Configuration Guide

How to Configure a BYOD Environment with the DWS-3160

(Mac Authentication+ Captive Portal)



Overview

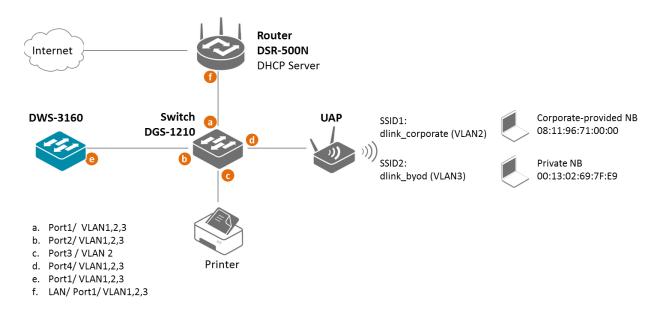
This guide describes how to configure and implement BYOD environment with the D-Link DWS-3160 Unified Switch for user and device authentication.



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-3160. 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 difference:

- dlink_corporate SSID: This SSID is for D-Link employee who works with corporate -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-3160's firmware version 4.3.0.5. 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-3160)

 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-3160-24PC> L2 Feature> VLAN> 802.1Q VLAN Settings.

| | 23 24 | | ly

 | Арр

 |

 |

 |

 |

 | 5) | ers | racte

 | cha

 | v: 22

 | 1010

 |
 |

 | _
 |
 |
 | |
 | |
 | | | | |
|---|---|---
--
--

--
--

--
--

--
--

--
--

--
--
---|---------|-----
--
--

--

--

--

--

--

--

--
---|---

---|---|---|---------|-----|----------|
| | 23 24 | _ |

 |

 |

 |

 |

 |

 | | |

 | 0.10

 | л. <i>э</i> 2

 |] (ivia

 |
 |

 | ult
 | defa
 | ie
 | Nam | .AN I
 | VL | •
 | d 🖣 | ablec | | |
| | \odot \odot | 0 | ۲

 | ٢

 | 0

 | 0

 | \bigcirc

 | \odot

 | 16
) | 1 | ٢

 | \odot

 | 0

 | \odot

 | \odot
 | 0

 | \bigcirc
 | 0
 | 0
 | 0 | 05
 | 0 | 0
 | 0 | \odot | All | agged [|
| All O | • •< | 0 | <td> <td> <td> <td> <td> <td>•
0</td><td>0</td><td> <td> <td> <td> <td> <td> <td> <td> <td> <td> <td> <td> <td> <td> <td></td><td>All</td><td>orbidden</td></td></td></td></td></td></td></td></td></td></td></td></td></td></td></td></td></td></td></td> | <td> <td> <td> <td> <td>•
0</td><td>0</td><td> <td> <td> <td> <td> <td> <td> <td> <td> <td> <td> <td> <td> <td> <td></td><td>All</td><td>orbidden</td></td></td></td></td></td></td></td></td></td></td></td></td></td></td></td></td></td></td> | <td> <td> <td> <td>•
0</td><td>0</td><td> <td> <td> <td> <td> <td> <td> <td> <td> <td> <td> <td> <td> <td> <td></td><td>All</td><td>orbidden</td></td></td></td></td></td></td></td></td></td></td></td></td></td></td></td></td></td> | <td> <td> <td>•
0</td><td>0</td><td> <td> <td> <td> <td> <td> <td> <td> <td> <td> <td> <td> <td> <td> <td></td><td>All</td><td>orbidden</td></td></td></td></td></td></td></td></td></td></td></td></td></td></td></td></td> | <td> <td>•
0</td><td>0</td><td> <td> <td> <td> <td> <td> <td> <td> <td> <td> <td> <td> <td> <td> <td></td><td>All</td><td>orbidden</td></td></td></td></td></td></td></td></td></td></td></td></td></td></td></td> | <td>•
0</td><td>0</td><td> <td> <td> <td> <td> <td> <td> <td> <td> <td> <td> <td> <td> <td> <td></td><td>All</td><td>orbidden</td></td></td></td></td></td></td></td></td></td></td></td></td></td></td> | •
0 | 0 | <td> <td> <td> <td> <td> <td> <td> <td> <td> <td> <td> <td> <td> <td></td><td>All</td><td>orbidden</td></td></td></td></td></td></td></td></td></td></td></td></td></td> | <td> <td> <td> <td> <td> <td> <td> <td> <td> <td> <td> <td> <td></td><td>All</td><td>orbidden</td></td></td></td></td></td></td></td></td></td></td></td></td> | <td> <td> <td> <td> <td> <td> <td> <td> <td> <td> <td> <td></td><td>All</td><td>orbidden</td></td></td></td></td></td></td></td></td></td></td></td> | <td> <td> <td> <td> <td> <td> <td> <td> <td> <td> <td></td><td>All</td><td>orbidden</td></td></td></td></td></td></td></td></td></td></td> | <td> <td> <td> <td> <td> <td> <td> <td> <td> <td></td><td>All</td><td>orbidden</td></td></td></td></td></td></td></td></td></td> | <td> <td> <td> <td> <td> <td> <td> <td> <td></td><td>All</td><td>orbidden</td></td></td></td></td></td></td></td></td> | <td> <td> <td> <td> <td> <td> <td> <td></td><td>All</td><td>orbidden</td></td></td></td></td></td></td></td> | <td> <td> <td> <td> <td> <td> <td></td><td>All</td><td>orbidden</td></td></td></td></td></td></td> | <td> <td> <td> <td> <td> <td></td><td>All</td><td>orbidden</td></td></td></td></td></td> | <td> <td> <td> <td> <td></td><td>All</td><td>orbidden</td></td></td></td></td> | <td> <td> <td> <td></td><td>All</td><td>orbidden</td></td></td></td> | <td> <td> <td></td><td>All</td><td>orbidden</td></td></td> | <td> <td></td><td>All</td><td>orbidden</td></td> | <td></td><td>All</td><td>orbidden</td> | | All | orbidden |

	1				-					1				-											
C	2				V	_AN	Nam	e	dlinl	<_co	rpora	ate	(Ma	x: 32	cha	racte	ers)					Арр	ly		
vertisement	En	ablec	•	•																					
ort S	elect All	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
agged 🛛	All	۲																							\odot
Intagged 🛛	All																								
orbidden 🗌	All	\odot	\bigcirc	\odot	\bigcirc	\bigcirc	\bigcirc	\bigcirc	\bigcirc	\odot	\bigcirc	\bigcirc	\bigcirc	\odot	\bigcirc	\odot	\bigcirc	\odot							
lot Member 🗌	All	\odot	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲
gged Ports	1																								
tagged Ports																									

AN List	Add/Edit	VLA	N	F	ind VI	LAN			VL	AN E	atch	Sett	ngs		то	otal E	ntrie	s: 3						
ID dvertisement	3 Disable	ed 🖣		VI	.AN N	Nam	e	dlin	k_by	od		(Ma	x: 32	cha	racte	ers)					Арр	ly		
Port Si Tagged Untagged Forbidden Not Member	elect All 01 All © All © All © All ©	0	03 © © 0	04 ⓒ ⓒ ⓒ	05 © © 0	06 © ©	07 ○ ○ ○	08 © © ©	09 © © 0	10 © © 0	11 © © 0	12 © © 0	13 ○ ○ ○ 	14 ⓒ ⓒ ⓒ	15 © © 0	16 ⓒ ⓒ ⓒ	17 ⓒ ⓒ ⓒ	18 〇 〇 〇 〇 〇	19 〇 〇 〇 〇 〇	20 ○ ○ ○	21 © © 0	22 © © 0	23 © © 0	24 ○ ○ ○ ○
agged Ports Intagged Ports orbidden Ports																								

VLAN List	Add/Ed	it VLAN Find	/LAN VLA	N Batch Settings	Total Entries: 3		
VID	VLAN Name	Advertisement	Tagged Ports	Untagged Ports	Forbidden Ports		
1	default	Enabled		1-24		Edit	Delete
2	dlink_corp	Enabled	1			Edit	Delete
3	dlink byod	Disabled	1			Edit	Delete

 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-3160-24PC> Administration> Advanced Configuration> Networks.

Networks			O Safeguard
Wireless Network Configuration			
SSID	dlink_corporate		
Hide SSID			
Deny Broadcast			
VLAN	2	(1 to 4094)	
MAC Authentication	Local C RADIUS C Di:	sable	
Redirect	None O HTTP		E
Redirect URL]	
Wireless ARP Suppression Mode	Disable 💌		
L2 Distributed Tunneling Mode	Disable 💌		
L3 Tunnel	Disable 💌		

Networks			O Safeguard
Wireless Network Configuration			
SSID	dlink_byod		
Hide SSID			
Deny Broadcast			
VLAN	3	(1 to 4094)	
MAC Authentication	CLocal CRADIUS ODis	sable	
Redirect	None O HTTP		=
Redirect URL			
Wireless ARP Suppression Mode	Disable 💌		
L2 Distributed Tunneling Mode	Disable 💌		
L3 Tunnel	Disable 💌		

etworks Network Name			O Safeguar Add
Fotal Entries: 18		Dele	te Refresh
ID SSID	VLAN	Hide SSID S	ecurity Redirect
11 dlink11	1-default	Disabled N	one None
12 dlink12	1-default	Disabled N	one None
13 dlink13	1-default	Disabled N	one None
14 dlink14	1-default	Disabled N	one None
15 dlink15	1-default	Disabled N	one None
<u>16</u> dlink16	1-default	Disabled N	one None
17 dlink corporate	2-dlink_corporate	Disabled N	one None
<u>18</u> <u>dlink byod</u>	3-dlink_byod	Disabled N	one None
		2/2 <<	< 1 2 Go

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

3-1. Create an AP Profile "BYOD". Navigate to WLAN> DWS-3160-24PC> Administration> Advanced Configuration> AP Profiles> BYOD> Global.

AP Profiles			_	() Safeguard
Summary 1-Default	2-BYOD			
Global	Radio	VAP	Qos	
Access Point Profile Globa	Configuration			AP Profile2-BYOD
Profile Name	-	BYOD		
Hardware Type		Any		
Disconnected AP Data Forw	arding Mode	Enable 💌		
Disconnected AP Managem	ent Mode	Enable 💌		
Wired Network Detection VL	AN ID	1 (0 to 4094)		
		Apply	Clear	Delete

3-2. Associate SSID dlink_corporate and dlink_byod on this AP Profile. Navigate to WLAN> DWS-3160-24PC> Administration> Advanced Configuration> AP Profiles> BYOD> VAP.

	imary 1-Default		2-BYOD	ļ	luur				
lob	081		Radio		VAP		Qos		
								AP Profile2-BYOD	Â
		AP Coi	nfiguration :		U2.11b/g/n L3	Hide		Apply	
	Network			VLAN	Tunnel	SSID	Security	Redirect	
7	17-dlink_corporate	-	Edit	1-default	Disabled	Disabled	None	None	
V	18-dlink_byod	-	Edit	1-default	Disabled	Disabled	None	None	
	3-dlink3	-	Edit	1-default	Disabled	Disabled	None	None	Ξ
	4-dlink4	-	Edit	1-default	Disabled	Disabled	None	None	-
	5-dlink5	-	Edit	1-default	Disabled	Disabled	None	None	
	6-dlink6	-	Edit	1-default	Disabled	Disabled	None	None	
	7-dlink7	-	Edit	1-default	Disabled	Disabled	None	None	
	8-dlink8	-	Edit	1-default	Disabled	Disabled	None	None	
	9-dlink9	-	Edit	1-default	Disabled	Disabled	None	None	
	10-dlink10	-	Edit	1-default	Disabled	Disabled	None	None	
	11-dlink11	–	Edit	1-default	Disabled	Disabled	None	None	
	12-dlink12	-	Edit	1-default	Disabled	Disabled	None	None	
	13-dlink13		Edit	1-default	Disabled	Disabled	None	None	Ŧ

AP Profiles	O Safeguard
Summary 1-Default 2-BYOD	
Profile Name	Add Copy
	Apply Delete Refresh
Total Entries: 2	
Profile	Profile Status
<u>1-Default</u>	Configured
2-BYOD	Configured

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-3160-24PC> 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.

How to Configure a BYOD Environment with the DWS-3160

CP Configuration			() Safeguard
CP Summary Default	Employee		
CP Configuration	(English)		
CP Configuration Employ	yee		<u>۸</u>
Enable Captive Portal	Enabled	Idle Timeout(0-900 secs)	0
Configuration Name	Employee	Session Timeout(0-86400 secs)	86400
Protocol Mode	● HTTP ○ HTTPS	Max Up Rate(bytes/sec, 0=unlimited)	0
Verification Mode	◯ ORADIUS © RADIUS	Max Down Rate(bytes/sec, 0=unlimited)	0
User Logout Mode	🛇 Enabled 💿 Disabled	Max Receive(bytes, 0=unlimited)	0
Redirect Mode	© Enabled 💿 Disabled	Max Transmit(bytes, 0=unlimited)	0
Redirect URL		Max Total(bytes, 0=unlimited)	0
User Group	2-dlink_er 💌	Add Delete Modify	
	Code	Language	
	en	(English) Clear	
		Clear	
		Clear	-

5. Create Captive Portal accounts on local database.

Create user account under User Group "2-dlink_employee". Navigate to WLAN> DWS-3160-24PC> Security> Captive Portal> Local User.

Local User	_	_		O Safeguard
Local User Sum	nmary Local User Config	uration		
User Name	rosanna chu	(1 to 32 characters)	Session Timeout (secs)	0 (0 to 86400)
Password	••••••		Idle Timeout (secs)	0 (0 to 900)
User Group	1-Default 2-dlink_employee		Max Up Rate (bytes/sec) Max Down Rate (bytes/sec)	0 (0 = unlimited) 0 (0 = unlimited)
	-		Max Receive (bytes)	0 (0 = unlimited)
			Max Transmit (bytes)	0 (0 = unlimited)
			Max Total (bytes)	0 (0 = unlimited)
				Add

Local User		() Safeguard
Local User Summary	Local User Configuration	
		Add Delete Delete All
Total Entries: 1		
User	Session Timeout	Idle Timeout
🔲 <u>rosanna chu</u>	0	0
		1/1 1 Go

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.

Interface Associa	ation			0	Safeguard
CP Configuration Associated Interfaces	2 - Employee Wireless Network 17 - dlink_corporate Wireless Network 18 - dlink_byod Delete	Interface List	Physical Port: 1 Gigabit - Level Physical Port: 2 Gigabit - Level Physical Port: 3 Gigabit - Level Physical Port: 4 Gigabit - Level Physical Port: 6 Gigabit - Level Physical Port: 6 Gigabit - Level Physical Port: 8 Gigabit - Level Physical Port: 8 Gigabit - Level Add	•	

7. Create device MAC authentication database on local database.

7-1. Choose MAC Authentication Mode as "white-list". Navigate to WLAN> DWS-3160-24PC> Administration> Advanced Configuration> Global.

Global		O Safeguard
General SNMP Traps Distributed Tunneling		
· · · · · · · · · · · · · · · · · · ·		
Peer Group ID	1 (1 to 255)	<u>^</u>
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 corporateprovided NB MAC 08:11:96:71:00:00 in the database. The Authentication Action is "Grant". Navigate to WLAN> DWS-3160-24PC> Administration> Advanced Configuration> Client> Known Clients.

08-11-96-71-00-00 💌	
corporate-provide_rosanna	
🛇 Global Action 🔘 Grant 🛛 Deny	
	corporate-provide_rosanna

Known Clients		() Safeguard
MAC Address 00-00-00-00-00		Add
Total Entries: 1		Delete Delete All
MAC Address	Name	Authentication Action
08-11-96-71-00-00	corporate-provide_rosanna	grant
		1/1 1 Go

8. Discover and manage an AP from the network.

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

All AP Status	_	_				_	_		0	Safeguard
							Delete All	Manage	Ac	knowledge
Fotal Entries: 4										
MAC Address	Location	Switch Port	IP Address	Software Version	Age	Status	Profile	Radio	Channel	Authenticated Clients
FC-75-16-76-FF-40		1	192.168.10.101	4.2.0.9_B001	0d:00:00:01	Managed	2-BYOD	1 - 802.11a/n 2 - 802.11b/g/n	157 11	0 0
00-94-E4-FD-A0-6A	N/A	N/A	N/A	N/A	0d:00:05:06	Rogue	N/A	802.11a	52	N/A
AC-86-74-01-7C-9F	N/A	N/A	N/A	N/A	0d:00:02:07	Rogue	N/A	802.11b/g	1	N/A
C0-A0-BB-26-A2-19	N/A	N/A	N/A	N/A	0d:00:02:07	Rogue	N/A	802.11b/g	1	N/A
									1/1 1	Go

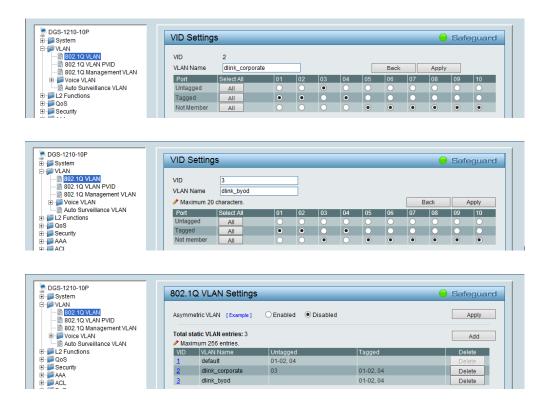
Configuration Steps (DGS-1210)

 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	Port ₂	Port ₃	Port4
VLAN1	Un-tag	Un-tag	-	Un-tag
VLAN2	Tag	Tag	Un-tag	Tag
VLAN ₃	Tag	Tag	-	Tag



How to Configure a BYOD Environment with the DWS-3160



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

	🍁 Wiza	ard	💽 He	lp 👻		_				104	💋 Logo
DGS-1210-10P ⊒		PoE	Port S	ettings						(Safeguar
VLAN 802.10 VLAN 802.10 VLAN 802.10 Management VLAN 802.10 Management VLAN 9 V 20 VLAN 400 Surveillance VLAN 410 Surveillance VLAN 9 12 Functions 9 005		1	e port 1 to	Port State 8 V Enabled port 8 can be set a W. Class 4: 30W.	▼ N/A		n 1W and 3	Prior	mal 🗸	Power Limit Auto Refresh by PSE: Class 1	Apply
AAA				.,							
Security AAA AA ACL POE POE PoE		Port	State	Time Range	Priority	Power	Power (W)	Voltage (V)	Current (mA)	Classification	Status
AAA ACL POE POE POE Global Settings			State Enabled		Priority					Classification N/A	Status POWER OFF
AAA ACL P PoE		1 2	Enabled Enabled	, Time Range	· ·	Limit	(W)	(V)	(mA)		
AAA ACL POE POE POE Global Settings POE Port Settings		1 2 3	Enabled Enabled Enabled	Time Range N/A N/A N/A	Normal Normal Normal	Limit Auto Auto Auto	(W) 0.0 0.0 0.0	(V) 0.0 0.0 0.0	(mA) 0.0 0.0 0.0	N/A N/A N/A	POWER OFF POWER OFF POWER OFF
AAA ACL POE POE Global Settings POE Port Settings SNMP		1 2 3 4	Enabled Enabled Enabled Enabled	Time Range N/A N/A N/A N/A	Normal Normal Normal Normal	Limit Auto Auto Auto Auto	(W) 0.0 0.0 0.0 0.0	(V) 0.0 0.0 0.0 0.0	(mA) 0.0 0.0 0.0 0.0	N/A N/A N/A N/A	POWER OFF POWER OFF POWER OFF POWER OFF
		1 2 3 4 5	Enabled Enabled Enabled Enabled Enabled	Time Range N/A N/A N/A N/A N/A	Normal Normal Normal Normal Normal	Limit Auto Auto Auto Auto Auto	(W) 0.0 0.0 0.0 0.0 0.0	(V) 0.0 0.0 0.0 0.0 0.0 0.0	(mA) 0.0 0.0 0.0 0.0 0.0 0.0	N/A N/A N/A N/A N/A	POWER OFF POWER OFF POWER OFF POWER OFF POWER OFF
		1 2 3 4 5 6	Enabled Enabled Enabled Enabled	Time Range N/A N/A N/A N/A	Normal Normal Normal Normal	Limit Auto Auto Auto Auto	(W) 0.0 0.0 0.0 0.0	(V) 0.0 0.0 0.0 0.0	(mA) 0.0 0.0 0.0 0.0	N/A N/A N/A N/A	POWER OFF POWER OFF POWER OFF POWER OFF

Configuration Steps (DSR-500N)

 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.

D-Li	-					
	1					
DSR-500N		SETUP	ADVANCED	TOOLS	STATUS	HELP
Wizard	►					Helpful Hints
Internet Settings	►	AVAILABLE VLANS			LOGOUT	Enter Name and ID and save the settings. Make
Wireless Settings	►	This page allows user to e	nable/disable VLAN support	t on the LAN.		sure that the ID provided is unique. Once the
Network Settings	►	Save Settings	Don't Save Settin	gs		settings are saved, you will be shown the List of
DMZ Setup	►	VLAN Configuration				Available VLANs where you can further add new VLAN(s) or edit/delete
VPN Settings	►			P 1 1		existing VLAN(s).
USB Settings	►	Name:		link_corporate		More
VLAN Settings	\triangleright	Id:	2			
		Inter VLAN Routing	g Enable: 🛛 🕅	1		
DSR-500N		SETUP	ADVANCED	TOOLS	STATUS	HELP
Wizard	►					Helpful Hints
Internet Settings	۲	AVAILABLE VLANS			LOGOUT	Enter Name and ID and save the settings. Make
Wireless Settings	۲	This page allows user to e	nable/disable VLAN support	t on the LAN.		sure that the ID provided is unique. Once the
Network Settings	۲	Save Settings	Don't Save Settin	igs		settings are saved, you will be shown the List of
DMZ Setup	►	MAN Configuration				Available VLANs where you can further add new VLAN(s) or edit/delete
VPN Settings	►	VLAN Configuration				existing VLAN(s).
USB Settings	►	Name:		link_byod		More
VLAN Settings	D	Id:	3			
		Inter VLAN Routing	j Enable: 🛛 🛛	/		

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

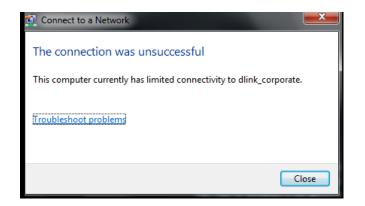
1-2. Enable DHCP server on default VLAN, VLAN2 and VLAN3. Navigate to SETUP> VLAN Settings> Multiple VLAN Subnets.

How to Configure a BYOD Environment with the DWS-3160

DSR-500N	SETUP	ADVANCED	TOOLS	STATUS	HELP				
Wizard 🕨		·	·		Helpful Hints				
Internet Settings	MULTI VLAN SUBNET	CONFIG		LOGOUT	By default, when you add a new VLAN, it is assigned				
Wireless Settings 🕨	This page shows the list o	an IP address of 192.168.2.1 with subnet-							
Network Settings	Save Settings	mask 255.255.255.0, the next added one is assigned 192.168.3.1 and							
DMZ Setup									
VPN Settings	MULTI VLAN SUBNET	1			assigned IP address, subnet mask and many other options here. The				
USB Settings	IP Address:	-	168.10.1		only non-editable field in VLAN ID.				
VLAN Settings					More				
	Subnet Mask:	255	.255.255.0						
	DHCP								
	DHCP Mode:	DH	CP Server 💌						
	Domain Name:	DLir	nk						
	Starting IP Addres	s: 192	.168.10.100						
	Ending IP Address:	192	.168.10.254						

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:E9, 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



2. 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.



www.dlink.com

D-Link, D-Link sub brand logos and D-Link product trademarks are trademarks or registered trademarks of D-Link Corporation and its subsidiaries. R11 otxer twird party marks mentioned werein are trademarks of the respective owners.

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