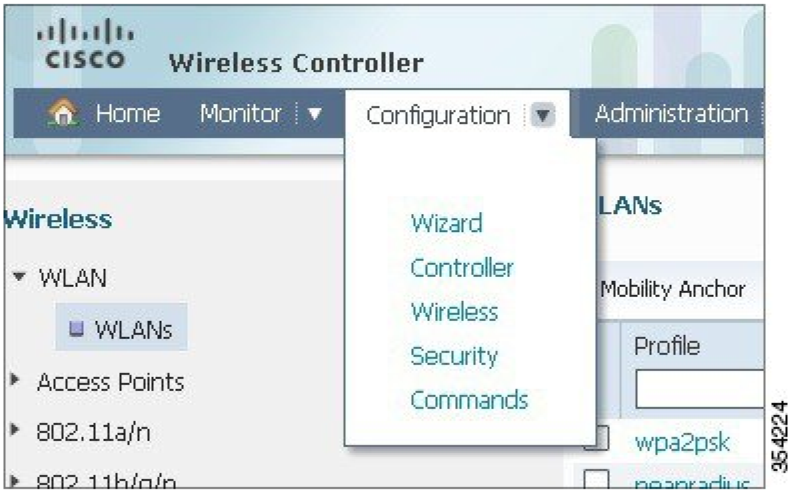
Auth Key Mgmt: 802.1x

# Configuring RADIUS Server on WLC (GUI)

The following section describes how to configure RADIUS server on WLC.

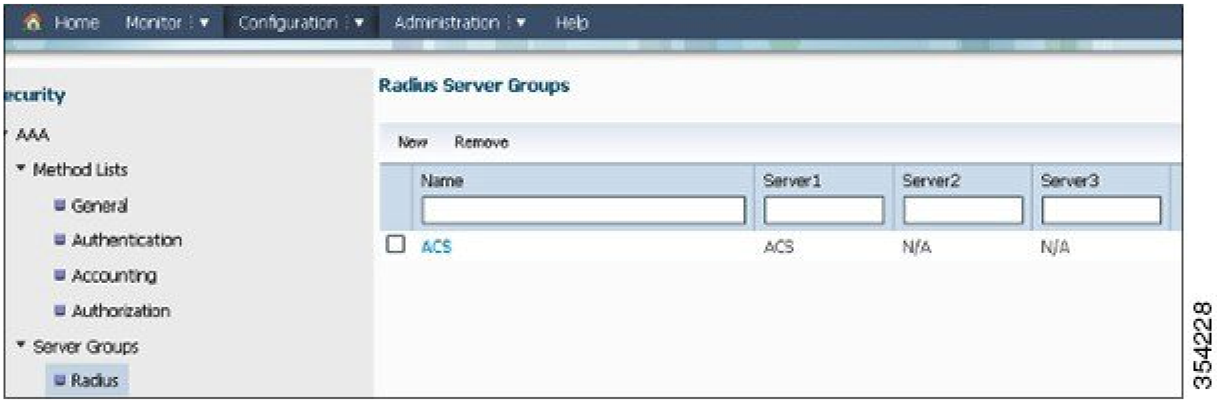
**Step 1** Navigate to **Configuration** > **Security.**

*Figure 6: Configuring Radius Server on WLC*



**Step 2** To create the Radius Server Groups, navigate to **AAA** > **Server Groups** > **Radius** (In this example, the Radius Server Group is named as **ACS**).

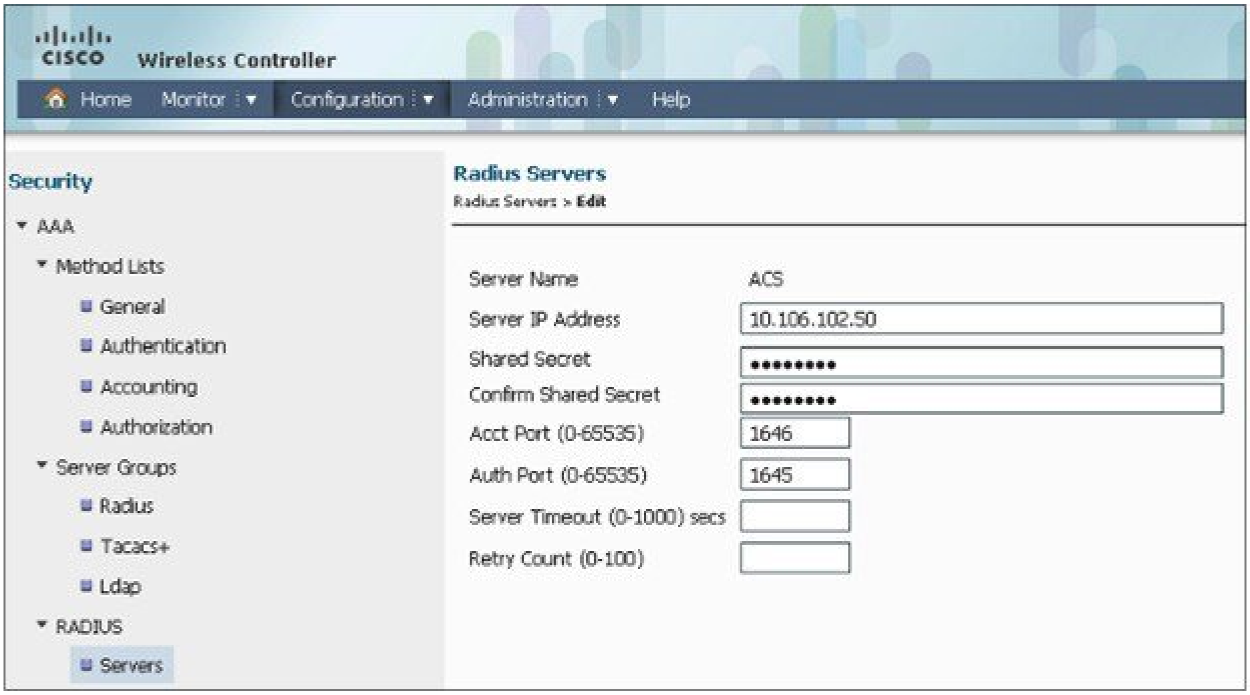
*Figure 7: Creating radius server group*



| | Name | Server1 | Server2 | Server3 |
|---|---|---|---|---|
| □ | ACS | ACS | N/A | N/A |

**Step 3** Edit the Radius Server entry to add the Server IP Address and the Shared Secret.

*Figure 8: Editing radius server*



Radius Servers

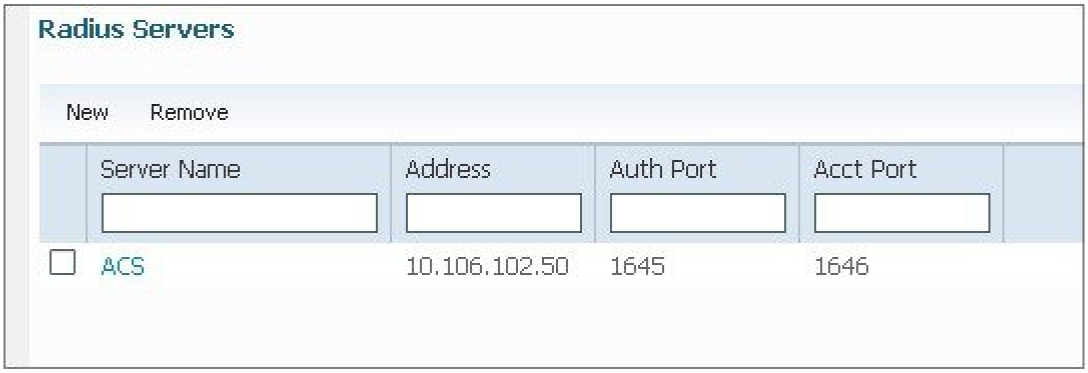
Radius Servers > Edit

| | |
|---|---|
| Server Name | ACS |
| Server IP Address | 10.106.102.50 |
| Shared Secret | ••••••••• |
| Confirm Shared Secret | ••••••••• |
| Acct Port (0-65535) | 1646 |
| Auth Port (0-65535) | 1645 |
| Server Timeout (0-1000) secs | |
| Retry Count (0-100) | |

**Note** The Shared Secret entered must be same as Shared Secret on the WLC and the RADIUS server.

**Step 4** The following figure shows, example of a complete configuration of Radius Server on WLC.

*Figure 9: Radius server example*



Radius Servers

| | Server Name | Address | Auth Port | Acct Port |
|---|---|---|---|---|
| □ | ACS | 10.106.102.50 | 1645 | 1646 |

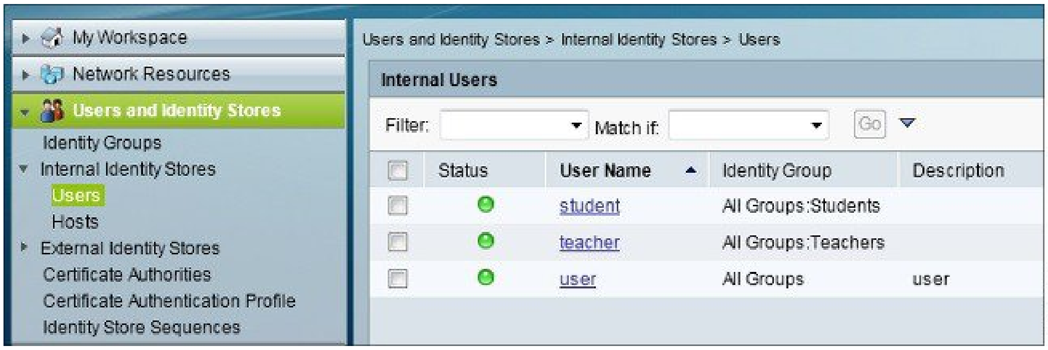
# Configuring RADIUS Server

Perform the following tasks to configure the RADIUS server.

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

**Step 2** Create the appropriate User Names and Identity Groups. In this example, student and teacher are created as Usernames and similarly All Groups:Students, and AllGroups:Teachers are created as Identity Groups.

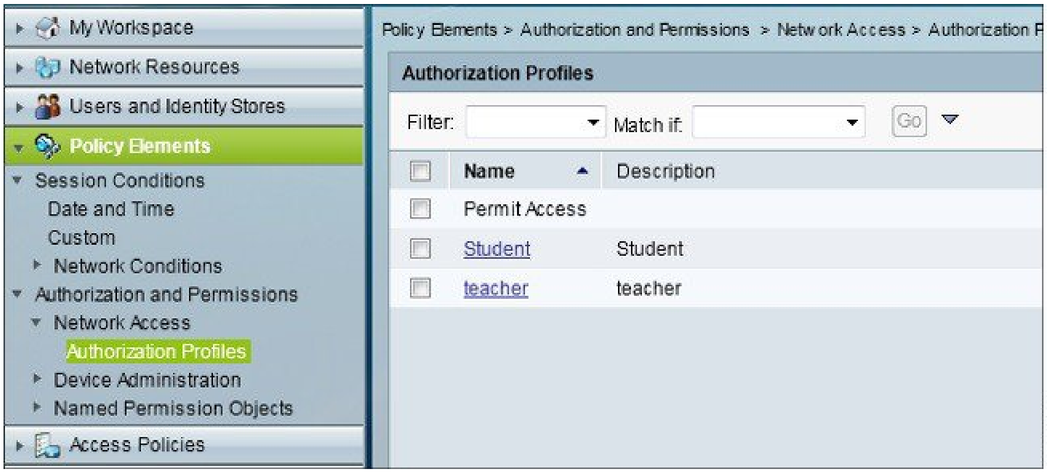
***Figure 10: Creating user names and identity groups***



| □ | Status | User Name ▲ | Identity Group | Description |
|---|---|---|---|---|
| □ | ● | student | All Groups:Students | |
| □ | ● | teacher | All Groups:Teachers | |
| □ | ● | user | All Groups | user |

**Step 3** Create the Authorization Profiles for AAA override by navigating to **Policy Elements** > **Authorization and Permissions** > **Network Access** > **Authorization Profiles.**

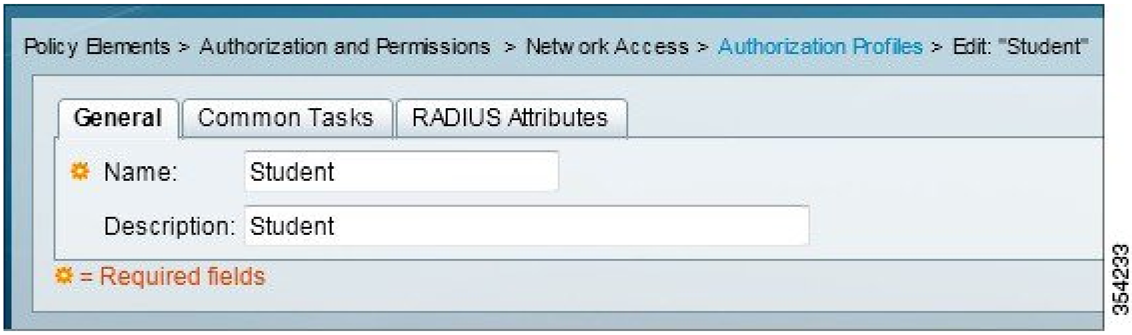
***Figure 11: Creating the auth profile***



| □ | Name ▲ | Description |
|---|---|---|
| □ | Permit Access | |
| □ | Student | Student |
| □ | teacher | teacher |

**Step 4** Edit the Authorization Profile for Student.

*Figure 12: Editing the auth profile*



Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles > Edit: "Student"

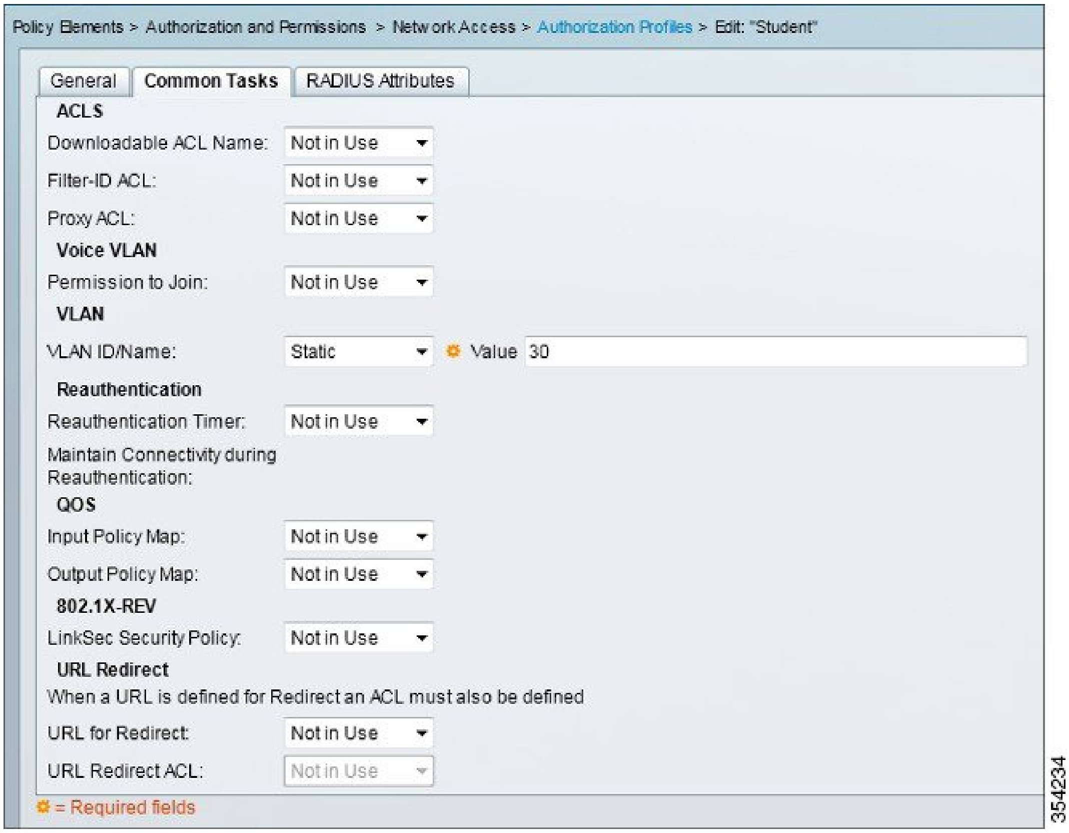
General | Common Tasks | RADIUS Attributes

| | |
|---|---|
| ✱ Name: | Student |
| Description: | Student |

✱ = Required fields

**Step 5** Set the VLAN ID/Name as **Static** using drop-down list and a Value of30 (VLAN 30) for student.

*Figure 13: Setting the VLAN*



Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles > Edit: "Student"

General | Common Tasks | RADIUS Attributes

| | |
|---|---|
| **ACLS** | |
| Downloadable ACL Name: | Not in Use |
| Filter-ID ACL: | Not in Use |
| Proxy ACL: | Not in Use |
| **Voice VLAN** | |
| Permission to Join: | Not in Use |
| **VLAN** | |
| VLAN ID/Name: | Static ✱ Value 30 |
| **Reauthentication** | |
| Reauthentication Timer: | Not in Use |
| Maintain Connectivity during Reauthentication: | |
| **QOS** | |
| Input Policy Map: | Not in Use |
| Output Policy Map: | Not in Use |
| **802.1X-REV** | |
| LinkSec Security Policy: | Not in Use |
| **URL Redirect** | |
| When a URL is defined for Redirect an ACL must also be defined | |
| URL for Redirect: | Not in Use |
| URL Redirect ACL: | Not in Use |

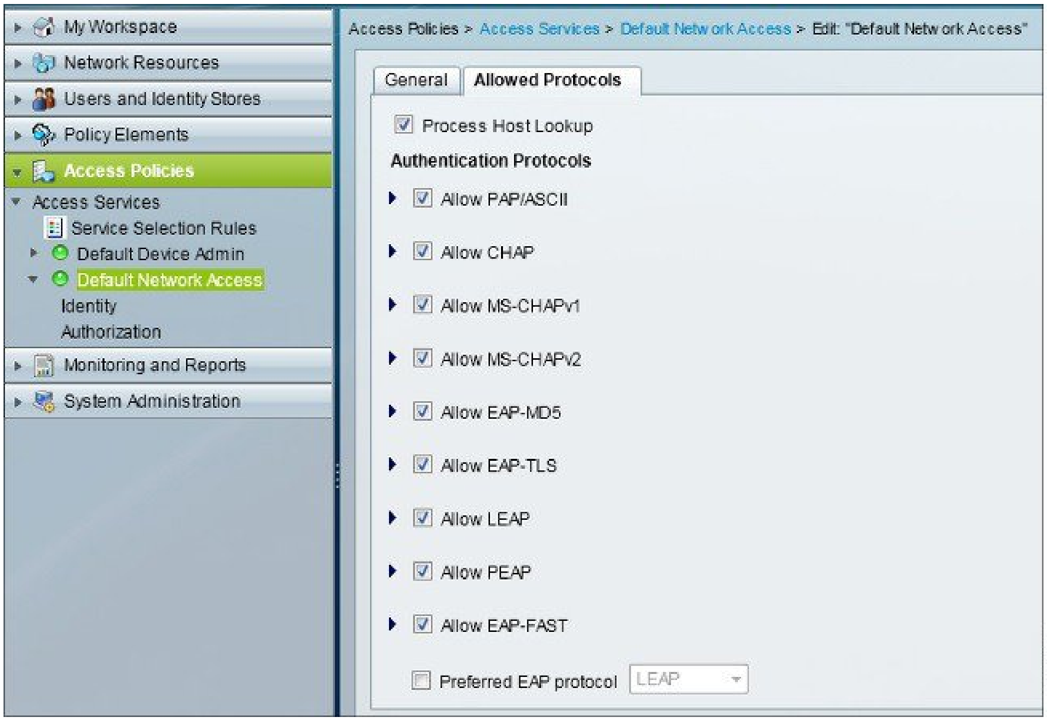
✱ = Required fields

**Step 6** Similarly, edit the Authorization Profile for Teacher.

**Step 7** Set the VLAN ID / Name as **Static** from drop-down list and a Value of 40 (VLAN 40) for teacher.

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

*Figure 14: Selecting allowed protocols*



☑ Process Host Lookup

Authentication Protocols

- ☑ Allow PAP/ASCII
- ☑ Allow CHAP
- ☑ Allow MS-CHAPv1
- ☑ Allow MS-CHAPv2
- ☑ Allow EAP-MD5
- ☑ Allow EAP-TLS
- ☑ Allow LEAP
- ☑ Allow PEAP
- ☑ Allow EAP-FAST

☐ Preferred EAP protocol LEAP

**Step 9** Define the rules in order to allow PEAP users by navigating to **Identity.**

**Step 10** Map Student and Teacher to the Authorization Policy by navigating to **Authorization**. In this configuration we mapped Student for VLAN30 and Teacher for VLAN 40.

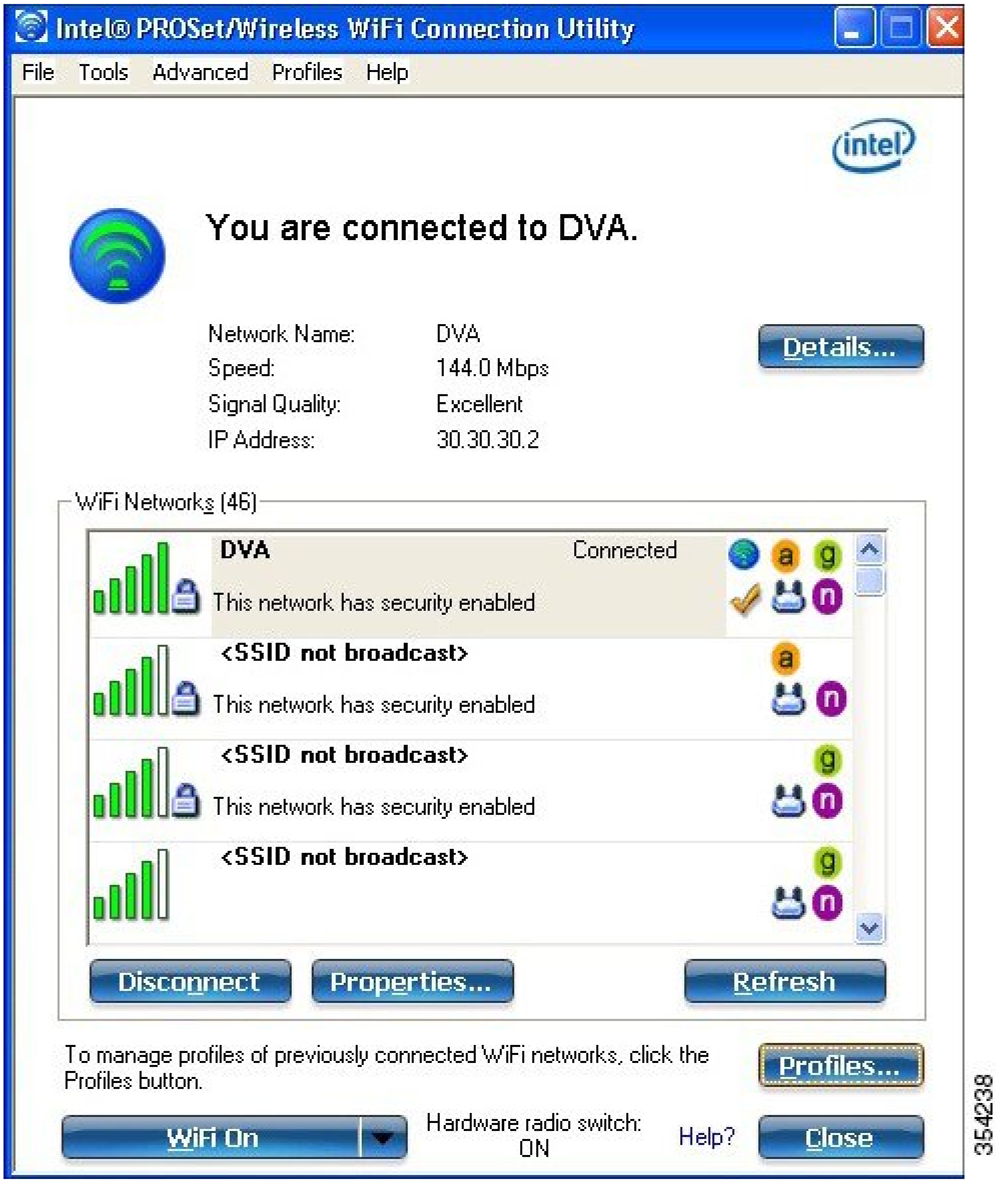
# Verifying the Dynamic VLAN Assignment with Converged Access Configuration

Perform the following task in order to verify Dynamic VLAN assignment with Converged Access configuration.

**Step 1** Monitor the page on the ACS that shows which clients are authenticated.

**Step 2** Connect to the DVA WLAN with Student Group, and review the client WiFi Connection Utility.

*Figure 15: Connecting to the DVA WLAN*



Intel® PROSet/Wireless WiFi Connection Utility

File Tools Advanced Profiles Help

You are connected to DVA.

| | |
|---|---|
| Network Name: | DVA |
| Speed: | 144.0 Mbps |
| Signal Quality: | Excellent |
| IP Address: | 30.30.30.2 |

WiFi Networks (46)

| | | |
|---|---|---|
| DVA | Connected | a g n |
| This network has security enabled | | |
| <SSID not broadcast> | | a n |
| This network has security enabled | | |
| <SSID not broadcast> | | g n |
| This network has security enabled | | |
| <SSID not broadcast> | | g n |

To manage profiles of previously connected WiFi networks, click the Profiles button.

Hardware radio switch: ON

**Step 3** Similarly, connect to the DVA WLAN with the Teacher Group, and review the client WiFi Connection Utility.

# Troubleshooting the Dynamic VLAN Assignment Configuration Issues

This section provides troubleshoot information of Dynamic VLAN Assignment with Converged Access configuration.

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

Useful debugs include **debug client mac-address** mac, as well as the following Converged Access 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 Converged Access 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 following type of output from the debugs as follows:

```
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)
```