

Configuration Guide

How to Configure a BYOD Environment with the DWS-4026

(MAC Authentication + Captive Portal)



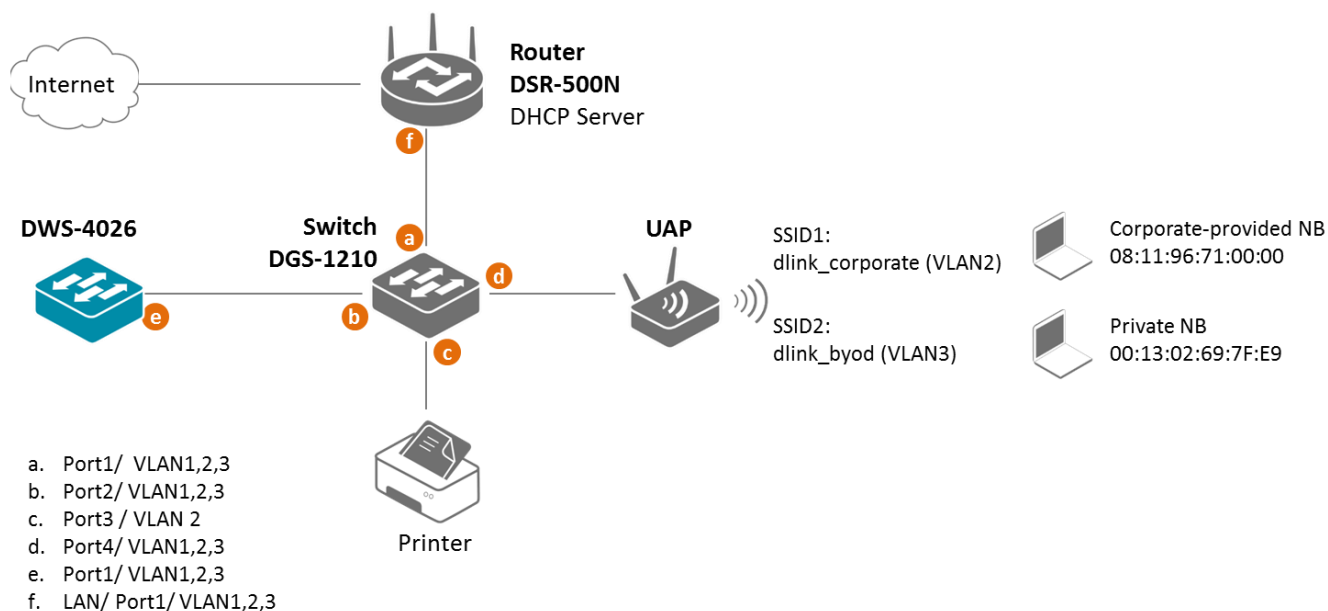
Overview

This guide describes how to configure and implement BYOD environment with the D-Link DWS-4026 Unified Switch for user and device authentication.

Situation Note

The trend of Bring Your Own Device (BYOD) in working place is a new challenge on network security and management. Many corporations that allow employees to use their own device at work expecting have better performance and productivity; however, on the downside, corporations also concern the network security and information leakage by using private device. How to distinguish corporate-provided device and private device (BYOD device), and give different authorities is the major task for IT teams.

The scenario in this guide shows you how to implement a BYOD environment with DWS-4026. Use device MAC authentication to enforce client associating specific SSIDs based on the device which is corporate-provided or private. All connection from SSIDs required performing authentication before granted authority.



The authentication methods on each SSID are different:

- dlink_corporate SSID: This SSID is for D-Link employee who works with cooperate-provided device. It requires device MAC authentication and Captive Portal to complete the authentication process. After complete authentication, the client is authorized in VLAN2 network.
- dlink_byod SSID: This SSID is for D-Link employee who works with his private device(BYOD device). It requires Captive Portal to complete the authentication process. After complete authentication, the client is authorized in VLAN3 network.

NOTE: The screenshots in this guide are from the DWS-4026's firmware version 4.3.0.3. If you are using an earlier version of the firmware, the screenshots may not be identical to what you see on your browser.

Configuration Steps (DWS-4026)

1. Set up VLANs based on the network architecture. Create three VLANs. VLAN1 is the default VLAN for AP management, VLAN2 is for the traffic associated from SSID dlink_corporate, and VLAN3 is for the traffic associated from SSID dlink_byod. Associate VLAN 1 to 3 memberships on Port1.

Create three VLANs. Un-tag VLAN1, and tag VLAN2 and VLAN3 on port 1 (0/1). Navigate to LAN > DWS-4026 > L2 Feature > VLAN > VLAN Configuration.

VLAN Configuration

VLAN ID List: 1
 VLAN Name: default (0 to 32 characters)
 VLAN Type: Default

VLAN ID-Individual/Range: Range[1-4093]
 VLAN Participation All:
 Participation All: Autodetect
 VLAN Participation: Tagging All:

Interface	Interface Status	Participation	Tagging
0/1	Include	Include	Untagged
0/2	Include	Include	Untagged

VLAN Configuration

VLAN ID List: 2
 VLAN Name: dlink_corporate (0 to 32 characters)
 VLAN Type: Static

VLAN ID-Individual/Range: Range[1-4093]
 VLAN Participation All:
 Participation All: Autodetect
 VLAN Participation: Tagging All:

Interface	Interface Status	Participation	Tagging
0/1	Include	Include	Tagged
0/2	Exclude	Autodetect	Untagged

VLAN Configuration

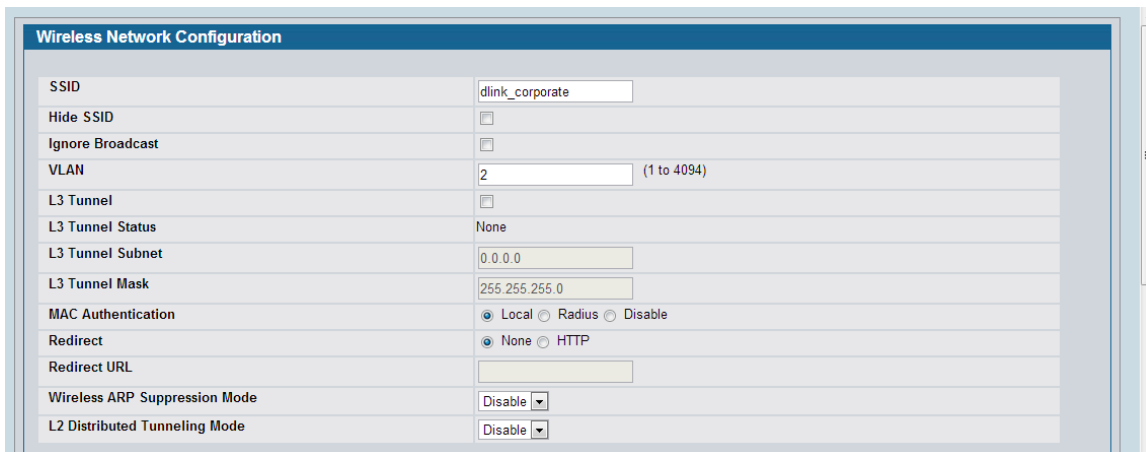
VLAN ID List: 3
 VLAN Name: dlink_byod (0 to 32 characters)
 VLAN Type: Static

VLAN ID-Individual/Range: Range[1-4093]
 VLAN Participation All:
 Participation All: Autodetect
 VLAN Participation: Tagging All:

Interface	Interface Status	Participation	Tagging
0/1	Include	Include	Tagged
0/2	Exclude	Autodetect	Untagged

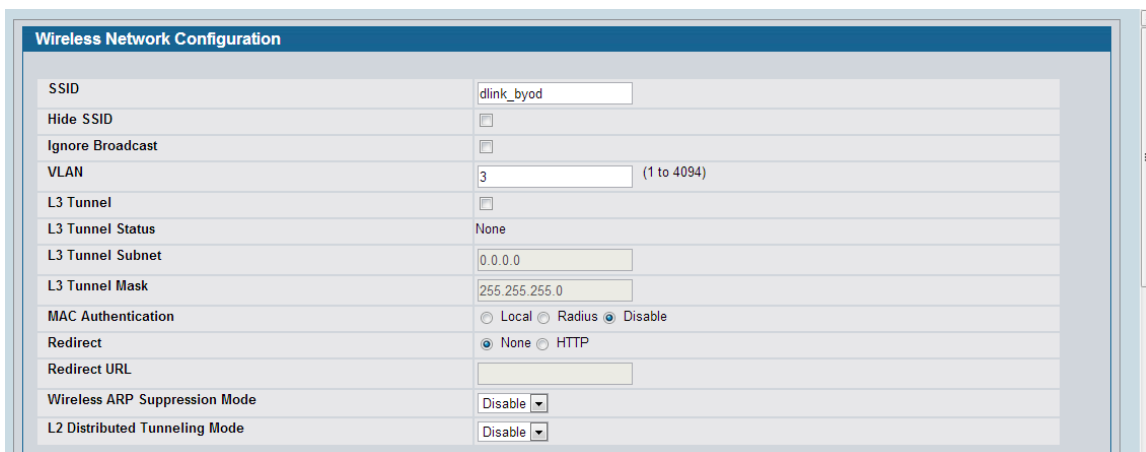
2. Create two SSIDs: SSID dlink_corporate and SSID dlink_byod, and assign VLAN 2 and 3 on these two SSIDs respectively. Enable MAC authentication on SSID dlink_corporate only. The MAC authentication database can be either (a) local database or (b) external RADIUS.

Set up two SSIDs. For the MAC authentication, if the MAC authentication database is local database, select "Local" on MAC Authentication, if RADIUS, select "RADIUS" on MAC Authentication. In this case, use local database as authentication server. Navigate to WLAN> DWS-4026> Administration> Networks.



Wireless Network Configuration

SSID	dlink_corporate
Hide SSID	<input type="checkbox"/>
Ignore Broadcast	<input type="checkbox"/>
VLAN	2 (1 to 4094)
L3 Tunnel	<input type="checkbox"/>
L3 Tunnel Status	None
L3 Tunnel Subnet	0.0.0.0
L3 Tunnel Mask	255.255.255.0
MAC Authentication	<input checked="" type="radio"/> Local <input type="radio"/> Radius <input type="radio"/> Disable
Redirect	<input checked="" type="radio"/> None <input type="radio"/> HTTP
Redirect URL	
Wireless ARP Suppression Mode	Disable
L2 Distributed Tunneling Mode	Disable



Wireless Network Configuration

SSID	dlink_byod
Hide SSID	<input type="checkbox"/>
Ignore Broadcast	<input type="checkbox"/>
VLAN	3 (1 to 4094)
L3 Tunnel	<input type="checkbox"/>
L3 Tunnel Status	None
L3 Tunnel Subnet	0.0.0.0
L3 Tunnel Mask	255.255.255.0
MAC Authentication	<input type="radio"/> Local <input type="radio"/> Radius <input checked="" type="radio"/> Disable
Redirect	<input checked="" type="radio"/> None <input type="radio"/> HTTP
Redirect URL	
Wireless ARP Suppression Mode	Disable
L2 Distributed Tunneling Mode	Disable

Wireless Network List							
ID	SSID	VLAN	Hide SSID	L3 Tunnel	Security	Redirect	
<input type="checkbox"/>	1	dlink1	1-default	Disabled	Disabled	None	None
<input type="checkbox"/>	2	dlink2	1-default	Disabled	Disabled	None	None
<input type="checkbox"/>	3	dlink3	1-default	Disabled	Disabled	None	None
<input type="checkbox"/>	4	dlink4	1-default	Disabled	Disabled	None	None
<input type="checkbox"/>	5	dlink5	1-default	Disabled	Disabled	None	None
<input type="checkbox"/>	6	dlink6	1-default	Disabled	Disabled	None	None
<input type="checkbox"/>	7	dlink7	1-default	Disabled	Disabled	None	None
<input type="checkbox"/>	8	dlink8	1-default	Disabled	Disabled	None	None
<input type="checkbox"/>	9	dlink9	1-default	Disabled	Disabled	None	None
<input type="checkbox"/>	10	dlink10	1-default	Disabled	Disabled	None	None
<input type="checkbox"/>	11	dlink11	1-default	Disabled	Disabled	None	None
<input type="checkbox"/>	12	dlink12	1-default	Disabled	Disabled	None	None
<input type="checkbox"/>	13	dlink13	1-default	Disabled	Disabled	None	None
<input type="checkbox"/>	14	dlink14	1-default	Disabled	Disabled	None	None
<input type="checkbox"/>	15	dlink15	1-default	Disabled	Disabled	None	None
<input type="checkbox"/>	16	dlink16	1-default	Disabled	Disabled	None	None
<input type="checkbox"/>	17	dlink_corporate	2	Disabled	Disabled	None	None
<input type="checkbox"/>	18	dlink_byod	3	Disabled	Disabled	None	None

3. Create an AP Profile and associate SSIDs on it.

3-1. Create an AP Profile "BYOD". Navigate to WLAN> DWS-4026> Administration> Advanced Configuration> AP Profiles> BYOD> Global.

Summary | Default | **2-BYOD**

Global | Radio | SSID | QoS | TSPEC

Access Point Profile Global Configuration AP Profile 2-BYOD

Profile Name:

Hardware Type ID:

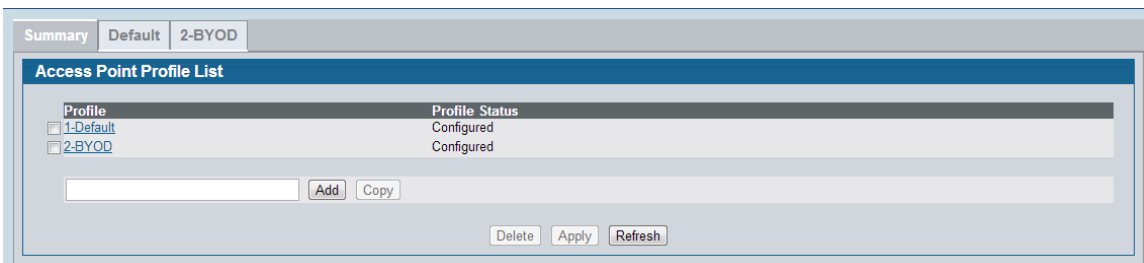
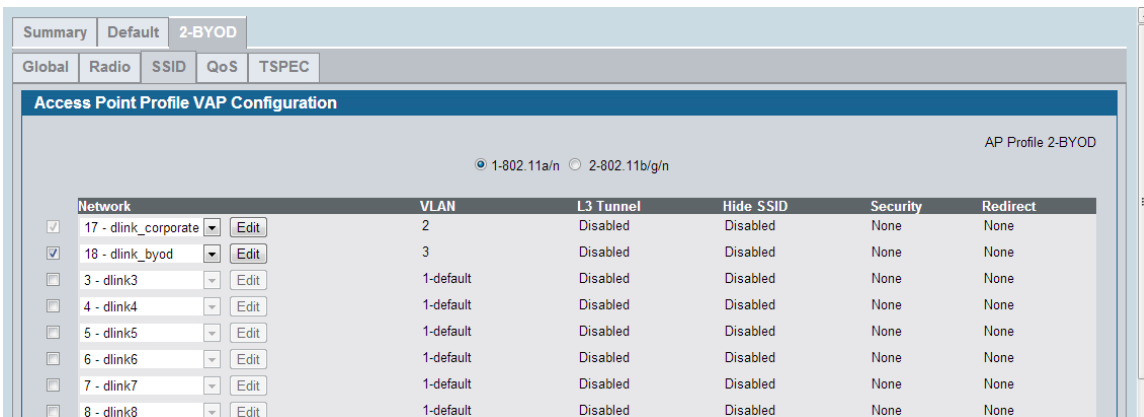
Disconnected AP Data Forwarding Mode:

Disconnected AP Management Mode:

AeroScout™ Engine Support:

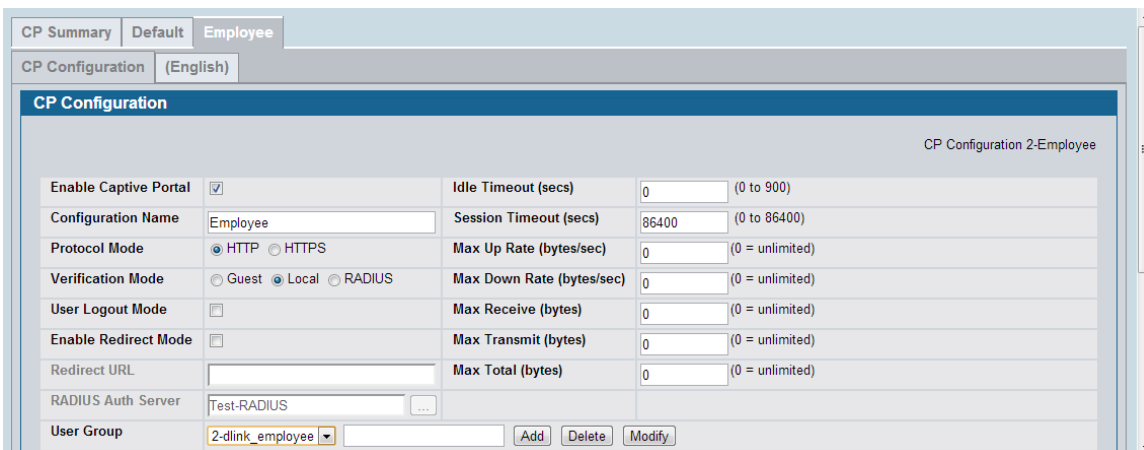
Wired Network Discovery VLAN ID: (0 to 4094)

3-2. Associate SSID dlink_corporate and dlink_byod on this AP Profile. Navigate to WLAN> DWS-4026> Administration> Advanced Configuration> AP Profiles> BYOD> SSID.



4. Create a CP Profile. Select the authentication server on the Captive Portal. The authentication server can be either (a) local database or (b) external RADIUS. In this case, use local database as authentication server.

Navigate to WLAN> DWS-4026> Security> Captive Portal> CP Configuration. There are three settings: (a) Create a CP Profile "Employee". (b) Select Verification Mode. If the user authentication database is local database, select "Local" on Verification Mode, if RADIUS, select "RADIUS" on Verification Mode. In this case, use local database as authentication server. (c) Add one User Group "dlink_employee", and then select it as User Group.



5. Create Captive Portal accounts on local database.

Create user account under User Group "2-dlink_employee". Navigate to WLAN> DWS-4026> Security> Captive Portal> Local User.

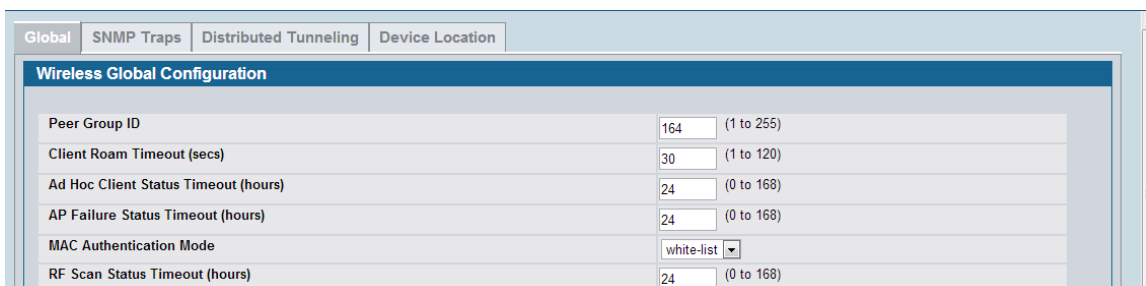
User	Session Timeout	Idle Timeout
<input type="checkbox"/> rosanna_chu	0	0

6. Associate these two SSID interfaces on CP Configuration "2-Employee".

Select CP Configuration "2-Employee". Add interface SSID dlink_corporate and SSID dlink_byod on Associated Interfaces. Navigate to WLAN> DWS-4026> Security> Captive Portal> Interface Association.

7. Create device MAC authentication database on local database.

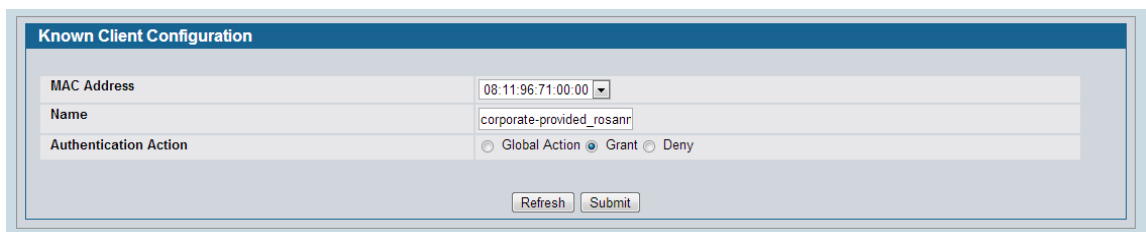
7-1. Choose MAC Authentication Mode as "white-list". Navigate to WLAN> DWS-4026> Administration> Advanced Configuration> Global.



The screenshot shows the 'Wireless Global Configuration' page. It has tabs for 'Global', 'SNMP Traps', 'Distributed Tunneling', and 'Device Location'. The 'Global' tab is active. The configuration includes several fields: Peer Group ID (164), Client Roam Timeout (secs) (30), Ad Hoc Client Status Timeout (hours) (24), AP Failure Status Timeout (hours) (24), MAC Authentication Mode (white-list), and RF Scan Status Timeout (hours) (24).

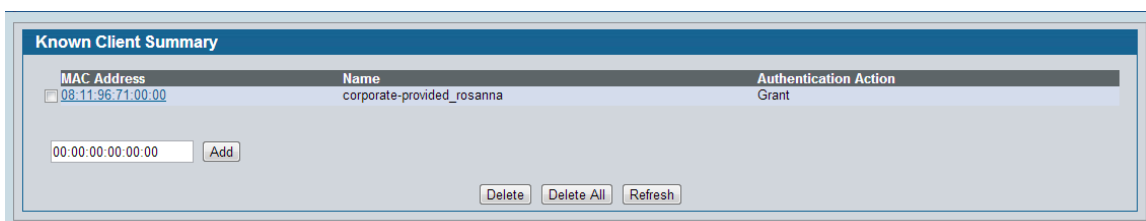
Field	Value	Range
Peer Group ID	164	(1 to 255)
Client Roam Timeout (secs)	30	(1 to 120)
Ad Hoc Client Status Timeout (hours)	24	(0 to 168)
AP Failure Status Timeout (hours)	24	(0 to 168)
MAC Authentication Mode	white-list	
RF Scan Status Timeout (hours)	24	(0 to 168)

7-2. Create device MAC authentication accounts in the Known Client database. Add corporate-provided NB MAC 08:11:96:71:00:00 in the database. The Authentication Action is "Grant". Navigate to WLAN> DWS-4026> Administration> Advanced Configuration> Client> Known Clients.



The screenshot shows the 'Known Client Configuration' page. It has fields for MAC Address (08:11:96:71:00:00), Name (corporate-provided_rosannr), and Authentication Action (Grant). There are 'Refresh' and 'Submit' buttons.

Field	Value
MAC Address	08:11:96:71:00:00
Name	corporate-provided_rosannr
Authentication Action	Grant



The screenshot shows the 'Known Client Summary' page. It displays a table with one entry: MAC Address 08:11:96:71:00:00, Name corporate-provided_rosanna, and Authentication Action Grant. There are 'Delete', 'Delete All', and 'Refresh' buttons.

MAC Address	Name	Authentication Action
<input type="checkbox"/> 08:11:96:71:00:00	corporate-provided_rosanna	Grant

8. Discover and manage an AP from the network.

Manage AP. Navigate to WLAN> DWS-4026> Monitoring> Access Point> All AP Status.

Global | Discovery | Profile | Radio | SSID | Valid AP | OUI

Valid Access Point Configuration

MAC address: fc:75:16:76:ff:40
 AP Mode: Managed
 Location:
 Authentication Password: Edit
 Profile: 2 - BYOD

Radio 1 - 802.11a/n	Forced Roaming	<input type="checkbox"/>	Roaming Threshold	20 (20 to 50)
Radio 2 - 802.11b/g/n	Forced Roaming	<input type="checkbox"/>	Roaming Threshold	20 (20 to 50)
Radio 1 - 802.11a/n	Channel	Auto	Power (%)	0
Radio 2 - 802.11b/g/n	Channel	Auto	Power (%)	0

Refresh Delete Submit

All AP Status

MAC address	Location	Switch Port	IP Address	Software Version	Age	Status	Profile	Radio	Channel	Authenticated Clients
fc:75:16:76:ff:40		0/1	192.168.10.101	4.2.0.9_B001	0h:0m:3s	Managed	2-BYOD	1-802.11a/n 2-802.11b/g/n	157 11	0 0

Delete All Manage Acknowledge Refresh Auto Refresh

Configuration Steps (DGS-1210)

- Set up VLANs based on the network architecture. Create three VLANs. VLAN₁ is the default VLAN for AP management, VLAN₂ is for the traffic associated from SSID dlink_corporate, and VLAN₃ is for the traffic associated from SSID dlink_byod. As DWS-4026 VLAN₁ is un-tag VLAN, set VLAN₁ as un-tag VLAN on switch. The VLAN table is as below.

	Port1	Port2	Port3	Port4
VLAN ₁	Un-tag	Un-tag	-	Un-tag
VLAN ₂	Tag	Tag	Un-tag	Tag
VLAN ₃	Tag	Tag	-	Tag

D-Link Building Networks for People *Smart* admin - 10.90.90.3

Save Tools Wizard Help Logout

DGS-1210-10P
System
VLAN
802.1Q VLAN
802.1Q VLAN PVID
802.1Q Management VLAN
Voice VLAN
Auto Surveillance VLAN
L2 Functions
QoS
Security

VID Settings

VID 1

VLAN Name: default

Port	Select All	01	02	03	04	05	06	07	08	09	10
Untagged	All	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Tagged	All	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Not Member	All	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Back Apply

Safeguard

How to Configure a BYOD Environment with the DWS-4026

VID Settings

VID: 2
 VLAN Name: dlink_corporate

Port	Select All	01	02	03	04	05	06	07	08	09	10
Untagged	All	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Tagged	All	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Not Member	All	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

VID Settings

VID: 3
 VLAN Name: dlink_byod

Maximum 20 characters.

Port	Select All	01	02	03	04	05	06	07	08	09	10
Untagged	All	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Tagged	All	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Not member	All	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

802.1Q VLAN Settings

Asymmetric VLAN [Example] Enabled Disabled

Total static VLAN entries: 3
 Maximum 256 entries.

VID	VLAN Name	Untagged	Tagged	Delete
1	default	01-02, 04		Delete
2	dlink_corporate	03	01-02, 04	Delete
3	dlink_byod		01-02, 04	Delete

- (Option) Enable PoE on the ports which connect with APs if needed. In default, all ports are enabled auto PoE detection.

PoE Port Settings

From Port: 1 To Port: 8 State: Enabled Time Range: N/A Priority: Normal Power Limit: Auto

The port 1 to port 8 can be set a power limit between 1W and 30W. Max power used by PSE: Class 1: 4W, Class 2: 7W, Class 3: 15.4W, Class 4: 30W.

Port	State	Time Range	Priority	Power Limit	Power (W)	Voltage (V)	Current (mA)	Classification	Status
1	Enabled	N/A	Normal	Auto	0.0	0.0	0.0	N/A	POWER OFF
2	Enabled	N/A	Normal	Auto	0.0	0.0	0.0	N/A	POWER OFF
3	Enabled	N/A	Normal	Auto	0.0	0.0	0.0	N/A	POWER OFF
4	Enabled	N/A	Normal	Auto	0.0	0.0	0.0	N/A	POWER OFF
5	Enabled	N/A	Normal	Auto	0.0	0.0	0.0	N/A	POWER OFF
6	Enabled	N/A	Normal	Auto	0.0	0.0	0.0	N/A	POWER OFF
7	Enabled	N/A	Normal	Auto	0.0	0.0	0.0	N/A	POWER OFF
8	Enabled	N/A	Normal	Auto	0.0	0.0	0.0	N/A	POWER OFF

Configuration Steps (DSR-500N)

1. Set up VLANs based on the network architecture. Create three VLANs. VLAN₁ is the default VLAN for AP management, VLAN₂ is for the traffic associated from SSID dlink_corporate, and VLAN₃ is for the traffic associated from SSID dlink_byod.

1-1. Set up VLAN₂ and VLAN₃. Navigate to SETUP> VLAN Settings> Available VLANs.

The screenshot shows the D-Link web interface for a DSR-500N device. The navigation menu on the left includes Wizard, Internet Settings, Wireless Settings, Network Settings, DMZ Setup, VPN Settings, USB Settings, and VLAN Settings. The main content area is titled 'AVAILABLE VLANs' and includes a 'LOGOUT' link. Below this, there is a section for 'VLAN Configuration' with the following fields: Name (dlink_corporate), Id (2), and Inter VLAN Routing Enable (checked). A 'Helpful Hints...' section on the right provides instructions on how to use the interface.

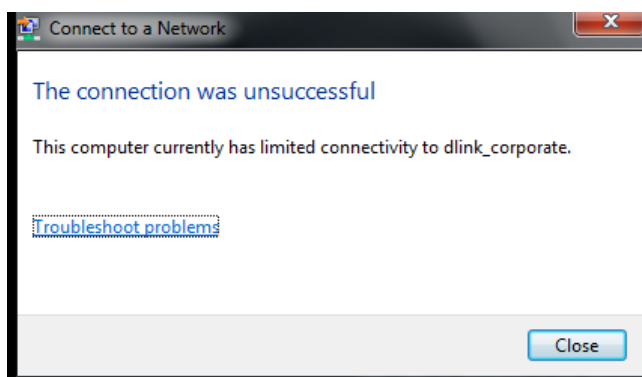
The screenshot shows the D-Link web interface for a DSR-500N device, similar to the previous one but with the 'Name' field set to 'dlink_byod' and the 'Id' field set to '3'. The 'Inter VLAN Routing Enable' checkbox is also checked. The 'Helpful Hints...' section on the right is also visible.

1-2. Enable DHCP server on default VLAN, VLAN₂ and VLAN₃. Navigate to SETUP> VLAN Settings> Multiple VLAN Subnets.

DSR-500N	SETUP	ADVANCED	TOOLS	STATUS	HELP
Wizard	<p>MULTI VLAN SUBNET CONFIG LOGOUT</p> <p>This page shows the list of available multiple VLAN subnets.</p> <p> <input type="button" value="Save Settings"/> <input type="button" value="Don't Save Settings"/> </p>				<p>Helpful Hints...</p> <p>By default, when you add a new VLAN, it is assigned an IP address of 192.168.2.1 with subnet-mask 255.255.255.0, the next added one is assigned 192.168.3.1 and so on. You can change the assigned IP address, subnet mask and many other options here. The only non-editable field in VLAN ID.</p> <p>More...</p>
Internet Settings	<p>MULTI VLAN SUBNET</p> <p>Vlan ID: 1</p> <p>IP Address: <input type="text" value="192.168.10.1"/></p> <p>Subnet Mask: <input type="text" value="255.255.255.0"/></p>				
Wireless Settings	<p>DHCP</p> <p>DHCP Mode: <input type="text" value="DHCP Server"/></p> <p>Domain Name: <input type="text" value="DLink"/></p> <p>Starting IP Address: <input type="text" value="192.168.10.100"/></p> <p>Ending IP Address: <input type="text" value="192.168.10.254"/></p>				
Network Settings					
DMZ Setup					
VPN Settings					
USB Settings					
VLAN Settings					

Proof of Concept

- The NB with MAC 08:11:96:71, which is the corporate-provided device, is allowed get IP address from both SSIDs. But for the NB with MAC 00:13:02:69:7F:Eg, which is the private device, is allowed get IP address only from SSID dlink_byod. If it associates SSID dlink_corporate, it could not get IP address and would get error message as below. The MAC authentication forces the private device associate network from SSID dlink_byod



- After NB associates with SSID and gets IP address, the system requires processing Captive Portal to identify the user.

3. While the corporate-provided NB associates SSID dlink_corporate and completes the authentication, it can access resources on VLAN₂, for example, printer and internet.
4. While the corporate-provided or private NB associates SSID dlink_byod and completes the authentication, it can access resources on VLAN₃, for example, internet.

D-Link[®]

WWW.DLINK.COM

D-Link, D-Link logo, D-Link sub brand logos and D-Link product trademarks are trademarks or registered trademarks of D-Link Corporation and its subsidiaries.
All other third party marks mentioned herein are trademarks of the respective owners.

Copyright © 2014 D-Link Corporation. All Rights Reserved.