2.6 Enable IEEE802.1X on switch.

2.6.1. Setup your FreeRADIUS server

a. Setup the IP address of your RADIUS server to 10.90.90.100/8b. Add a client entry to the FreeRADIUS server, client.conf file for the 10.0.0.0/8 network:

```
client 10.0.0/8 {
    secret = 12345678
    shortname = Radius_Authentication
}
```

c. Add a user to the the users.conf file as following

```
User1 Auth-Type := EAP, User-Password == "123456789"
```

```
🗱 D:\Dean\Wy\D-Link Relative\20080910-Switch 802.1x\users.conf - Notepad++
                                                                                     Eile Edit Search View Format Language Settings Macro Run TextFX Plugins Window ?
  ] 🔁 🖶 🖕 🕞 🚵 🖌 🐚 🌆 🧶 😋 🛤 🍢 🔍 😤 ⊑ 🖕 🖬 🐺 🐷 🗩 🐼 🖼
🔚 change log 🔚 clients.conf 🚆 eap.conf 🔚 radius.log 😑 users.conf 🔚 users.conf
  221
       #DEFAULT
                                                                                           ^
       # Service-Type = Login-User,
   222
       #
            Login-Service = Rlogin,
   223
       # Login-IP-Host = shellbox.ispdomain.com
   224
   225
   226 ##
   227
       # # Last default: shell on the local terminal server.
   228
       # #
   229 # DEFAULT
   230 # Service-Type = Shell-User
   231
   232
       # On no match, the user is denied access.
   233
   234
       # For Wireless Clients MAC Authentication security
   235
   236
       00-13-02-20-33-B3 Auth-Type := Local, User-Password == "NOPASSWORD"
   237
       00-1C-BF-AA-02-AB Auth-Type := Local, User-Password == "NOPASSWORD"
   238
   239
       # For AP Validation
       00-17-9a-d2-8d-70 Auth-Type := Local, User-Password == ""
   240
   241
   242
       # For Switch 802.1X
   243
       User1 Auth-Type := EAP, User-Password == "12345678"
   244
   245
        # For EAP-PEAP
   246
       Test Auth-Type := EAP, User-Password == "testtest"
   247
Normal text file nb char : 8196
                                 Ln:243 Col:52 Sel:0
                                                                 Dos\Windows ANSI
                                                                                       INS
```

d. Save and restart your RADIUS server

2.6.2. Add the IP address of the RADIUS server on Switch, and give it correct settings

a. Go to LAN tab Security \rightarrow RADIUS \rightarrow RADIUS Authentication Server Configuration, select Add and give the 10.90.90.100 as the IP Address

	D-L ink			1 3	5 7	9 11	13 15	17 19	21 23	Combol Combo3
D-Link	Power Console	Link/ACT/Spec O PoE			گ گ	گگ			گ گ	
Building Networks for People	0 RPS	-	Concolo			10 12	14 16	18 20	22 24	
	DW3-5024	CULTURE CULTURE	Compose	- +		10 12	14 10	02 01	44. (44	Comboz Comboy
	Tool							Ì	🥖 Logo	ut 🕜 Hel
DWS-3024	RADIUS Authentication	Server Configu	ration							
Administration					-					
L2 Features	RADIUS Server IP Address	s			Add	*				
L3 Features	IP Address				10.90	90.100				
in Qos										
Access Control Lists			Subr	nit						
Security			-							
Port Security Administ										
Port Security Interface										
Port Security Static										
SSL Configuration										
SSH Configuration										
🖯 🍘 Radius										
Radius Configuratio										
RADIUS Authentica										
Accounting Server										
Clear Statistics										

- b. Specify the following settings
- **Port** 1812
- Secret 12345678 (Apply)
- Primary Server Yes

Then press the "Submit".

DISC	D-Li &	1 3 5 7 9 11 13 15 17 19 21 23 CombotCombod
Building Networks for People	O Concole O RPS DWS-3024	Concole 2 4 5 8 10 12 14 16 18 20 22 24 Combo2Combo4
	Tool	💋 Logout 📀 Help
🗃 DWS-3024	RADIUS Authentication Server Confi	guration
Administration L2 Features	RADIUS Server IP Address	10.90.90.100 🗸
E Castures	Port	1812 (0 to 65535)
€ 🕼 QoS	Secret	Apply
Access Control Lists	Primary Server	
🖻 📾 Security 🧧	Message Authenticator	Enable
Port Security Administ	Secret Configured	No
Port Security Static	Current	Yes
SSL Configuration		
SSH Configuration	Su	bmit Remove Refresh
🖻 🗃 Radius		
Radius Configuratio		
RADIUS Authentica		
Accounting Server (
security/radius/radius_server.html		😱 🎱 Internet 🔍 100% 👻

2.6.3. Add a new authentication list on switch.

a. Go to LAN tab \rightarrow Administration \rightarrow Authentication List, Select Create and give it a name as Wired_Auth

	(WLAN	Tool			- 100 Logout
DWS-40	026 ninistration	Authentication List Config	uration		
	initial auton system Description switch Configuration card Configuration terial Port P Address letwork DHCP Client (ITTP Configuration leser Accounts tuthentication List Cor liser Accounts benial Of Service Prot fultiple Port Mirroring releat Sessions Dubbound Telnet Clien ite Tarb	Authentication List Authentication List Name	Create Vired_Auth	(1 to 15 Alphanumeric Characters)	

b. Set the radius as the first authentication method for this list.

LAN	WLAN	🔨 Tool 🔰	
🛅 DW	5-4026	Authentication List Configuration	
÷ 🔁 i	Administration	Automication List Configuration	
	System Description	Authentication List	Wired Auth
- Ē	Switch Configuration	Method 1	radius 🔻
-E	Card Configuration	Method 2	
-C	PoE Configuration	Method 2	
-C	Serial Port	Method 3	undefined 🔽
-8	IP Address		
-6	Network DHCP Client (Submit Del	ete
-6	HTTP Configuration		
	User Accounts		
Ē	Authentication List Cor		
Ē	User Login		
	Denial Of Service Prot		
···(Multiple Port Mirroring		
	Telnet Sessions		
	Outbound Telnet Clien		

c. LAN \rightarrow Security \rightarrow Port Access Control \rightarrow User Login Configuration, choose Wired_Auth, and click submit to assign the Wire_auth as the Non-configured user authentication list for 802.1x

🗄 🔁 QoS	K Tool	
🗄 🧰 Access Control Lists		
🖻 🚖 Security	Port Access Control User Login Configuration	
Port Security Administ		
Bort Security Interface	Users Non-configured user	
Port Security Static	Login	
SSL Configuration	Wired Auth	
SSH Configuration		
🗄 🛅 Captive Portal		
E C RADIUS		
Port Access Control	Submit Refresh	
Configuration		_
Port Configuration		
PAE Capability Cont		
Supplicant Port Con		
Port Access Privileg		
E TACACS+		

2.6.4. Configure the ports that don't need to be authenticated.

a. Go to LAN \rightarrow Security \rightarrow Port Access Control \rightarrow Port Configuration, select Port 0/1 and from the Control Mode option, select Force Authorized.

QoS			
Access Control Lists	Port Access Control Port Configuration		
Security	Port	0/1 💌	L
Port Security Interface	Control Mode	Force A	Authorized
Port Security Static	Quiet Period (secs)	60	(0 to 65535)
SSL Configuration	Transmit Period (secs)	30	(1 to 65535)
SSH Configuration	Guest VLAN ID	0	(0 to 3965)
RADIUS	Guest VLAN Period (secs)	90	(1 to 300)
Port Access Control	Unauthenticated VLAN ID	0	(0 to 3965)
Configuration	Supplicant Timeout (secs)	30	(1 to 65535)
PAE Capability Cont	Server Timeout (secs)	30	(1 to 65535)
Supplicant Port Con	Maximum Requests	2	(1 to 10)
🗒 User Login Configur	Reauthentication Period (secs)	3600	(1 to 65535)
Port Access Privileg	Reauthentication Enabled	False	-
TACACOT	Maximum Users	16	14 4 4 63

b. Do the same setting on **Port 0/20**

2.6.5. Enable the 802.1X

a. Connect your RADIUS Server to port 19, your PC that used to configure Switch connect to port 20

b. Enable the 802.1X Go to LAN → Security → Port Access Control → configuration, Enable the Administrative Mode

NOTE: Before you enable the 802.1X, please make sure you finish the step 2.6.4, and connect to the correct port, or you will loose all the connections.

H 1 13 Features	Tool	🧖 Logi
🗄 🛅 QoS		
Access Control Lists	Port Access Control Configuration	
E Security		
Port Security Administ	Administrative Mode	Enable
Port Security Interface	VLAN Assignment Mode	Disable -
Port Security Static		,
SSL Configuration	Submit	Cancel
SSH Configuration		
E Captive Portal		
E C RADIUS		
Port Access Control		
Configuration		
Port Configuration		
PAE Capability Cont		
Supplicant Port Con		
User Login Configur		
Port Access Privileg		
E TACACS+		

2.7 Configure the PC as the 802.1X supplicant.

[Client XP or Vista or Win7]:

1. Use the MMC and go to the **Services**, check the **Wired AutoConfig** services is Started.

File Action View Favorite	s Window Help								
🗢 🤿 🙋 📅 📴 🤹 🛃	2 🗊 🕨 🗉 II ID								
Console Root	O Consiste (Learn)								Actions
Services (Local)	Services (Local)								Services (Local)
		AL ^	D	C 1.1	C				Services (Local)
	Wired AutoConfig	Name	Description	Status	startup Type	Log Un As			More Actions
		Windows Error Re	Allows error	Started	Automatic	Local Syste			Wired AutoConfig
	Stop the service	Windows Event C	This service		Manual	Network S			More Actions
	Restart the service	Windows Event Log	This service	Started	Automatic	Local Service			
		Windows Firewall	Windows Fi	Started	Automatic	Local Service			
		Windows Font Ca	Optimizes p	Started	Manual	Local Service			
	Description	Windows Image A	Provides im	Started	Automatic	Local Service			
	Description:	Windows Installer	Adds, modi		Manual	Local Syste			
	This service performs IEEE	Windows Live Fa	This service		Manual	Local Syste			
	802.1X authentication on	Windows Live ID S	Enables Win	Started	Automatic	Local Syste			
	Ethernet interfaces	Windows Live Me	Lets you co		Disabled	Local Syste			
		Windows Manage	Provides a c	Started	Automatic	Local Syste			
		Windows Media C	Allows Win		Disabled	Local Service			
		Windows Media C	Windows M		Manual	Network S			
		Windows Media C	Starts and st		Manual	Network S			
		Windows Media C	Starts Wind		Automatic (D	Local Service			
		🖓 Windows Media P	Shares Win		Manual	Network S			
		Windows Module	Enables inst		Manual	Local Syste			
		😪 Windows Presenta	Optimizes p	Started	Manual	Local Service			
		🔍 Windows Presenta	Optimizes p		Manual	Local Service			
		🧠 Windows Remote	Windows R		Manual	Network S			
		🔍 Windows Search	Provides co	Started	Automatic	Local Syste			
		🎧 Windows Time	Maintains d	Started	Automatic	Local Service			
		🌼 Windows Update	Enables the	Started	Automatic (D	Local Syste			
	l r	Se WINTER WED FILL	WHILITTE I		ivianuai	Local Service	1		
		🌼 Wired AutoConfig	This service	Started	Manual	Local Syste			
		WLAN Autocomig	This service	Starteu	Automatic	Local Syste		=	
		🔍 WMI Performance	Provides pe		Manual	Local Syste			
		🔍 Workstation	Creates and	Started	Automatic	Local Service			
		🔍 XAudioService	User-mode	Started	Automatic	Local Syste		+	
	Extended Standard							_	

2. Under the NIC setting, make sure the **Authentication** tab come up. Then click the **Settings** button.

General	Networking Authentication Sharing
Connection IPv4 Connectivity: IPv6 Connectivity: Media State: Duration: Speed: Details	Local Select this option to provide authenticated network access for this Ethemet adapter.
Activity Sent Rec Bytes: 5,806,159 30,85 Properties Plasable Diagnose	to this network
	Close Crossel

3. Click the **Configure..** button and disselect the **Automatically.....**

Mhen connecting:	s 18 20 22 24 25 atus	1.28 I Area Co
Connect to these servers:	Network	king Au
Trusted Root Certification Authorities: AddTrust External CA Root Class 3 Public Primary Certification Authority DigiCert High Assurance EV Root CA DST Root CA X3 Entrust.net Certification Authority (2048) Entrust.net Secure Server Certification Authority	Local Selic Limited Enabled I 05:03:56 100.0 Mbps Mi	ect this o Ethemet Enable IB pose a ne crosoft: F
Equifax Secure Certificate Authority Equifax Secure Certificate Authority Do not prompt user to authorize new servers or trusted certification authorities.	EAP MSCHAPv2 Properties	x
Select Authentication Method:	Automatically use my Windows logon name password (and domain if any).	and
Secured password (EAP-MSCHAP v2) Configure	OK Cancel	