# Scenario 5 – Dynamic VLAN Assignment

**NOTE:** Before beginning to configure the Switch and AP, remember to reset all the configurations to factory default.

To reset the switch configuration, click the **Tools** menu and select **Reset Configuration**, or with the "clear config" command

To reset the AP configuration, you will need to telnet into the AP CLI and use the "factory-reset" command

This scenario will show you when and how to use the Dynamic VLAN Assignment function.

The objectives in this setup are as follows:

- To understand how to use dynamic vlan function
- To know how to set up the RADIUS server for Dynamic VLAN environment
- Different users assign to Different VLAN



An overview of the configuration steps needed for Unified Switch and APs are as follows:

5.1 Configure VLAN Settings

- 5.2 Configure VLAN Routing5.3 Setup DHCP Server5.4 Configure WLAN Settings5.5 Setup RADIUS Servers5.6 Device Connections
- 5.7 Verify Configuration

# 5.1 Configure VLAN Settings

All of the features you configure in this section are within the **LAN** tab on the D-LINK Unified Switch.

#### 5.1.1 Configure the VLANs

The summary information for the VLAN configuration is shown in following table

VLAN ID	VLAN Name	Include Ports	IP Address
VLAN 100 (Interface 4/1)	AP1	Port 0/1 and 0/9 (Untagged)	192.168.100.254
VLAN 101 (Interface 4/2)	User Group 1	Port 0/1 (Tagged)	192.168.101.254
VLAN 102 (Interface 4/3)	User Group 2	Ports 0/1 (Tagged)	192.168.102.254

Use the following steps to create and configure VLAN 100, and then repeat them to configure VLAN 101, 102. Refer to the table for information about what value to configure for each VLAN.

a. From the LAN tab on the switch Web interface, click L2 Features > VLAN > VLAN Configuration.

b. Select Create from VLAN ID and Name dropdown menu.

c. Enter the VLAN ID.

d. Enter VLAN Name.

e. On the Slot/Port row, select **0/1** choose **Include** from the **Participation** dropdown menu, Tagging menu select **Untagged**, repeat to port **0/9** f. Click **Submit** 

f. Click Submit.

Forwarding DB Config	VLAN ID and Na	me	Create	×	
	VLAN ID		100 (21	to 3965)	
VLAN Configuration	VLAN Name		AP1		
Port Configuration	VLAN Type		Static		
Protocol-based VLA	Slot/Port	Status		Participation	Tagging
MAC-based VLAN	Ali			×	~
Double VLAN	0/1			Include 💌	Untagged 💌
Reset Configuration	0/2			Autodetect 💌	Untagged 🖌
Protected Ports	0/3			Autodetect 👻	Untagged 🖌
Filters	0/4			Autodetect 💌	Untagged 🛩
Hin GARP	0/5			Autodetect 💌	Untagged 🖌
IGMP Snooping	0/6			Autodetect 💌	Untagged 🖌
1 Spanning Tree	0/7			Autodetect 🖌	Untagged 🖌
DHCP Filtering	0/8			Autodetect 💌	Untagged 🖌
LLDP	0/9			Include 💌	Untagged 🐱
L3 Features	0/10			Autodetect 🔽	Untagged 🖌
M 0oS	0/11			Autodetect V	

Repeat the steps to create VLAN 101 and 102.

### 5.1.2 Configure PVID

Configure the Port VLAN ID for ports 0/1, 0/9

a. From the LAN tab on the switch Web interface, click L2 Features > VLAN > Port Configuration.

- Select port 0/1 from the Slot/Port dropdown menu.
- Enter 100 in the **Port VLAN ID** field.
- Click Submit.



- b. Select port 0/9 from the Slot/Port dropdown menu.
  - Enter 100 in the **Port VLAN ID** field.
  - Click Submit.

## 5.2 Configure VLAN Routing

#### 5.2.1 Create Routing Interface

To configure the new VLAN routing interfaces, use the following steps.

a. Select the LAN tab from the navigation panel and click **L3 Features > VLAN Routing Configuration**.

b. To create a routing interface for VLAN 100, enter 100 into the **VLAN ID** field and select **Create**.

This creates a logical routing interface with the slot/port designation of 4/1 for VLAN 100.

S-3026	VLAN Routing Configuration	n	
Administration	VLAN ID	100 (1 to 3965)	
3 Features	Slot/Port	4/1	
BOOTP/DHCP Relay Ager	MAC Address	00:50 ba:aa:aa ac	
ARP	IP Address	0.0.0.0	
IP	Subnet Mask	0.0.0.0	
<ul> <li>Interface Configuration</li> <li>Loopbacks</li> <li>Router</li> </ul>		Create	
VLAN Routing Configurati			
VRRP			
los			
Contraction of the Contraction o			

c. Repeat the previous step to create the VLAN routing interfaces for VLAN 101 and 102

### 5.2.2 Configure Routing Interface

Navigate to L3 Features > IP > Interface Configuration.

a. Select interface 4/1 from the Slot/Port dropdown menu and enter the following information:

- IP Address: 192.168.100.254

- Subnet Mask: 255.255.255.0
- Routing Mode: Enable

#### Click Submit.

3026	IP Interface Configuration	
Features	Slot/Port	4/1 💌
Features	IP Address	192.168.100.254
BOOTP/DHCP Relay Ager	Subnet Mask	255.255.255.0
ARP	Routing Mode	Enable 💌
IP Configuration	Administrative Mode	Enabled
Interface Configuration	Forward Net Directed Broadcasts	Disable 💌
Loopbacks	Active State	Active
Router	MAC Address	00:50:BA:AA:AA:AC
VLAN Routing Configurati	Encapsulation Type	Ethernet 💌
VRRP	Proxy Arp	Enable 💌
ess Control Lists	Local Proxy Arp	Disable 💌
curity	IP MTU	1500 (68 to 1500)

b. Select interface 4/2 from the Slot/Port dropdown menu and enter the following information:

- IP Address: 192.168.101.254
- Subnet Mask: 255.255.255.0
- Routing Mode: Enable

#### Click Submit.

c. Select interface 4/3 from the Slot/Port dropdown menu and enter the following information:

- IP Address: 192.168.102.254
- Subnet Mask: 255.255.255.0
- Routing Mode: Enable

Click Submit.

#### 5.2.3 Enable Global Routing

You need to enable the routing mode to allow the switch to operate as a L3 device in this scenario. To do this, navigate to the L3 Features > IP > Configuration



## 5.3 Setup DHCP Server

#### 5.3.1 Enable DHCP Server

Use the following procedures to configure the global DHCP settings.

a. Select the LAN tab from the navigation panel and access Administration  $\rightarrow$  DHCP Server  $\rightarrow$  Global Configuration, enable the Admin Mode

b. Add the excluded addresses as following:

- From 192.168.100.100 to 192.168.100.255
- From 192.168.101.100 to 192.168.101.255
- From 192.168.102.100 to 192.168.102.255

User Accounts	DHCP Server Global Configuration	
Authentication List Cor	Admin Mode	Enable 🔹
Denial Of Service Prot	Ping Packet Count	2 (0, 2 to 10)
Multiple Port Mirroring	Conflict Logging Mode	Enable 👻
System Severity Setti	Bootp Automatic Mode	Disable 👻
Telnet Sessions	Add Excluded Addresses *	
Ping Test	From	0.0.0.0
SNTP	То	0.0.0.0
Port Configuration	Delete Excluded Addresses	
	192.168.100.100 - 192.168.100.255	
DHCP Server	192.168.101.100 - 192.168.101.255	
Global Configuratio	□ 192.168.102.100 - 192.168.102.255	
Pool Configuration		

### **5.3.2 Pool Configuration**

This section describes how to configure the address pool for the wireless clients.

a. Select **Pool Configuration** in the Navigation tree.

Select **create** and specify the following settings:

- Pool Name AP1
- Type of Binding Dynamic
- Network Number 192.168.100.0
- Network Mask 255.255.255.0
- Default Router Addresses 192.168.100.254

Click **Submit** to create the address pool.

User Accounts	DHCP Server Pool Configuration	
Authentication List Cor     User Login	Pool Name	AP1 V
Denial Of Service Prot	Type of Binding	Dynamic 💌
Multiple Port Mirroring	Network Number	192.168.100.0
System Severity Settin	Network Mask	255 255 255 0
Telnet Sessions     Outbound Telnet Clien	Prefix Length	(0-32)
Ping Test	Lease Time	Specified Duration 👻
SNTP	Days	1 (0 to 59)
P Port Configuration	Hours	0 (0 to 1439)
E Log	Minutes	0 (0 to 86399)
Ball DHCP Server	Default Router Addresses	
Global Configuratio		192.168.100.254
Pool Configuration		
Pool Options		

b. From the Pool Configuration, select **create** and specify the following settings:

- Pool Name User Group 1
- Type of Binding Dynamic
- Network Number 192.168.101.0
- Network Mask 255.255.255.0
- Default Router Addresses 192.168.101.254

Click **Submit** to create the address pool.

c. From the Pool Configuration, select **create** and specify the following settings:

- Pool Name User Group 2
- Type of Binding Dynamic
- Network Number 192.168.102.0
- Network Mask 255.255.255.0
- Default Router Addresses 192.168.102.254

Click **Submit** to create the address pool.

## 5.4 Configure WLAN Settings

#### 5.4.1 Add L2 Discovery

Use the following steps to configure the Unified Switch and the APs.

a. Go to **WLAN** tab > **Administration > Basic Setup** page, click **Discovery** tab.

b. Add VLAN 100 to the **L2/VLAN Discovery** (to allow automatic discovery of the APs connected to ports on VLAN 100), then click **Submit**.

tion	Vireless Discove	ry Configuration			
tion	1 2/ID Dissources				
	Lone Discovery			L2/VLAN Discovery	
iration	IP List	<empty list=""></empty>		VLAN List	1 - Default 100
	IP Address Range	From	To	VLAN (1-4094)	100

## 5.4.2 Configure RADIUS Server

Click **Next** to go to **AAA/RADIUS** page, enter 192.168.100.100 as the **IP Address** of RADIUS Server, **Secret** equal to 12345678

		2.2.4		oono   vana /u		
ity oring	Wireless Defa	ult AAA/RADIUS (	Configuratio	n		
istration						AP Profile 1-Defa
anagement	RADIUS			MAC Authentica	tion	
ced Configuration	IP Address	192.168.100.100		Default Action	Allow O Deny	
alization	Secret		Edit	Allow MAC List	<empty list=""></empty>	
	Accounting					
						_
				MAC Address		
					Add Delete	

## 5.4.3 Configure WLAN settings

a. Click the SSID tab to configure the VAP and Network settings

- b. Select the 802.11b/g radio.
- c. Select the check box next to **1-Guest Network** and click **Edit**.
- d. Change the following Network parameters and select **Submit**:
  - SSID: S5-Group1-DVLAN (depend on your group.)
  - Security: WPA/WPA2 WPA Enterprise
  - WPA Versions: WPA & WPA2
  - WPA Ciphers: TKIP & CCMP

-3026	Wireless Network C	Configuration	i.		
Security	SSID	Dynamic VLAN		Security	○None ○WEP ⊙WPA/WPA2
Administration	Hide SSID				OWPA Personal OWPA Enterprise
Basic Setup	VLAN	1 (1 to 40	094)	WPA Versions	
AP Management	L3 Tunnel			WPA Ciphers	
VLAN Visualization	L3 Tunnel Status	None		Pre-Authentication	
	L3 Tunnel Subnet	0.0.0.0	_		
	L3 Tunnel Mask	255.255.255.0	-		
	MAC Authentication	O Local O Ra	dius 💿 Disable		
	RADIUS IP Address	0.0.0,0	Use Profile		
	RADIUS Secret	[	Edit		
	RADIUS Accounting				

#### 5.5 Setup RADIUS Servers

a. Setup the IP address of your RADIUS server to 192.168.100.100/24b. Add a client entry to the FreeRADIUS server, client.conf file for the 192.168.0.0/16 network:

```
client 192.168.0.0/16 {
    secret = 12345678
    shortname = private-network-1
}
```

c. Add a user to the the users.conf file for the User Group 1 as following:

```
DVLANUSer1 User-Password == "12345678"

Tunnel-Type = "VLAN",

Tunnel-Medium-Type = "IEEE-802",

Tunnel-Private-Group-Id = "101",
```

d. Add a user to the the users.conf file for the User Group 2 as following:

```
DVLANUser2 User-Password == "12345678"
Tunnel-Type = "VLAN",
Tunnel-Medium-Type = "IEEE-802",
Tunnel-Private-Group-Id = "102",
```

e. Save and restart your RADIUS server

## 5.6 Device Connections

### 5.6.1 Connect AP and RADIUS Server

- a. Connect AP1 to port 1 of the switch
- b. Connect the RADIUS to port 9 of the Wireless Switch.

### 5.6.2 Manage APs

Wait about 60 seconds and click **Monitoring > Access Points > All Access Points**, check AP1's MAC Address and click **Manage** 

### 5.6.3 Save Changes

Save the switch configuration

	O Power	Link/ACT/Spec	1									
D-LINK	O Console O RPS	🖉 o PoE	·									
uilding Networks for People	DWS-3024		Console	2 4	6 8	10	2	14 16	18	20 2	2 24	Combo2 Co
10												
WIAN	🔨 Tool									12	Log	out 🛛 📀
	Reset Configuration											
5-3024	Reset Password											
Security	Reboot System											
Monitoring	Save Changes	anges will cause all cha	inges to con	nfigura	tion p	anels	hat v	vere a	appli	ed, bu	it not	saved,
	SANCES ALCONOMICS	aining their new values a	across a sys	tem re	boot.							
Global	Download File											
Global Peer Switch	Download File Upload File			-								
Global Peer Switch Access Point	Download File Upload File Multiple Image Service		Save	•								
Global Peer Switch Access Point	Download File Upload File Multiple Image Service		Sav									
Global Peer Switch Access Point I All Access Points Managed Access Points	Download File Upload File Multiple Image Service		Sav	•]								
Global Peer Switch Access Point E All Access Points E Managed Access Points E Authentication Failed A	Download File Upload File Multiple Image Service		Save	•)								
Global Peer Switch Access Point All Access Points Managed Access Points Authentication Failed A Rogue/RF Scan Access	Download File Upload File Multiple Image Service		Savi	•								
Global Peer Switch Access Point Al Access Points Al Access Points Authentication Failed A Rogue/RF Scan Access Client	Download File Upload File Multiple Image Service		Savi									
Global Peer Switch Access Point Managed Access Points Authentication Failed A Rogue/RF Scan Access I Client Client	Download File Upload File Multiple Image Service		Sav	•								

# 5.7 Verify Configuration

a. Follow 3.11.2, connect a wireless client to the S5-Group1-DVLAN, enter the username and password as **DVLANUser1**, **12345678** 

Enter Credent	ials 🛛 🔀
User name:	DVLANUser1
Password:	•••••
Logon domain:	
	OK Cancel

b. Make sure you get the IP address belong to 192.168.101.0/24 subnet, then ping 192.168.100.100.

c. Follow 3.11.2, connect another wireless client to the S5-Group1-DVLAN, enter the username and password as **DVLANUser2**, **12345678** 

d. Make sure you get the 192.168.102.0/24 IP address.

e. Ping between both wireless clients