Introduction
This document introduces the concept of dynamic VLAN assignment. It also describes how to configure the wireless LAN controller (WLC) and a RADIUS server − Access Control Server (ACS) that runs version 5.2 − in order to assign wireless LAN (WLAN) clients to a specific VLAN dynamically.

Prerequisites

Requirements

Make sure that you meet these requirements before you attempt this configuration:

- Have a basic knowledge of the WLC and Lightweight Access Points (LAPs)
- Have a functional knowledge of the AAA server
- Have a 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 5508 WLC that runs firmware release 7.0.220.0
- Cisco 3502 Series LAP
- Microsoft Windows 7 Native Supplicant with Intel 6300–N Driver Version 14.3
- Cisco Secure ACS that runs version 5.2
- Cisco 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.

Conventions

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

Dynamic VLAN Assignment with a 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 assigning users to a specific VLAN is handled by a RADIUS authentication server, such as Cisco Secure ACS. This can be used, for example, 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 (WLAN, in terms of WLC) of the client 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 this to VLAN.
- IETF 65 (Tunnel Medium Type) – Set this to 802.
- IETF 81 (Tunnel Private Group ID) – Set this to 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 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 this
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**

In this section, you are presented with the information to configure the features described in this document.

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

**Network Diagram**

This document uses this network setup:

- The IP address of the ACS (RADIUS) server is 192.168.150.24.
- The Management and AP–manager Interface address of the WLC is 192.168.75.44.
- The DHCP servers address 192.168.150.25.
- VLAN 253 and VLAN 257 are used throughout this configuration. Student−1 is configured for placement into VLAN 253 and Teacher−1 is configured for placement into VLAN 257 by the RADIUS server when both users connect to the same SSID "goa".

- **VLAN 253:** 192.168.153.x/24. Gateway: 192.168.153.1
Note: Cisco recommends that you use advanced authentication methods, such as EAP−FAST and EAP−TLS authentication, in order to secure the WLAN.

Assumptions

- Switches are configured for all Layer 3 VLANs.
- The DHCP server is assigned a DHCP scope.
- Layer 3 connectivity exists between all devices in the network.
- The LAP is already joined to the WLC.
- Each VLAN has /24 mask.
- ACS 5.2 has a Self−Signed Certificate installed.

Configuration Steps

This configuration is separated into three high−level steps:

1. Configure the RADIUS Server.
2. Configure the WLC.
3. Configure the Wireless Client Utility.

Configure the RADIUS Server

Configuration of RADIUS server is divided into four steps:

1. Configure network resources.
2. Configure users.
3. Define policy elements.
4. Apply access policies.

ACS 5.x is a policy−based access control system. That is, ACS 5.x uses a rule−based policy model instead of the group−based model used in the 4.x versions.

The ACS 5.x rule−based policy model provides more powerful and flexible access control compared to the older group−based approach.

In the older group−based model, a group defines policy because it contains and ties together three types of information:

- Identity information – This information can be based on membership in AD or LDAP groups or a static assignment for internal ACS users.
- Other restrictions or conditions – Time restrictions, device restrictions, and so on.
- Permissions – VLANs or Cisco IOS® privilege levels.

The ACS 5.x policy model is based on rules of the form:

- If condition then result

For example, we use the information described for the group−based model:
If identity-condition, restriction-condition then authorization-profile.

As a result, this gives us the flexibility to limit under what conditions the user is allowed to access the network as well as what authorization level is allowed when specific conditions are met.

**Configure Network Resources**

This procedure explains how to add the WLC as a AAA client on the RADIUS server so that the WLC can pass the user credentials to the RADIUS server.

Complete these steps:

1. From the ACS GUI, go to **Network Resources > Network Device Groups > Location**, and click **Create** (at the bottom).

2. Add the required fields, and click **Submit**.

You will now see this screen:
3. Click **Device Type > Create**.

4. Click **Submit**. You will now see this screen:
5. Go to Network Resources > Network Devices and AAA Clients.
6. Click Create, and fill in the details as shown here:

7. Click Submit. You will now see this screen:

**Configure Users**

In this section, you will create local users on ACS (Student−1 and Teacher−1). Student−1 is assigned to the "Students" group and Teacher−1 is assigned to the "Teachers" group.

1. Go to Users and Identity Stores > Identity Groups > Create.
2. Once you click Submit, the page will look like this:

3. Create and assign users Student-1 and Teacher-1 to their respective groups.
4. Click Users and Identity Stores > Identity Groups > Users > Create.
5. Similarly, create Teacher-1.

The screen will look like this:

Define Policy Elements

Complete these steps in order to define IETF attributes for the users:

2. From the Common Tasks tab:

3. Add these IETF attributes:

   - Tunnel–Type = 64 = VLAN
   - Tunnel–Medium–Type = 802
   - Tunnel–Private–Group–ID = 253 (Student–1) and 257 (Teacher–1)

   For Group Students:
For Group Teachers:

4. Once both attributes are added, the screen will look like this:
Apply Access Policies

Complete these steps in order to select which Authentication methods are to be used and how the rules are to be configured (based on the previous steps):


2. Select which EAP method you would like the wireless Clients to Authenticate. In this example, we use PEAP–MSCHAP–V2.
3. Click Submit.
4. Verify the Identity group you have selected. In this example, we use Internal Users, which we created on ACS. Save the changes.


You can customize under what conditions you will allow user access to the network and what authorization profile (attributes) you will pass once authenticated. This granularity is only available in ACS5.x. In this example, we selected Location, Device Type, Protocol, Identity Group, and EAP Authentication Method.
6. Click **OK**, and **Save Changes**.

7. The next step is to create a Rule. If no Rules are defined, the Client is allowed access without any conditions.

   Click **Create > Rule−1**. This Rule is for Student−1.

8. Similarly, create a Rule for Teacher−1. Click **Save Changes**.
The screen will look like this:

9. We will now define Service Selection Rules. Use this page in order to configure a simple or rule-based policy to determine which service to apply to incoming requests. In this example, a rule-based policy is used.
Configure the WLC

This configuration requires these steps:

1. Configure the WLC with the details of the Authentication Server.
2. Configure the Dynamic Interfaces (VLANs).
3. Configure the WLANs (SSID).

Configure the WLC with the Details of the Authentication Server

It is necessary to configure the WLC so it can communicate with the RADIUS server in order to authenticate the clients, and also for any other transactions.

Complete these steps:

1. From the controller GUI, click **Security**.
2. Enter the IP address of the RADIUS server and the Shared Secret key used between the RADIUS server and the WLC.

   This Shared Secret key should be the same as the one configured in the RADIUS server.

Configure the Dynamic Interfaces (VLANs)

This procedure describes how to configure dynamic interfaces on the WLC. As explained earlier in this document, the VLAN ID specified under the Tunnel–Private–Group ID attribute of the RADIUS server must also exist in the WLC.

In the example, Student−1 is specified with the **Tunnel–Private–Group ID of 253 (VLAN =253)** on the RADIUS server. Similarly, Teacher−1 is specified with the **Tunnel–Private–Group ID of 257 (VLAN =257)** on the RADIUS server. See the IETF RADIUS Attributes section of the User Setup window.

Complete these steps:

1. The dynamic interface is configured from the controller GUI, in the **Controller > Interfaces** window.
2. Click Apply.

   This takes you to the Edit window of this dynamic interface (VLAN 253 here).
3. Enter the IP Address and default Gateway of this dynamic interface.
4. Click **Apply**.
5. Similarly, we will create a dynamic Interface for VLAN 257 for Teacher−1.
Controller
  General
  Inventory
  Interfaces
  Interface Groups
  Multicast
  Network Routes
  Internal DHCP Server
  Mobility Management
  Ports
  NTP
  CDP
  Advanced

Interfaces > New

<table>
<thead>
<tr>
<th>Interface Name</th>
<th>VLAN Id</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan237</td>
<td>237</td>
</tr>
</tbody>
</table>
6. The configured Interfaces configured will look like this:
Configure the WLANs (SSID)

Complete these steps in order to configure the WLANs in the WLC:

1. From the controller GUI, go to **WLANs > Create New** in order to create a new WLAN. The New WLANs window is displayed.
2. Enter the WLAN ID and WLAN SSID information.

   You can enter any name as the WLAN SSID. This example uses **goa** as the WLAN SSID.

3. Click **Apply** in order to go to the Edit window of the WLAN goa.
Enable the Allow AAA Override option in the controller for each WLAN (SSID) configured. The Allow AAA Override option of a WLAN allows you to configure the WLAN for identity networking. It allows you to apply VLAN tagging, QoS, and ACLs to individual clients based on the returned RADIUS attributes from the AAA server. In this example, it is used in order to assign a VLAN to Clients.

Most of the configuration for allowing AAA override is done at the RADIUS server. Enabling this parameter allows the controller to accept the attributes returned by the RADIUS server. The controller then applies these attributes to its clients.

**Note:** When the interface group is mapped to a WLAN and clients connect to the WLAN, the client does not get the IP address in a round robin fashion. The AAA override with interface group is not supported.
Configure the Wireless Client Utility

In our test client, we are using Windows 7 Native supplicant with an Intel 6300–N card running 14.3 driver version. It is recommended to test using the latest drivers from vendors.

Complete these steps in order to create a Profile in Windows Zero Config (WZC):

1. Go to Control Panel > Network and Internet > Manage Wireless Networks.
2. Click the Add tab.
3. Click Manually create a network profile.
4. Add the details as configured on the WLC.

   **Note:** The SSID is case sensitive.

5. Click **Next**.

6. Click **Change connection settings** in order to double-check the settings.
7. In this example, we are not validating the server certificate. If you check this box and are not able to connect, try disabling the feature and test again.
8. Alternatively, you can use your Windows credentials in order to log in. However, in this example we are not going to use that. Click **OK**.

9. Click **Advanced settings** in order to configure Username and Password.
10. Once you have finished testing Student−1, test Teacher−1. Click OK.

Your Client utility is now ready to connect.
Verify

Use this section in order to confirm that your configuration works properly.

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

Verify Student−1

From the WLC GUI, go to **Monitor > Clients**, and select the MAC address.

![WLC GUI Client Details]

WLC RADIUS Stats:

```
(Cisco Controller) > show radius auth statistics
Authentication Servers:
  Server Index........................................... 1
  Server Address........................................ 192.168.150.24
  Msg Round Trip Time................................. 1 (msec)
  First Requests........................................ 8
  Retry Requests........................................ 0
  Accept Responses.................................... 1
  Reject Responses.................................... 0
  Challenge Responses................................ 7
  Malformed Msns...................................... 0
  Bad Authenticator Msns.............................. 0
  Pending Requests.................................... 0
  Timeout Requests.................................... 0
  Unknownmsn Msns.................................... 0
  Other Drops.......................................... 0
```

ACS Logs:
1. Complete these steps in order to view the Hit counts:

   a. If you check the logs within 15 minutes of authentication, make sure you refresh the Hit count.

   ![Image](image1.png)

   b. You have a tab for **Hit Count** at the bottom of the same page.

   ![Image](image2.png)

2. Click **Monitoring and Reports** and a New pop-up window appears. Go to **Authentications Radius Today**. You can also click **Details** in order to verify which Service selection rule was applied.

   ![Image](image3.png)

**Verify Teacher–1**

From the WLC GUI, go to **Monitor > Clients**, and select the MAC address.
ACS Logs:

1. Complete these steps in order to view the Hit counts:

   a. If you check the logs within 15 minutes of authentication, make sure you refresh the HIT count.

   b. You have a tab for **Hit Count** at the bottom of the same page.
2. Click **Monitoring and Reports** and a New pop-up window appears. Go to **Authentications Radius Today**. You can also click **Details** in order to verify which Service selection rule was applied.

---

**Troubleshoot**

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

**Troubleshooting Commands**

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

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

1. If you experience any problems, issue these commands on the WLC:
   
   - `debug client <mac add of the client>`
   - `debug aaa all enable`
   - `show client detail <mac addr>` – Verify the policy manager state.
   - `show radius auth statistics` – Verify the failure reason.
   - `debug disable−all` – Turn off debugs.
   - `clear stats radius auth all` – Clear radius statistics on the WLC.

2. Verify the logs in the ACS and note the failure reason.

**Related Information**

- Dynamic VLAN Assignment with RADIUS Server ACS 4.1 and Wireless LAN Controller Configuration Example
- Technical Support & Documentation – Cisco Systems