Configuration Guide

How to Configure a BYOD Environment with the DWS-3160

(RADIUS Server)

Overview

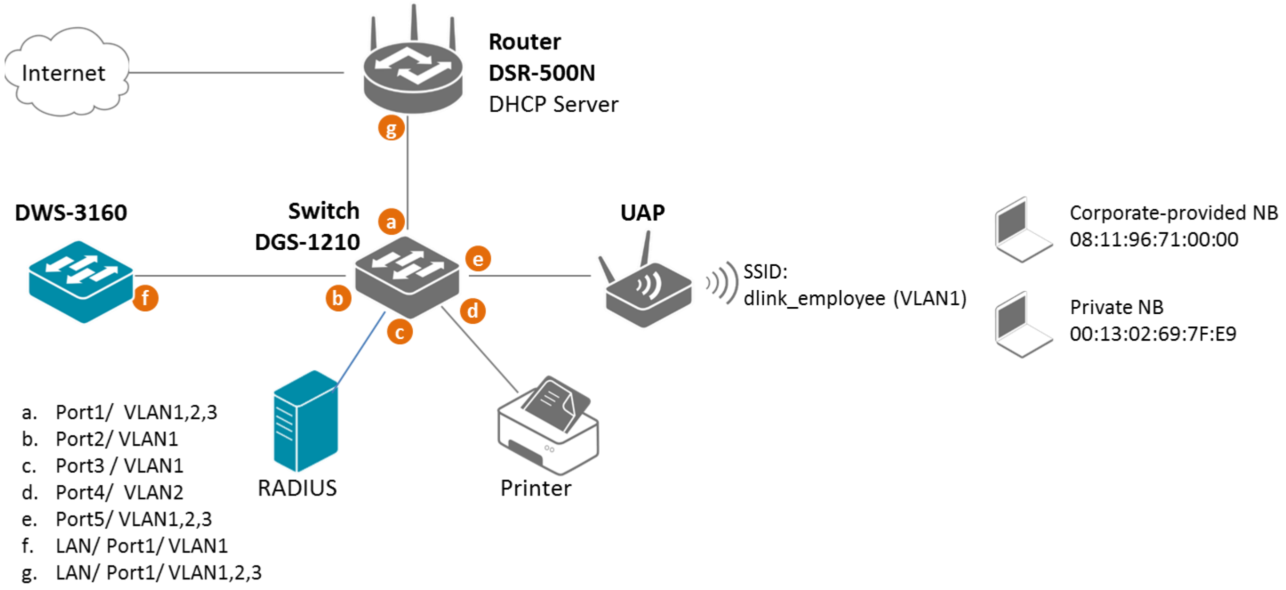
This guide describes how to configure and implement BYOD environment with the D-Link DWS-3160 Unified Switch for user and device authentication.

D-Link®

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 single SSID on DWS-3160 and external RADIU (FreeRADIUS) server. Use username, password, and device MAC info to assign particular VLAN. All connection from the SSID required performing authentication before granted authority.



The security protocol on SSID dlink_employee is WPA2 Enterprise. The authentication database is external RADIUS server. In the RADIUS database, one user account includes username, password, and device MAC address which is the corporate-provided. The authorized network is assigned based on authentication information:

- If authentication info matches username, password, and device MAC address of the user account, the user is authorized in VLAN2 network.
- If authentication info matches username and password, but it doesn't match the device MAC address (for example, use the Private NB to log on), the user is authorized in VLAN3 network.
- If authentication info doesn't match either username or password, the user doesn't get any access.

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 (FreeRADIUS)

1. Basic Requirement

   In order to setup the RADIUS server, the following is the minimum requirement.

   - A standard x86/x86-64 PC
   - Installed Fedora Linux distribution (Fedora 18+ is preferred)
   - 10GB HDD storage at least
   - 1GB ram at least
   - Internet connection

2. Recommend Software Package list

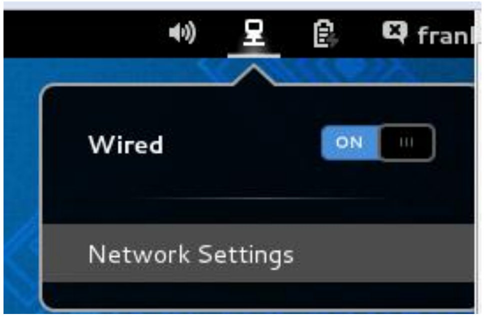
   All configuration steps are verification base on software version below:

Software Type	Software Name	Version
Operation System	Fedora	3.9.5-301.fc19.x86_64
FreeRadius	freeradius	2.2.0-6.fc19.x86_64
FreeRadius	freeradius-utils	2.2.0-6.fc19.x86_64
FreeRadius	freeradius-postgresql	2.2.0-6.fc19.x86_64
Postgresql	postgresql-server	9.2.6-1.fc19.x86_64
Postgresql	postgresql-libs	9.2.6-1.fc19.x86_64

3. Configure IP address on Fedora via GUI.

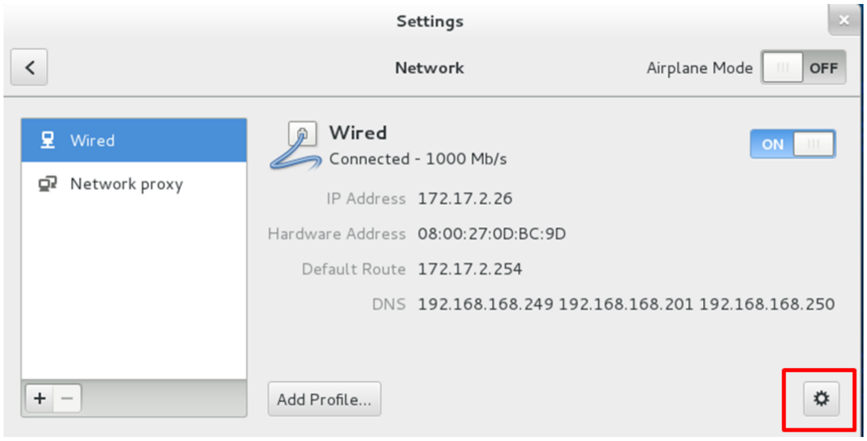
   3-1. Log in as root in GUI.

   3-2. Select Network Settings.



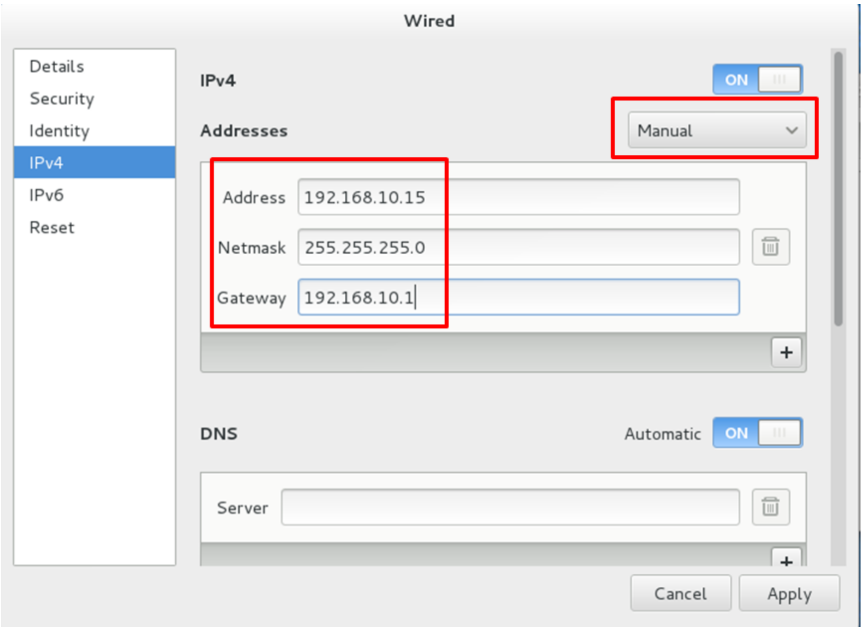
   3-3. Click the gear. Manually set the IP address, Netmask and Gateway. In this case, set the FreeRADIUS IP address as 192.168.10.15. The Netmask is 255.255.255.0. The Gateway IP address is 192.168.10.1.

   Note: Make sure the RADIUS server connect to internet before process following procedures.



Wired
Connected - 1000 Mb/s

IP Address 172.17.2.26
Hardware Address 08:00:27:0D:BC:9D
Default Route 172.17.2.254
DNS 192.168.168.249 192.168.168.201 192.168.168.250



IPv4: ON

Addresses: Manual

Address 192.168.10.15
Netmask 255.255.255.0
Gateway 192.168.10.1

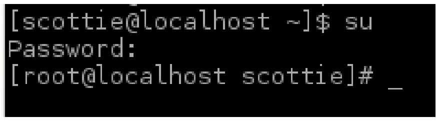
DNS Automatic: ON

Server

4. Manual-Installation Procedure
   Install FreeRADIUS steps-by-steps through the following description.

   4-1. Open a terminal console and switch to root account

   Use the su command and enter root's password to get the root privilege as the following steps are all needed root privilege.

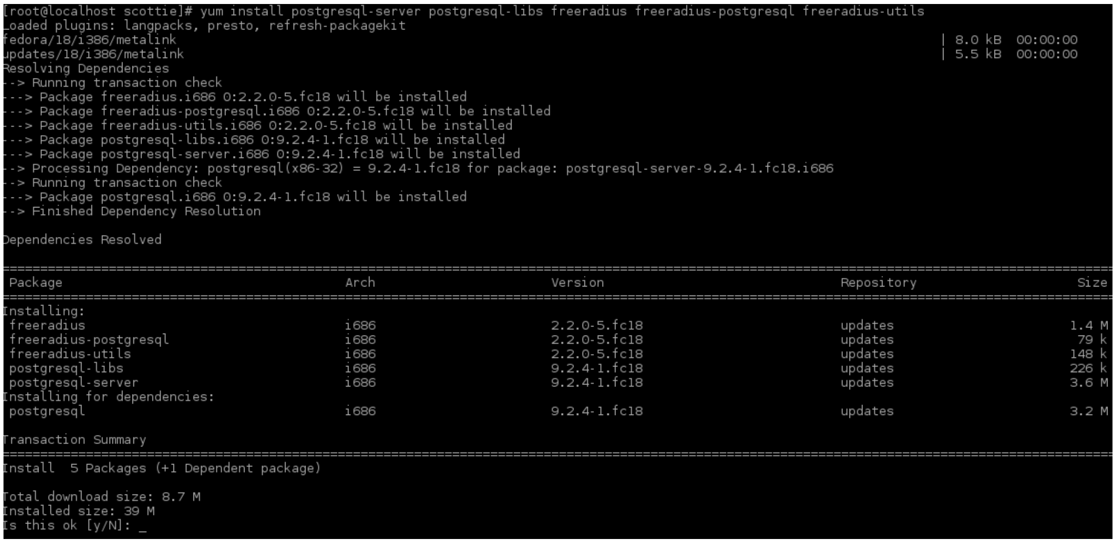


```
[scottie@localhost ~]$ su
Password:
[root@localhost scottie]# _
```

4-2. Install the required package (the table listed in above)

Use the following command to install freeradius, postgresql, and the libraries. In default, the installation path for FreeRADIUS is /etc/raddb.

```
----------------------
yum install postgresql-server postgresql-libs freeradius freeradius-postgresql freeradius-utils
----------------------
```



```
[root@localhost scottie]# yum install postgresql-server postgresql-libs freeradius freeradius-postgresql freeradius-utils
Loaded plugins: langpacks, presto, refresh-packagekit
fedora/18/i386/metalink                                                              | 8.0 kB  00:00:00
updates/18/i386/metalink                                                             | 5.5 kB  00:00:00
Resolving Dependencies
--> Running transaction check
---> Package freeradius.i686 0:2.2.0-5.fc18 will be installed
---> Package freeradius-postgresql.i686 0:2.2.0-5.fc18 will be installed
---> Package freeradius-utils.i686 0:2.2.0-5.fc18 will be installed
---> Package postgresql-libs.i686 0:9.2.4-1.fc18 will be installed
---> Package postgresql-server.i686 0:9.2.4-1.fc18 will be installed
--> Processing Dependency: postgresql(x86-32) = 9.2.4-1.fc18 for package: postgresql-server-9.2.4-1.fc18.i686
--> Running transaction check
---> Package postgresql.i686 0:9.2.4-1.fc18 will be installed
--> Finished Dependency Resolution

Dependencies Resolved

=========================================================================================================================
 Package                           Arch                  Version                         Repository                  Size
=========================================================================================================================
Installing:
 freeradius                        i686                  2.2.0-5.fc18                    updates                    1.4 M
 freeradius-postgresql             i686                  2.2.0-5.fc18                    updates                     79 k
 freeradius-utils                  i686                  2.2.0-5.fc18                    updates                    148 k
 postgresql-libs                   i686                  9.2.4-1.fc18                    updates                    226 k
 postgresql-server                 i686                  9.2.4-1.fc18                    updates                    3.6 M
Installing for dependencies:
 postgresql                        i686                  9.2.4-1.fc18                    updates                    3.2 M

Transaction Summary
=========================================================================================================================
Install  5 Packages (+1 Dependent package)

Total download size: 8.7 M
Installed size: 39 M
Is this ok [y/N]: _
```

4-3. Configure FreeRADIUS. All configuration files for FreeRADIUS will be stored under /etc/raddb.

Add the management VLAN in the FreeRADIUS. Edit /etc/raddb/client.conf. Add shared secret for each client or each subnet. And save.

The fill in information is as below:

- short_name : the name of this entry
- secret : the secret for to this entry
- ipaddr and netmask : the ip address for this entry, you can specify an address or a subnet

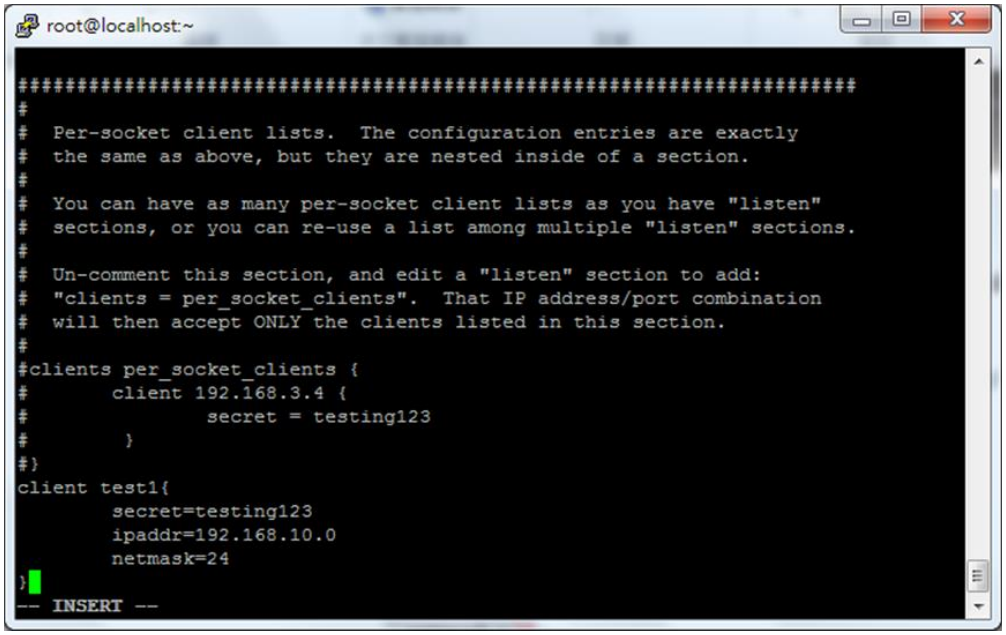
The red items are the options you can edit

```
--------------------------------------
client  short_name{
        secret = shared_secret
        ipaddr = 192.168.0.0
        netmask = 24
```

}

In this case, add VLAN1 IP subnet. For example, add a new entry named **test1**, secret is **testing123**, and the subnet is **192.168.10.0/24**

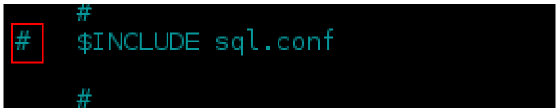
```
client test1{
        secret=testing123
        ipaddr=192.168.10.0
        netmask=24
}
```



```
#######################################################################
#
#  Per-socket client lists.  The configuration entries are exactly
#  the same as above, but they are nested inside of a section.
#
#  You can have as many per-socket client lists as you have "listen"
#  sections, or you can re-use a list among multiple "listen" sections.
#
#  Un-comment this section, and edit a "listen" section to add:
#  "clients = per_socket_clients".  That IP address/port combination
#  will then accept ONLY the clients listed in this section.
#
#clients per_socket_clients {
#       client 192.168.3.4 {
#               secret = testing123
#        }
#}
client test1{
        secret=testing123
        ipaddr=192.168.10.0
        netmask=24
}
```

4-4. Setup SQL server is as source database. Uncomment sql.conf in /etc/raddb/radiusd.conf.

Remove "#" in the beginning of "$INCLUDE sql.conf" to enable SQL as the data source of FreeRADIUS. And save.

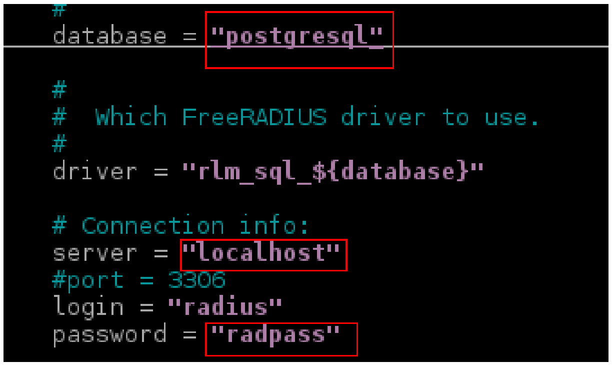


```
        #
#       $INCLUDE sql.conf

        #
```

4-5. Setup database type, host name and server username/ password.

Edit below info under /etc/raddb/sql.conf. And save.

4-5-1. Set "database" = "postgresql"
4-5-2. Set "server" = the database server ip. Leave it as "localhost" if you don't have separate database.
4-5-3. Change "password" as desired. Suggest keep it as "radpass"

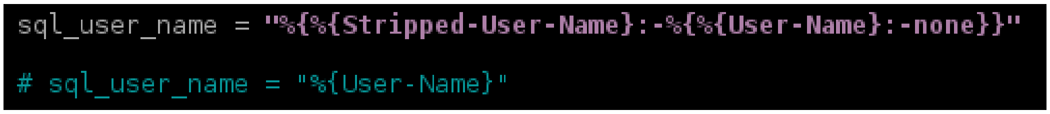


```
#
database = "postgresql"

#
#  Which FreeRADIUS driver to use.
#
driver = "rlm_sql_${database}"

# Connection info:
server = "localhost"
#port = 3306
login = "radius"
password = "radpass"
```

4-6. Edit log in format.

Edit below info under /etc/raddb/sql/postgresql/dialup.conf. And save.

4-6-1. Remove "#" in the beginning of "sql_user_name = "%{%{Stripped-User-Name}:-%{%{User-Name}:-none}}" "
4-6-2. Add "#" in the beginning of "sql_user_name = "%{User-Name}""

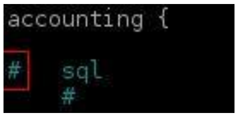


```
sql_user_name = "%{%{Stripped-User-Name}:-%{%{User-Name}:-none}}"

# sql_user_name = "%{User-Name}"
```

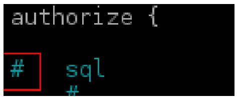
4-7. Enable Authorize and Accounting function on the SQL.

Edit below info under /etc/raddb/sites-enabled/default. And save.

4-7-1. Remove "#" in the beginning of "sql" in the sections of "authorize", "accounting"



```
accounting {

#     sql
      #
```



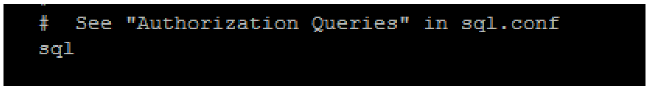
```
authorize {

#     sql
      #
```

4-7-2. Please insert text below to the /etc/raddb/sites-enabled/default after line 511 and save change.

```
-----------------------------------------------------------------------------
if ( "%{request:Calling-Station-Id}" != "" && "%{request:Calling-Station-Id}" == "%{sql: SELECT callingstationid FROM radmacvlan WHERE username='%{User-Name}' and callingstationid=upper('%{request:Calling-Station-Id}')}" ) {
        update reply {
            Tunnel-Private-Group-ID := "%{sql: SELECT tunnelprivategroupid FROM radmacvlan WHERE username='%{User-Name}' and callingstationid=upper('%{request:Calling-Station-Id}')}"
            Tunnel-Type := "%{sql: select value from radgroupreply right outer join radusergroup on radgroupreply.groupname=radusergroup.groupname where radusergroup.username='%{User-Name}' and radgroupreply.attribute='Tunnel-Type' }"
            Tunnel-Medium-Type := "%{sql: select value from radgroupreply right outer join radusergroup on radgroupreply.groupname=radusergroup.groupname where radusergroup.username='%{User-Name}' and radgroupreply.attribute='Tunnel-Medium-Type' }"
        }
    }
    else {
        update reply {
            Tunnel-Private-Group-Id := "%{sql: select value from radgroupreply right outer join radusergroup on radgroupreply.groupname=radusergroup.groupname where radusergroup.username='%{User-Name}' and radgroupreply.attribute='Tunnel-Private-Group-Id' }"
            Tunnel-Type := "%{sql: select value from radgroupreply right outer join radusergroup on radgroupreply.groupname=radusergroup.groupname where radusergroup.username='%{User-Name}' and radgroupreply.attribute='Tunnel-Type' }"

             Tunnel-Medium-Type := "%{sql: select value from radgroupreply right outer join radusergroup on radgroupreply.groupname=radusergroup.groupname where radusergroup.username='%{User-Name}' and radgroupreply.attribute='Tunnel-Medium-Type' }"

        }
    }

-----------------------------------------------------------------------------
```

3-8. Edit /etc/raddb/sites-enabled/ inner-tunnel

Remove "#" in the beginning of "sql" in the sections of "authorize"



```
#   See "Authorization Queries" in sql.conf
sql
```

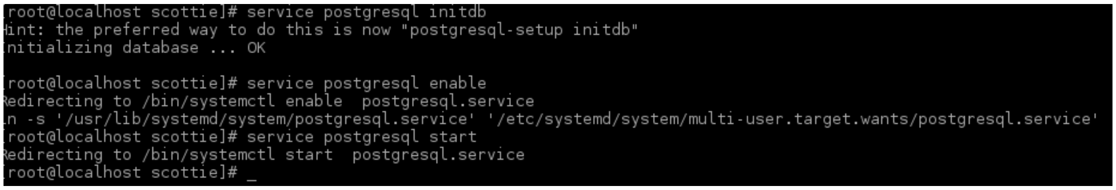
5. Setup PostgreSQL server

5-1. Start Postgresql service

Execute the following commands to init and start postgresql. And save.

----

service postgresql initdb
service postgresql enable
service postgresql start



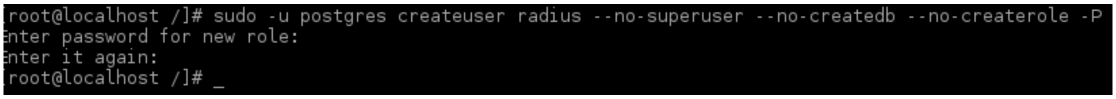
```
[root@localhost scottie]# service postgresql initdb
Hint: the preferred way to do this is now "postgresql-setup initdb"
Initializing database ... OK

[root@localhost scottie]# service postgresql enable
Redirecting to /bin/systemctl enable  postgresql.service
ln -s '/usr/lib/systemd/system/postgresql.service' '/etc/systemd/system/multi-user.target.wants/postgresql.service'
[root@localhost scottie]# service postgresql start
Redirecting to /bin/systemctl start  postgresql.service
[root@localhost scottie]# _
```

5-2. Create a database user for FreeRADIUS.

5-2-1. Create a database user for FreeRADIUS. Please note that the username and password must be matched with username/password which set in /etc/raddb/sql.conf. In the settings of previous steps, the username/ password are radius/ radpass.

----

sudo -u postgres createuser radius --no-superuser --no-createdb --no-createrole –P



```
[root@localhost /]# sudo -u postgres createuser radius --no-superuser --no-createdb --no-createrole -P
Enter password for new role:
Enter it again:
[root@localhost /]# _
```

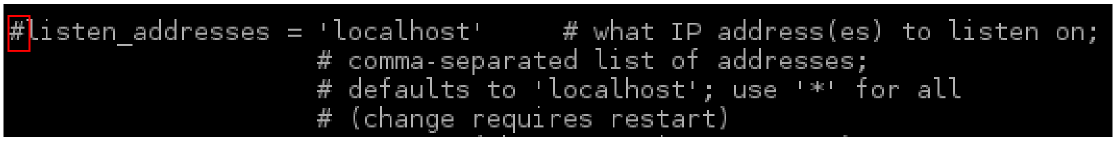
5-2-2. Create a database for FreeRadius
Create a database for FreeRADIUS. The owner of this database should be the one we defined in /etc/raddb/sql.conf.

----

sudo -u postgres createdb radius --owner=radius

5-2-2-1. Modify PostgreSQL listen address

Set IP address that PostgreSQL are listened on. Edit /var/lib/pgsql/data/postgresql.conf. Remove "#" in the beginning listen_addresses. And save.



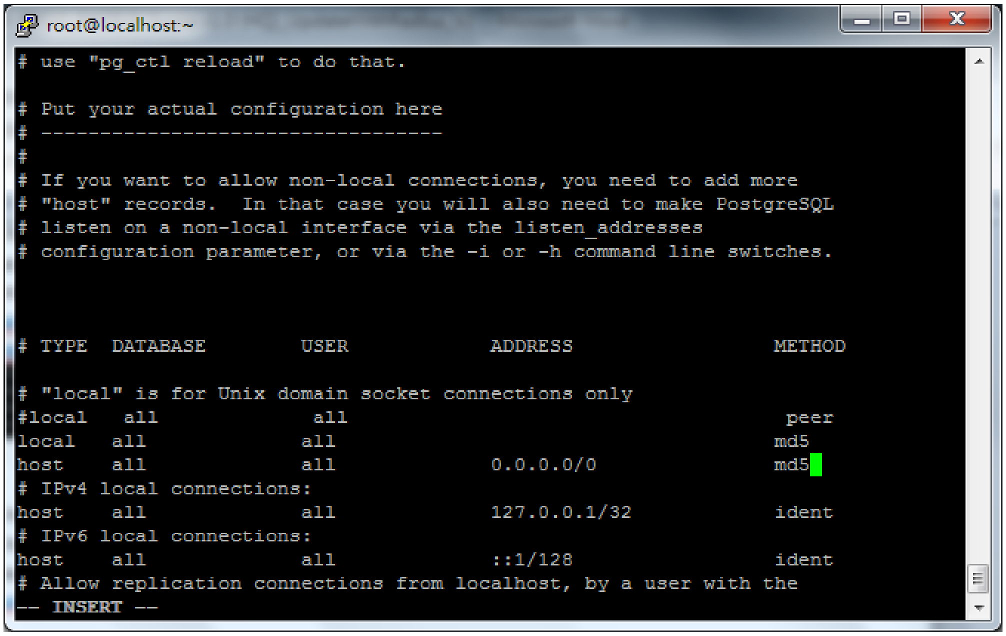
```
#listen_addresses = 'localhost'         # what IP address(es) to listen on;
                                        # comma-separated list of addresses;
                                        # defaults to 'localhost'; use '*' for all
                                        # (change requires restart)
```

5-2-2-2. Edit /var/lib/pgsql/data/pg_hba.conf.

Remove "#" in the beginning of "local all all peer".

Add two pieces info in the next line.

```
local    all    all    md5
host     all    all    0.0.0.0/0       md5
```



```
# use "pg_ctl reload" to do that.

# Put your actual configuration here
# ----------------------------------
#
# If you want to allow non-local connections, you need to add more
# "host" records.  In that case you will also need to make PostgreSQL
# listen on a non-local interface via the listen_addresses
# configuration parameter, or via the -i or -h command line switches.



# TYPE  DATABASE        USER            ADDRESS                 METHOD

# "local" is for Unix domain socket connections only
#local   all             all                                     peer
local   all             all                                     md5
host    all             all             0.0.0.0/0               md5
# IPv4 local connections:
host    all             all             127.0.0.1/32            ident
# IPv6 local connections:
host    all             all             ::1/128                 ident
# Allow replication connections from localhost, by a user with the
-- INSERT --
```

5-2-2-3. Run the following command to re-start PostgreSQL

----

service postgresql restart

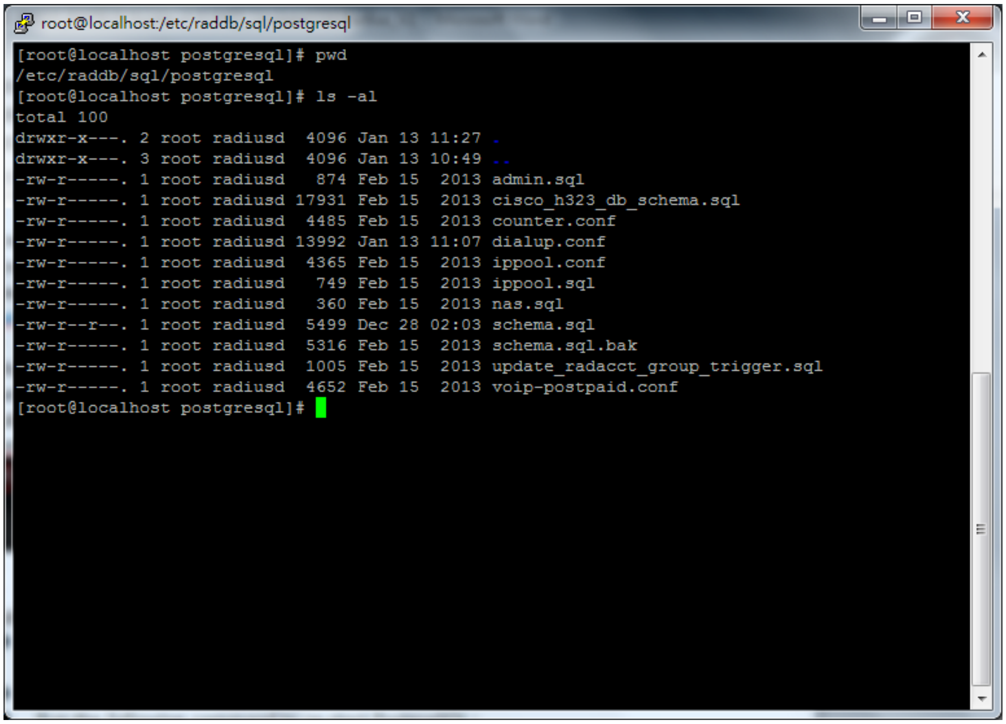
5-2-3. Import FreeRADIUS schemas.

Create a default group and insert a test user into the database. Please copy the schema.sql file which provide by D-Link to replace the existence one under /etc/raddb/sql/postgresql/.

----

cd /etc/raddb/sql/postgresql/

chown root:radius schema.sql



```
[root@localhost postgresql]# pwd
/etc/raddb/sql/postgresql
[root@localhost postgresql]# ls -al
total 100
drwxr-x---. 2 root radiusd  4096 Jan 13 11:27 .
drwxr-x---. 3 root radiusd  4096 Jan 13 10:49 ..
-rw-r-----. 1 root radiusd   874 Feb 15  2013 admin.sql
-rw-r-----. 1 root radiusd 17931 Feb 15  2013 cisco_h323_db_schema.sql
-rw-r-----. 1 root radiusd  4485 Feb 15  2013 counter.conf
-rw-r-----. 1 root radiusd 13992 Jan 13 11:07 dialup.conf
-rw-r-----. 1 root radiusd  4365 Feb 15  2013 ippool.conf
-rw-r-----. 1 root radiusd   749 Feb 15  2013 ippool.sql
-rw-r-----. 1 root radiusd   360 Feb 15  2013 nas.sql
-rw-r--r--. 1 root radiusd  5499 Dec 28 02:03 schema.sql
-rw-r-----. 1 root radiusd  5316 Feb 15  2013 schema.sql.bak
-rw-r-----. 1 root radiusd  1005 Feb 15  2013 update_radacct_group_trigger.sql
-rw-r-----. 1 root radiusd  4652 Feb 15  2013 voip-postpaid.conf
[root@localhost postgresql]#
```

Use the command below to create the table schema for database.

----

sudo cat /etc/raddb/sql/postgresql/schema.sql | psql -U radius radius

----

5-2-4. Set the default attribute to the default group.

Please use commands below to add the 3 default attributes to default group.

The values need to change:

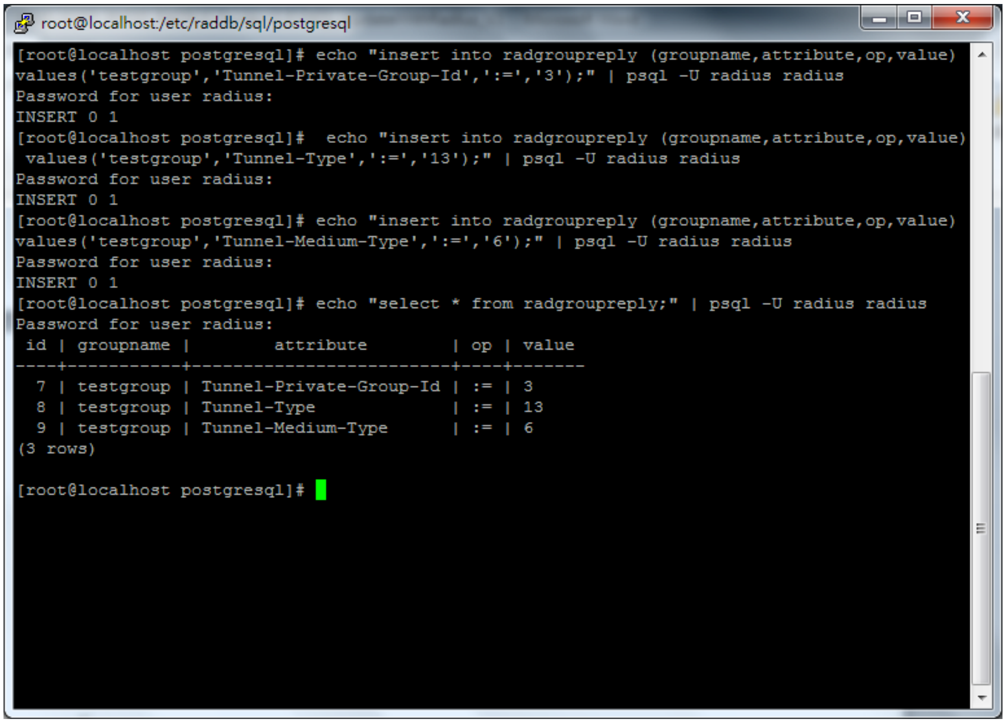
- groupname: Define by user. We can only define one default vlan in the demo scenario.
- default_vlan_id: Define by user. We can only define one default vlan in the demo scenario.

```
---------------------------
echo “insert into radgroupreply (groupname,attribute,op,value) values('groupname','Tunnel-Private-Group-Id',':=','default_vlan_id');” | psql -U radius radius
---------------------------
```

```
---------------------------
echo “insert into radgroupreply (groupname,attribute,op,value) values('groupname',' Tunnel-Type',':=','13');” | psql -U radius radius
---------------------------
```

```
---------------------------
echo “insert into radgroupreply (groupname,attribute,op,value) values('groupname',' Tunnel-Medium-Type',':=','6');” | psql -U radius radius
---------------------------
```

In this case, set the default VLAN as VLAN3. While the authentication information matches username/ password but doesn’t match MAC address, the RADIUS accepts the authentication but assign attribute default VLAN, VLAN3, to this client. The setting information is as below.



```
[root@localhost postgresql]# echo "insert into radgroupreply (groupname,attribute,op,value)
values('testgroup','Tunnel-Private-Group-Id',':=','3');" | psql -U radius radius
Password for user radius:
INSERT 0 1
[root@localhost postgresql]#  echo "insert into radgroupreply (groupname,attribute,op,value)
 values('testgroup','Tunnel-Type',':=','13');" | psql -U radius radius
Password for user radius:
INSERT 0 1
[root@localhost postgresql]# echo "insert into radgroupreply (groupname,attribute,op,value)
values('testgroup','Tunnel-Medium-Type',':=','6');" | psql -U radius radius
Password for user radius:
INSERT 0 1
[root@localhost postgresql]# echo "select * from radgroupreply;" | psql -U radius radius
Password for user radius:
 id | groupname |        attribute        | op | value
----+-----------+-------------------------+----+-------
  7 | testgroup | Tunnel-Private-Group-Id | := | 3
  8 | testgroup | Tunnel-Type             | := | 13
  9 | testgroup | Tunnel-Medium-Type      | := | 6
(3 rows)

[root@localhost postgresql]#
```

5-2-5. Create accounts in the database.

Please use command below to create accounts (username/ password/ MAC address) in database for testing users.

The values need to change:

- Username: Define by user.
- Groupname: Define by user. We can only define one default vlan in the demo scenario.

```
----------------------------
echo “insert into radusergroup (username,groupname,priority)
values('username','groupname','1');” | psql -U radius radius
--------------------------
```

The values need to change:

- Username: Define by user.
- Value: Password for user

```
--------------------------
echo "insert into radcheck (username,attribute,op,value) values ('test','Cleartext-
Password',':=','test');" |psql -U radius radius
--------------------------
```

The values need to change:

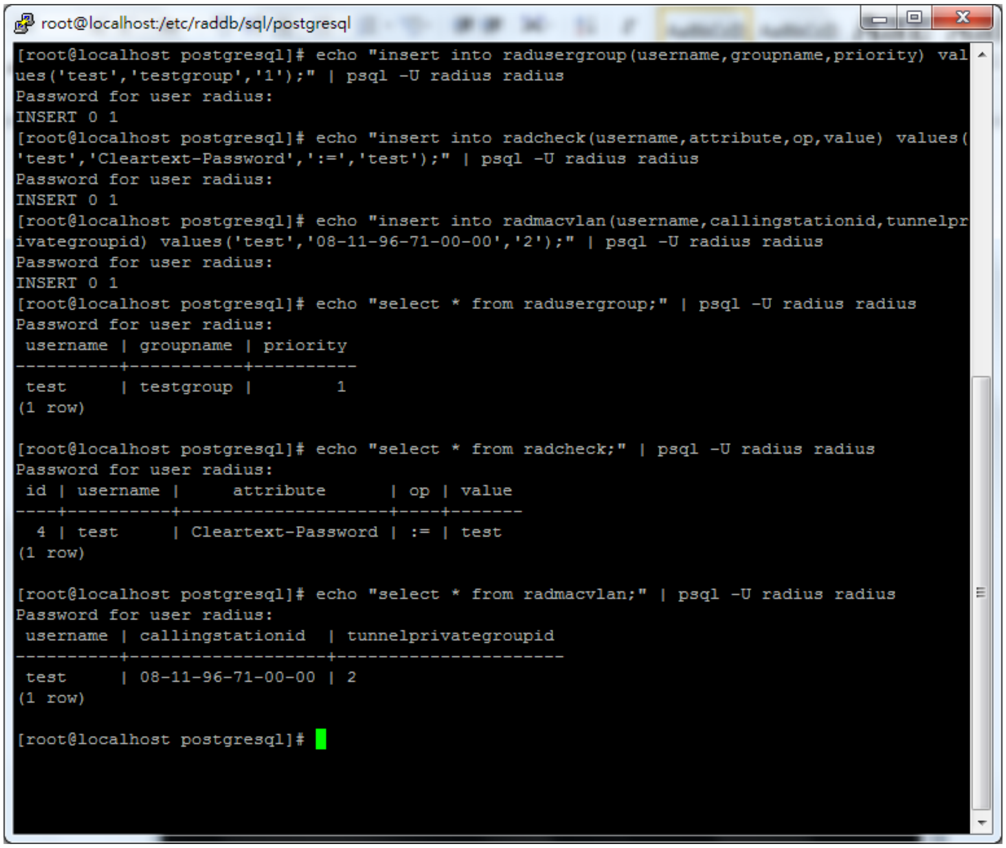
- Username: Define by user.
- Macaddr: MAC address of device
- Vlanid: Define by user

----

echo "insert into radmacvlan (username,callingstationid,tunnelprivategroupid) values('username','macaddr','vlanid');" |psql -U radius radius

----

In this case, set the username/ password are as test/ test. The MAC address is the one of the corporate-provided NB (08:11:96:71:00:00). While three factors are matched, the RADIUS assign attribute VLAN2 to this client. The setting information is as below.



```
[root@localhost postgresql]# echo "insert into radusergroup(username,groupname,priority) val
ues('test','testgroup','1');" | psql -U radius radius
Password for user radius:
INSERT 0 1
[root@localhost postgresql]# echo "insert into radcheck(username,attribute,op,value) values(
'test','Cleartext-Password',':=','test');" | psql -U radius radius
Password for user radius:
INSERT 0 1
[root@localhost postgresql]# echo "insert into radmacvlan(username,callingstationid,tunnelpr
ivategroupid) values('test','08-11-96-71-00-00','2');" | psql -U radius radius
Password for user radius:
INSERT 0 1
[root@localhost postgresql]# echo "select * from radusergroup;" | psql -U radius radius
Password for user radius:
 username | groupname | priority
----------+-----------+----------
 test     | testgroup |        1
(1 row)

[root@localhost postgresql]# echo "select * from radcheck;" | psql -U radius radius
Password for user radius:
 id | username |     attribute      | op | value
----+----------+--------------------+----+-------
  4 | test     | Cleartext-Password | := | test
(1 row)

[root@localhost postgresql]# echo "select * from radmacvlan;" | psql -U radius radius
Password for user radius:
 username | callingstationid  | tunnelprivategroupid
----------+-------------------+----------------------
 test     | 08-11-96-71-00-00 | 2
(1 row)

[root@localhost postgresql]# 
```

6. Stop the firewall process on FreeRadius server

----

service firewalld disable

```
service firewalld stop
--------------------------
```

7. Start FreeRADIUS service

7-1. Enable and start FreeRADIUS sevice

Use the following commands to enable and start FreeRADIUS service

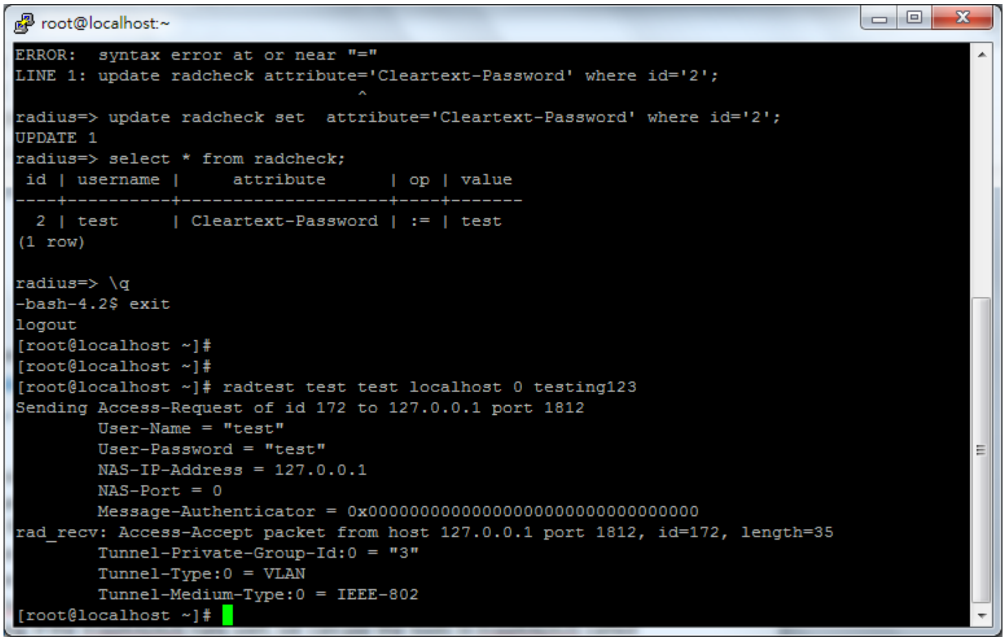
```
--------------------------
service radiusd enable
service radiusd start
--------------------------
```

7-2. Test FreeRADIUS

Use the tool radtest of FreeRADIUS to check if FreeRADIUS run well. The example command is as below.

```
--------------------------
radtest username password radius_ip o shared_secret
--------------------------
```

If the test is passed, it will show Access-Accept as below:



```
ERROR:  syntax error at or near "="
LINE 1: update radcheck attribute='Cleartext-Password' where id='2';
                                 ^
radius=> update radcheck set  attribute='Cleartext-Password' where id='2';
UPDATE 1
radius=> select * from radcheck;
 id | username |     attribute      | op | value
----+----------+--------------------+----+-------
  2 | test     | Cleartext-Password | := | test
(1 row)

radius=> \q
-bash-4.2$ exit
logout
[root@localhost ~]#
[root@localhost ~]#
[root@localhost ~]# radtest test test localhost 0 testing123
Sending Access-Request of id 172 to 127.0.0.1 port 1812
        User-Name = "test"
        User-Password = "test"
        NAS-IP-Address = 127.0.0.1
        NAS-Port = 0
        Message-Authenticator = 0x00000000000000000000000000000000
rad_recv: Access-Accept packet from host 127.0.0.1 port 1812, id=172, length=35
        Tunnel-Private-Group-Id:0 = "3"
        Tunnel-Type:0 = VLAN
        Tunnel-Medium-Type:0 = IEEE-802
[root@localhost ~]#
```

8. Post check after installation with RADIUS client

8-1. Download the FreeRadius client

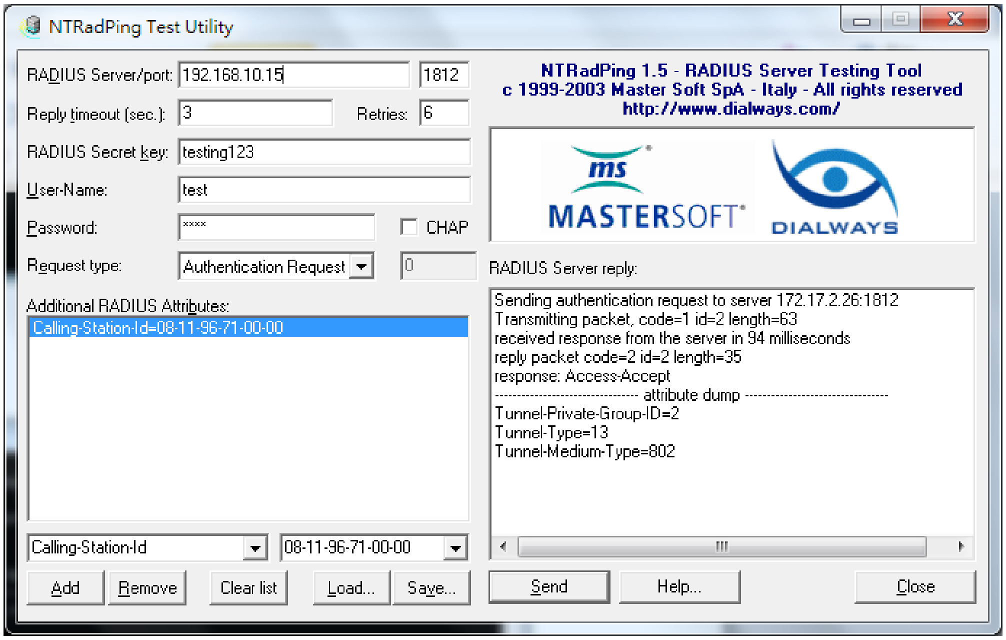
There are many FreeRadius clients can be used for testing. The example in below is using NTRadPing which is downloaded from internet.

7-2. Install the RADIUS client in your laptop which running with Win7.After installed, you can configure RADIUS client through GUI.

Set few parameters when before start testing.

RADIUS Server/port: 192.168.10.15
Port: No need to change, default is 1812.
RADIUS Secret Key: Define by user.
User Name/Password: Define by user.
Additional RADIUS Attributes: Please select Calling-Station-Id in the left and input the MAC Address of your device in the right.

Click Send to send the Authentication Request to the RADIUS server, you can find the reply from RADIUS server in RADIUS Server reply window.



NTRadPing Test Utility

RADIUS Server/port: 192.168.10.15 1812
Reply timeout (sec.): 3 Retries: 6
RADIUS Secret key: testing123
User-Name: test
Password: **** □ CHAP
Request type: Authentication Request 0

Additional RADIUS Attributes:
Calling-Station-Id=08-11-96-71-00-00

Calling-Station-Id 08-11-96-71-00-00

NTRadPing 1.5 - RADIUS Server Testing Tool
c 1999-2003 Master Soft SpA - Italy - All rights reserved
http://www.dialways.com/

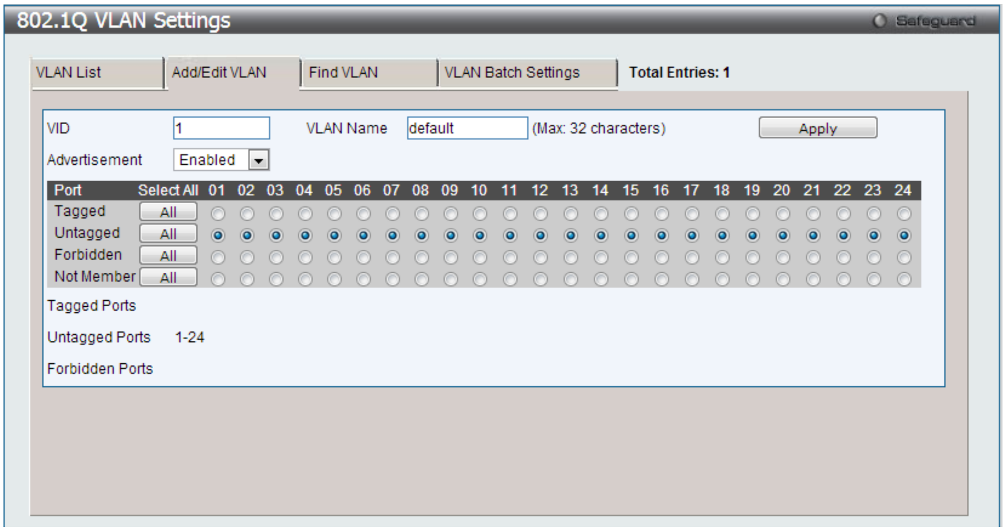
RADIUS Server reply:

```
Sending authentication request to server 172.17.2.26:1812
Transmitting packet, code=1 id=2 length=63
received response from the server in 94 milliseconds
reply packet code=2 id=2 length=35
response: Access-Accept
------------------------- attribute dump ---------------------------
Tunnel-Private-Group-ID=2
Tunnel-Type=13
Tunnel-Medium-Type=802
```

Configuration Steps (DWS-3160)

9. Set up VLAN based on the network architecture. VLAN1 is the default VLAN for AP management. Associate VLAN1 on Port1.

   Navigate to LAN> DWS-3160-24PC> L2 Feature> VLAN> 802.1Q VLAN Settings.



Total Entries: 1

VID 1 VLAN Name default (Max: 32 characters)

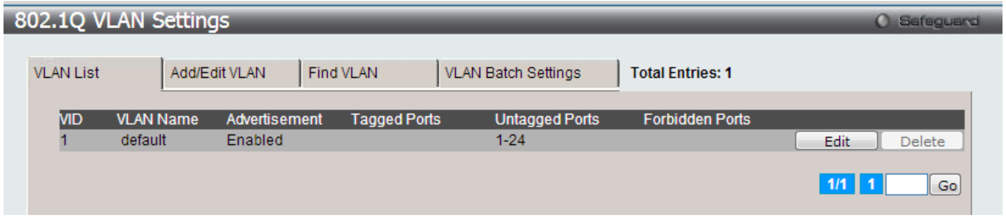
Advertisement Enabled

Port	Select 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
Tagged	All	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Untagged	All	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Forbidden	All	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Not Member	All	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○

Tagged Ports

Untagged Ports 1-24

Forbidden Ports



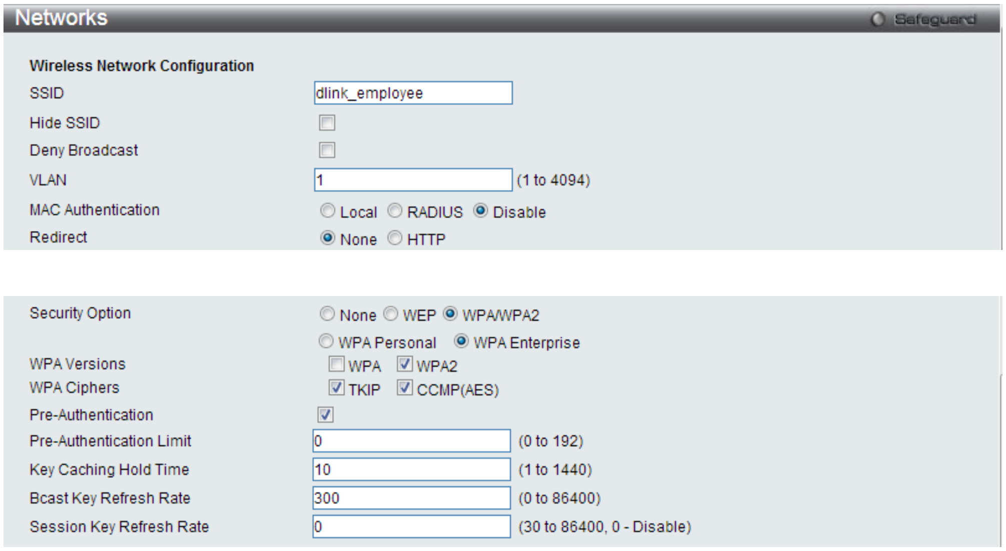
Total Entries: 1

VID	VLAN Name	Advertisement	Tagged Ports	Untagged Ports	Forbidden Ports		
1	default	Enabled		1-24		Edit	Delete

10. Create SSID. Enable security mode WPA2 Enterprise.

    Navigate to WLAN> DWS-3160-24PC> Administration> Advanced Configuration> Networks. Create a SSID. Assign VLAN1 on this SSID. Enable Security WAP/ WAP2. The security detail setting is as below:

    Security: WPA/ WPA2, WPA Enterprise
    WPA Version: WPA2
    WPA Ciphers: TKIP, CCMP (AES)



Wireless Network Configuration

SSID: dlink_employee

Hide SSID: □

Deny Broadcast: □

VLAN: 1 (1 to 4094)

MAC Authentication: ○ Local ○ RADIUS ● Disable

Redirect: ● None ○ HTTP

Security Option: ○ None ○ WEP ● WPA/WPA2

○ WPA Personal ● WPA Enterprise

WPA Versions: □ WPA ☑ WPA2

WPA Ciphers: ☑ TKIP ☑ CCMP(AES)

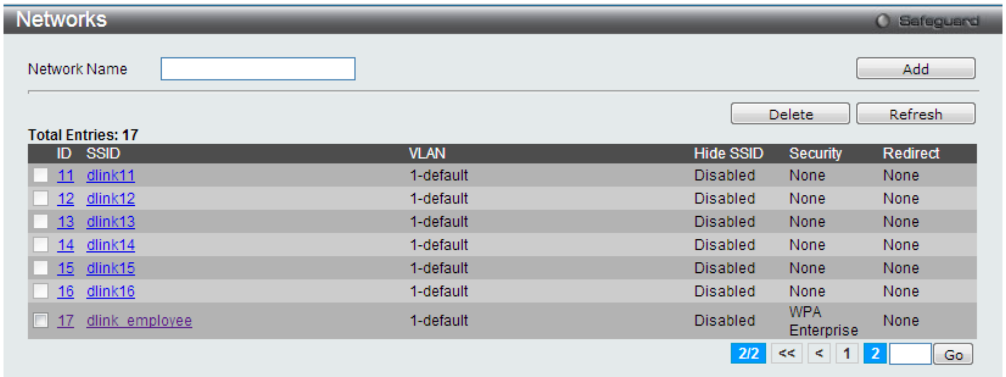
Pre-Authentication: ☑

Pre-Authentication Limit: 0 (0 to 192)

Key Caching Hold Time: 10 (1 to 1440)

Bcast Key Refresh Rate: 300 (0 to 86400)

Session Key Refresh Rate: 0 (30 to 86400, 0 - Disable)

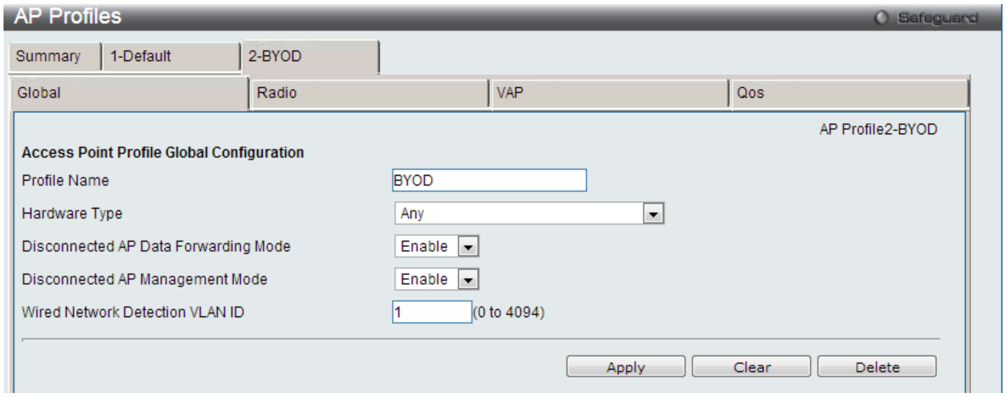


Total Entries: 17

	ID	SSID	VLAN	Hide SSID	Security	Redirect
□	11	dlink11	1-default	Disabled	None	None
□	12	dlink12	1-default	Disabled	None	None
□	13	dlink13	1-default	Disabled	None	None
□	14	dlink14	1-default	Disabled	None	None
□	15	dlink15	1-default	Disabled	None	None
□	16	dlink16	1-default	Disabled	None	None
□	17	dlink_employee	1-default	Disabled	WPA Enterprise	None

11. Create an AP Profile and associate the SSID on it.

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



Access Point Profile Global Configuration

Profile Name: BYOD

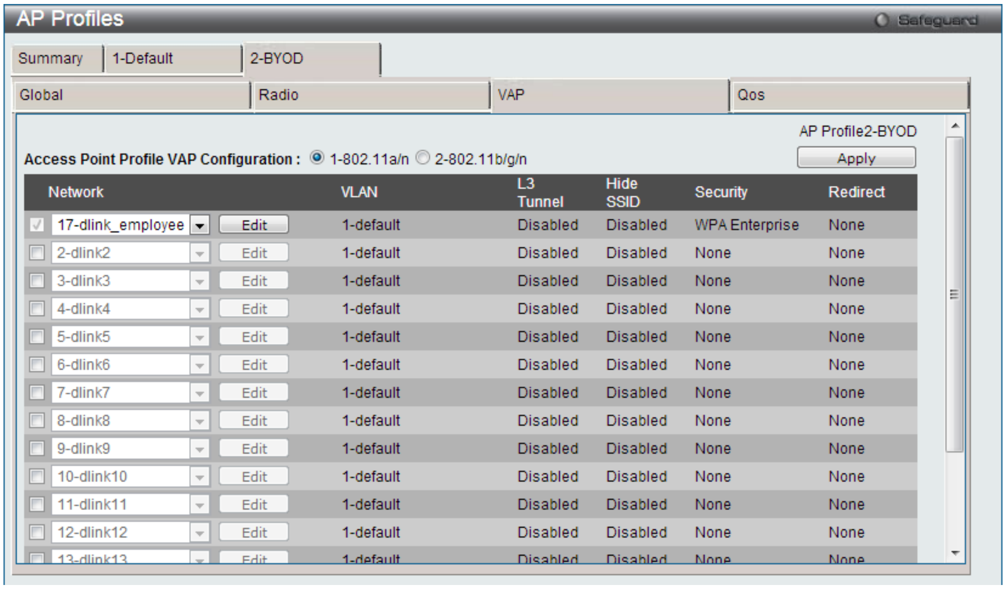
Hardware Type: Any

Disconnected AP Data Forwarding Mode: Enable

Disconnected AP Management Mode: Enable

Wired Network Detection VLAN ID: 1 (0 to 4094)

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



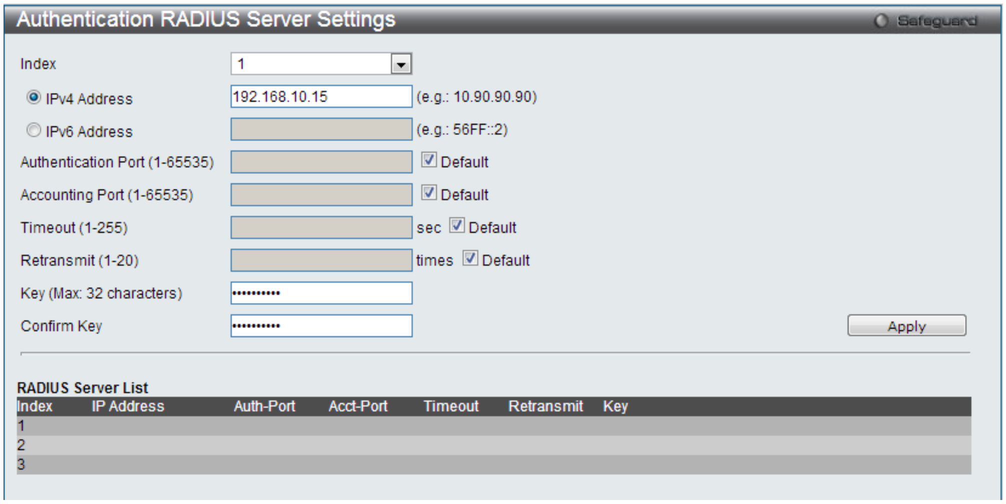
AP Profile2-BYOD

Access Point Profile VAP Configuration : ● 1-802.11a/n ○ 2-802.11b/g/n

	Network		VLAN	L3 Tunnel	Hide SSID	Security	Redirect
☑	17-dlink_employee	Edit	1-default	Disabled	Disabled	WPA Enterprise	None
□	2-dlink2	Edit	1-default	Disabled	Disabled	None	None
□	3-dlink3	Edit	1-default	Disabled	Disabled	None	None
□	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

12. Set RADIUS server.

Fill in RADIUS server IP address, and Key. Navigate to LAN> DWS-3160-24PC> Security> RADIUS> Authentication RADIUS Server Settings.



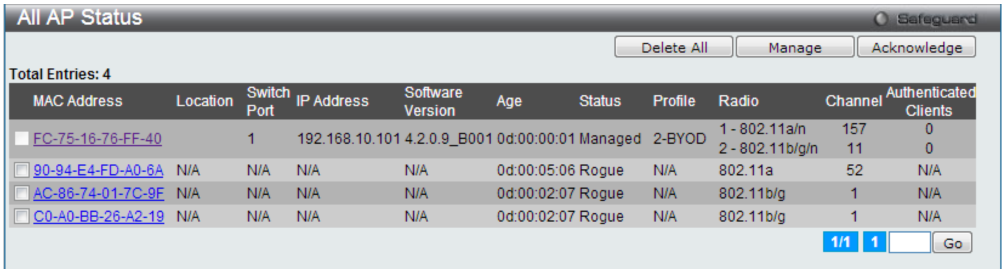
Index	1	
● IPv4 Address	192.168.10.15	(e.g.: 10.90.90.90)
○ IPv6 Address		(e.g.: 56FF::2)
Authentication Port (1-65535)		☑ Default
Accounting Port (1-65535)		☑ Default
Timeout (1-255)		sec ☑ Default
Retransmit (1-20)		times ☑ Default
Key (Max: 32 characters)	••••••••••	
Confirm Key	••••••••••	

RADIUS Server List

Index	IP Address	Auth-Port	Acct-Port	Timeout	Retransmit	Key
1						
2						
3						

13. Discover and manage an AP from the network.

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



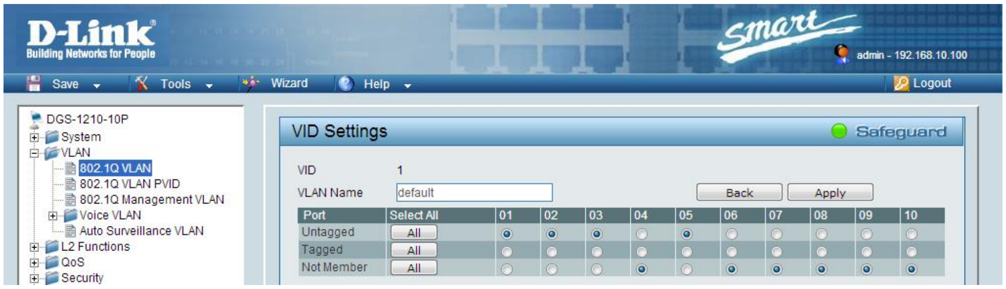
Total Entries: 4

	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
□	90-94-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

Configuration Steps (DGS-1210)

1. Set up VLANs based on the network architecture. Create three VLANs. VLAN1 is the default VLAN for AP management and external RADIUS server, VLAN2 is for the user using corporate-provided NB with full access on internal resources (for example, internet and printer), and VLAN3 is for the user using private NB with limited access (for example, internet). As DWS-3160 VLAN1 is un-tag VLAN, set VLAN1 as un-tag VLAN on switch. The VLAN table is as below.

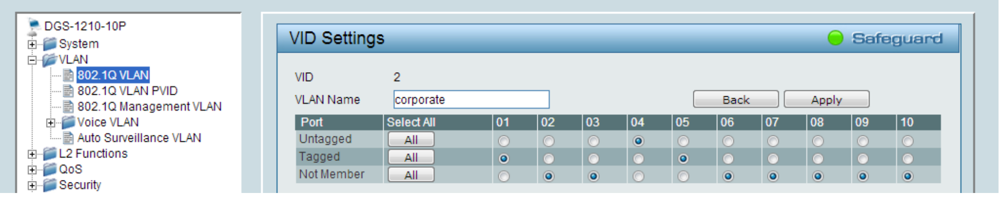
	Port1	Port2	Port3	Port4	Port5
VLAN1	Un-tag	Un-tag	Un-tag	-	Un-tag
VLAN2	Tag	-	-	Un-tag	Tag
VLAN3	Tag	-	-	-	Tag



VID 1

VLAN Name default

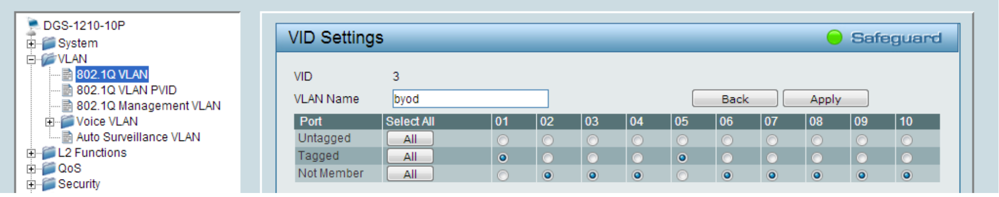
Port	Select All	01	02	03	04	05	06	07	08	09	10
Untagged	All	●	●	●	○	●	○	○	○	○	○
Tagged	All	○	○	○	○	○	○	○	○	○	○
Not Member	All	○	○	○	●	○	●	●	●	●	●



VID 2

VLAN Name corporate

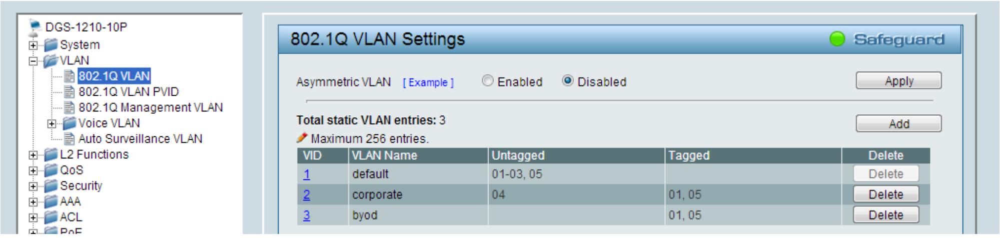
Port	Select All	01	02	03	04	05	06	07	08	09	10
Untagged	All	○	○	○	●	○	○	○	○	○	○
Tagged	All	●	○	○	○	●	○	○	○	○	○
Not Member	All	○	●	●	○	○	●	●	●	●	●



VID 3

VLAN Name byod

Port	Select All	01	02	03	04	05	06	07	08	09	10
Untagged	All	○	○	○	○	○	○	○	○	○	○
Tagged	All	●	○	○	○	●	○	○	○	○	○
Not Member	All	○	●	●	●	○	●	●	●	●	●



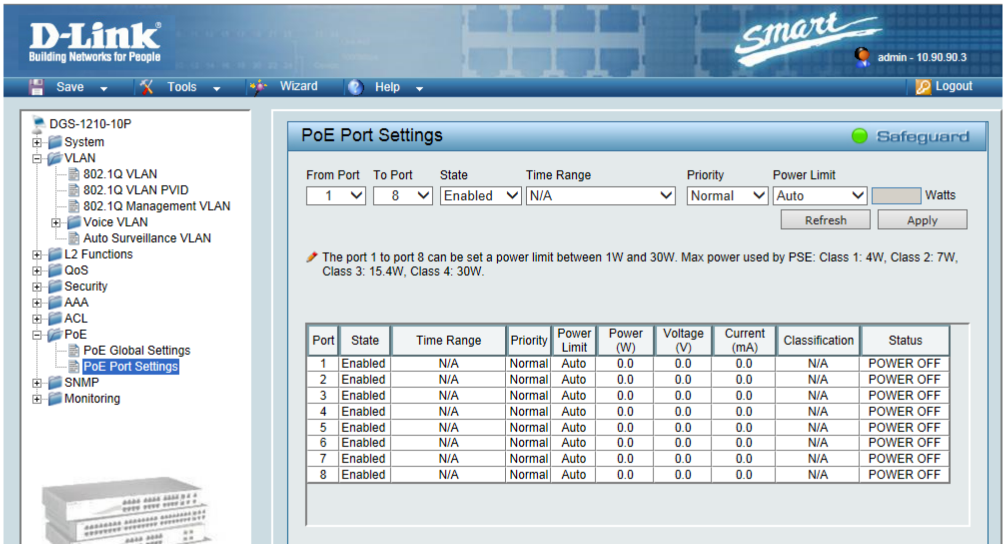
802.1Q VLAN Settings

Asymmetric VLAN [Example] ○ Enabled ● Disabled

Total static VLAN entries: 3
Maximum 256 entries.

VID	VLAN Name	Untagged	Tagged	Delete
1	default	01-03, 05		Delete
2	corporate	04	01, 05	Delete
3	byod		01, 05	Delete

2. (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	To Port	State	Time Range	Priority	Power Limit	
1	8	Enabled	N/A	Normal	Auto	Watts

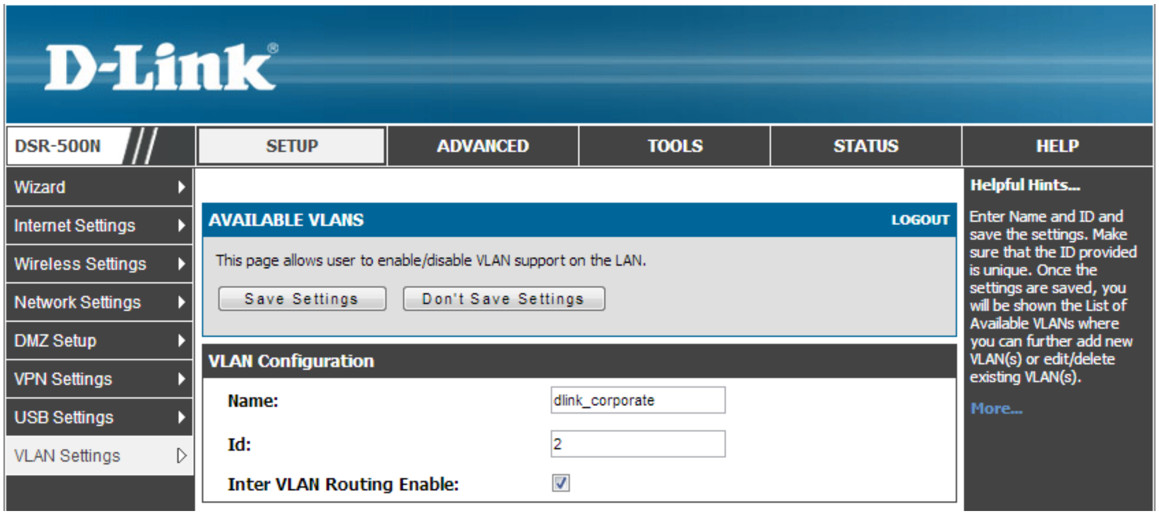
The port 1 to port 8 can be set a power limit between 1W and 30W. Max power used by PSE: Class 1: 4W, Class 2: 7W, Class 3: 15.4W, Class 4: 30W.

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 and external RADIUS server, VLAN2 is for the user using corporate-provided NB with full access on internal resources (for example, internet and printer), and VLAN3 is for the user using private NB with limited access (for example, internet).

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



AVAILABLE VLANS

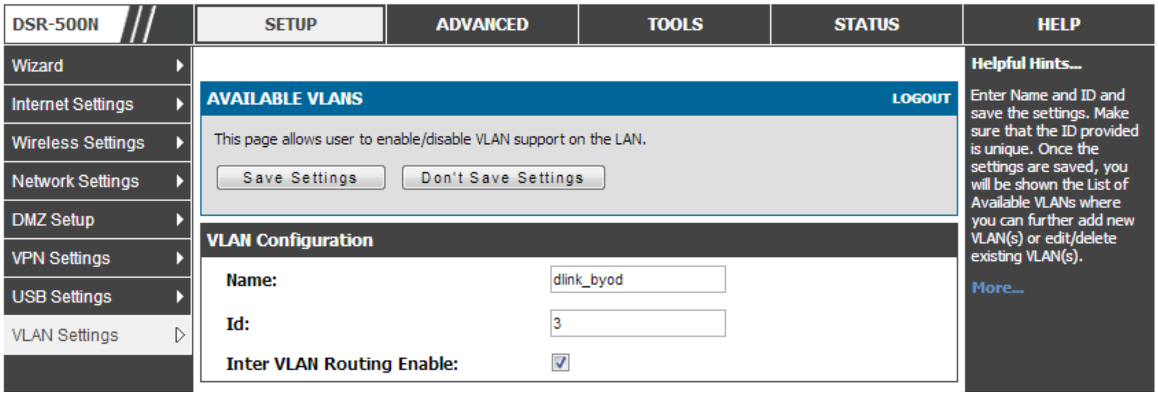
This page allows user to enable/disable VLAN support on the LAN.

VLAN Configuration

Name:	dlink_corporate
Id:	2
Inter VLAN Routing Enable:	☑

Helpful Hints...

Enter Name and ID and save the settings. Make sure that the ID provided is unique. Once the settings are saved, you will be shown the List of Available VLANs where you can further add new VLAN(s) or edit/delete existing VLAN(s).



AVAILABLE VLANS

This page allows user to enable/disable VLAN support on the LAN.

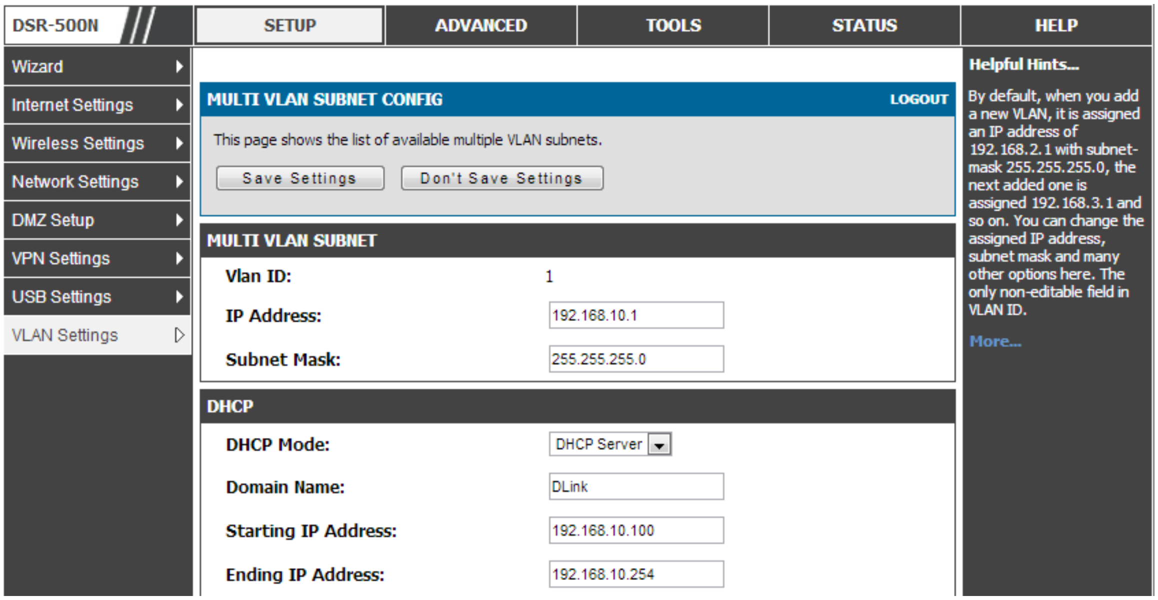
VLAN Configuration

Name:	dlink_byod
Id:	3
Inter VLAN Routing Enable:	☑

Helpful Hints...

Enter Name and ID and save the settings. Make sure that the ID provided is unique. Once the settings are saved, you will be shown the List of Available VLANs where you can further add new VLAN(s) or edit/delete existing VLAN(s).

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



MULTI VLAN SUBNET CONFIG

This page shows the list of available multiple VLAN subnets.

MULTI VLAN SUBNET

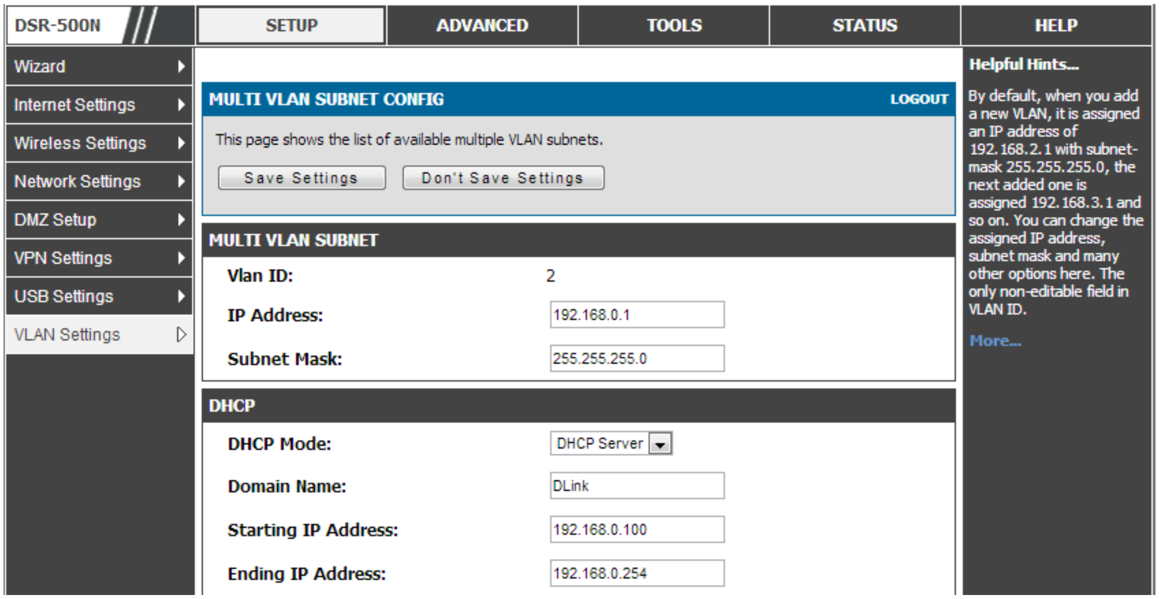
Vlan ID:	1
IP Address:	192.168.10.1
Subnet Mask:	255.255.255.0

DHCP

DHCP Mode:	DHCP Server
Domain Name:	DLink
Starting IP Address:	192.168.10.100
Ending IP Address:	192.168.10.254

Helpful Hints...

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.



MULTI VLAN SUBNET CONFIG

This page shows the list of available multiple VLAN subnets.

MULTI VLAN SUBNET

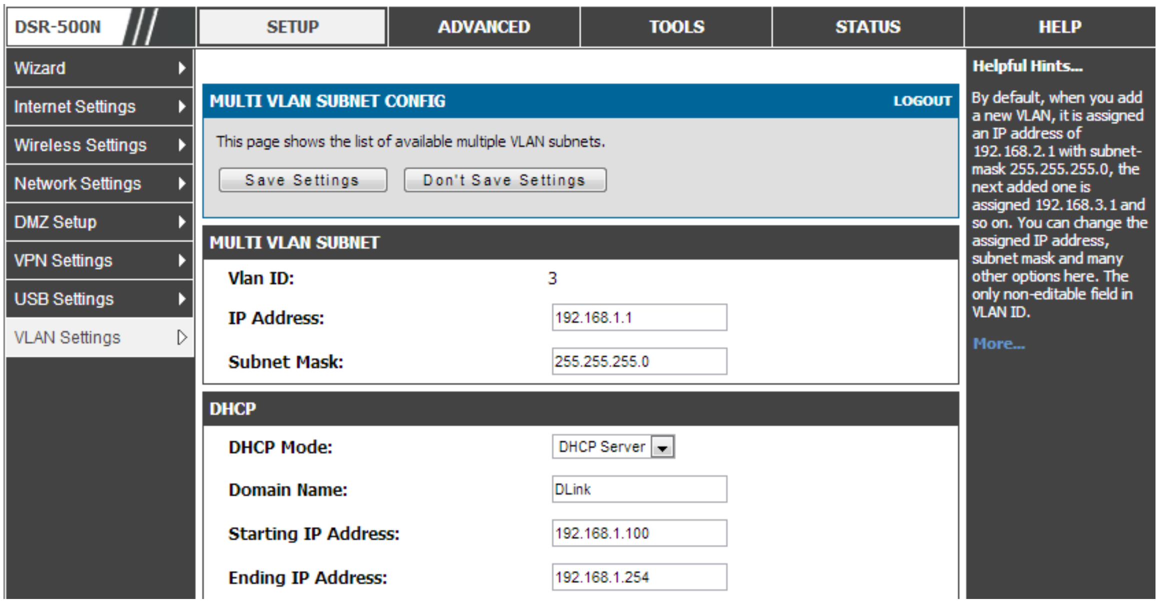
Vlan ID:	2
IP Address:	192.168.0.1
Subnet Mask:	255.255.255.0

DHCP

DHCP Mode:	DHCP Server
Domain Name:	DLink
Starting IP Address:	192.168.0.100
Ending IP Address:	192.168.0.254

Helpful Hints...

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.



MULTI VLAN SUBNET CONFIG

This page shows the list of available multiple VLAN subnets.

MULTI VLAN SUBNET

Vlan ID:	3
IP Address:	192.168.1.1
Subnet Mask:	255.255.255.0

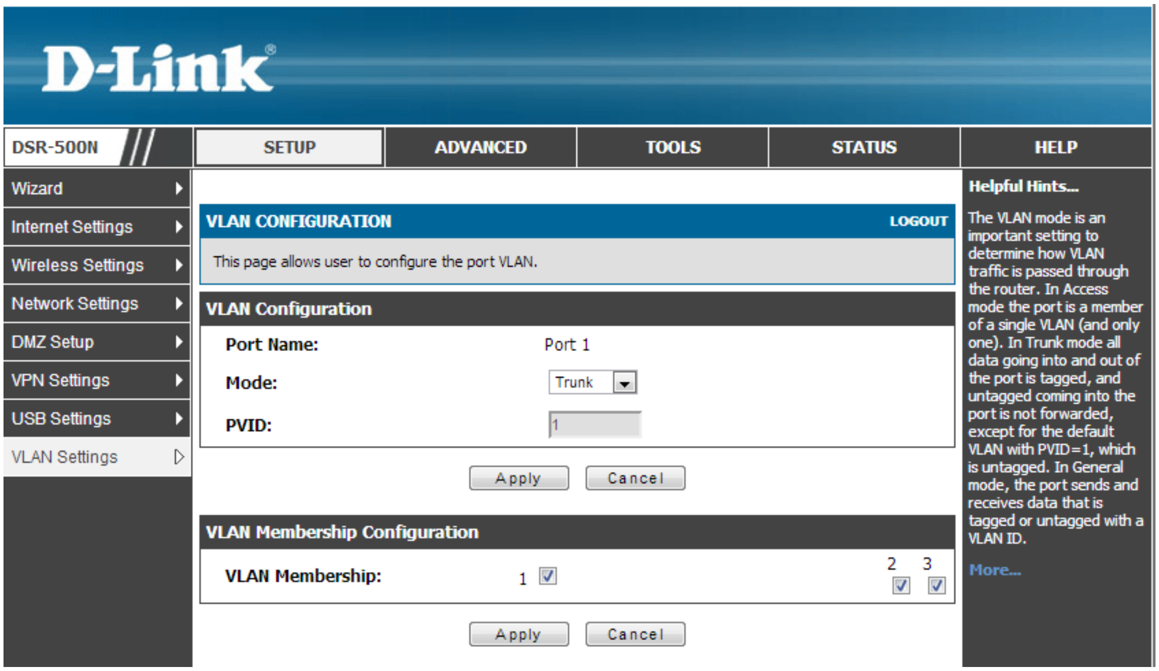
DHCP

DHCP Mode:	DHCP Server
Domain Name:	DLink
Starting IP Address:	192.168.1.100
Ending IP Address:	192.168.1.254

Helpful Hints...

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.

1-3. Associate VLAN1 to 3 in Trunk mode on Port1.



VLAN CONFIGURATION

This page allows user to configure the port VLAN.

VLAN Configuration

Port Name: Port 1

Mode: Trunk

PVID: 1

VLAN Membership Configuration

VLAN Membership: 1 ☑ 2 ☑ 3 ☑

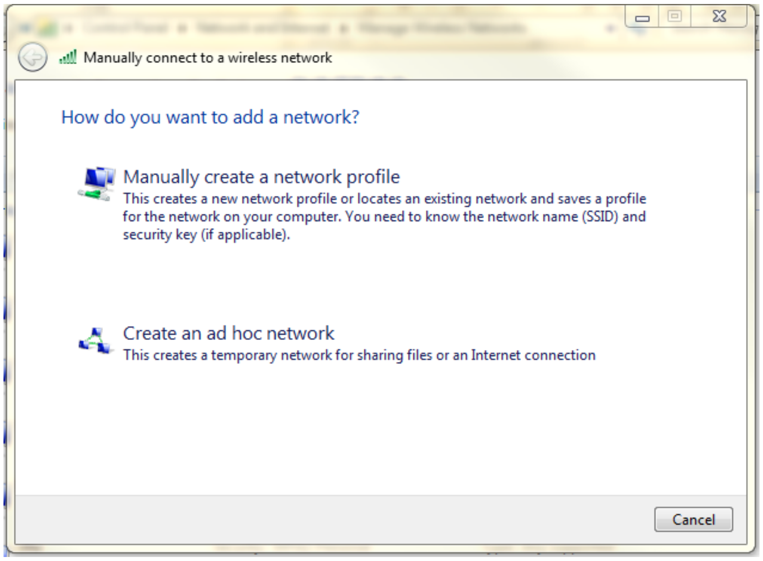
Helpful Hints...

The VLAN mode is an important setting to determine how VLAN traffic is passed through the router. In Access mode the port is a member of a single VLAN (and only one). In Trunk mode all data going into and out of the port is tagged, and untagged coming into the port is not forwarded, except for the default VLAN with PVID=1, which is untagged. In General mode, the port sends and receives data that is tagged or untagged with a VLAN ID.

Configuration Steps (Notebook, Microsoft/ Win7)

1. Set up wireless security.

1-1. Navigate to START> Control Panel> Network and Sharing Center. Click “Manage wireless network”. Click “Add” to add a new wireless network. Select “Manually create a network profile”.

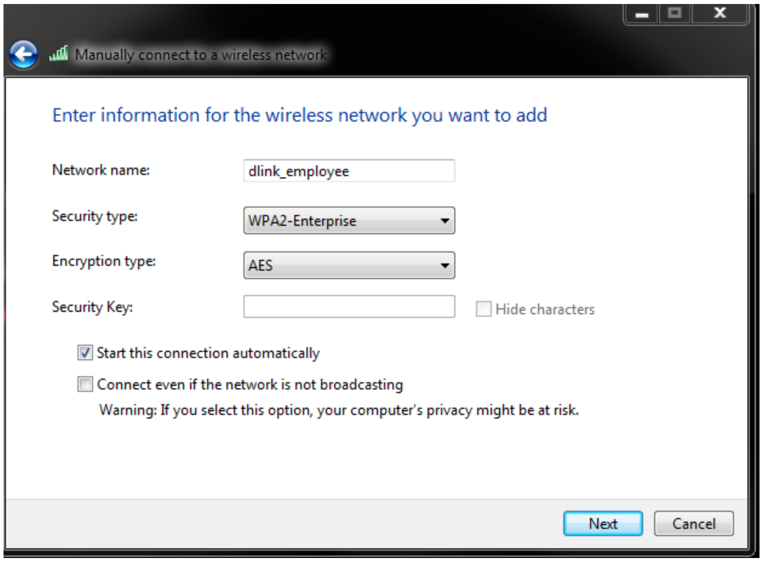


How do you want to add a network?

Manually create a network profile
This creates a new network profile or locates an existing network and saves a profile for the network on your computer. You need to know the network name (SSID) and security key (if applicable).

Create an ad hoc network
This creates a temporary network for sharing files or an Internet connection

1-2. Fill in the network name. Select security type as WPA2-Enterprise. Select the Encryption is AES. Click "Next".



Enter information for the wireless network you want to add

Network name: dlink_employee

Security type: WPA2-Enterprise

Encryption type: AES

Security Key:

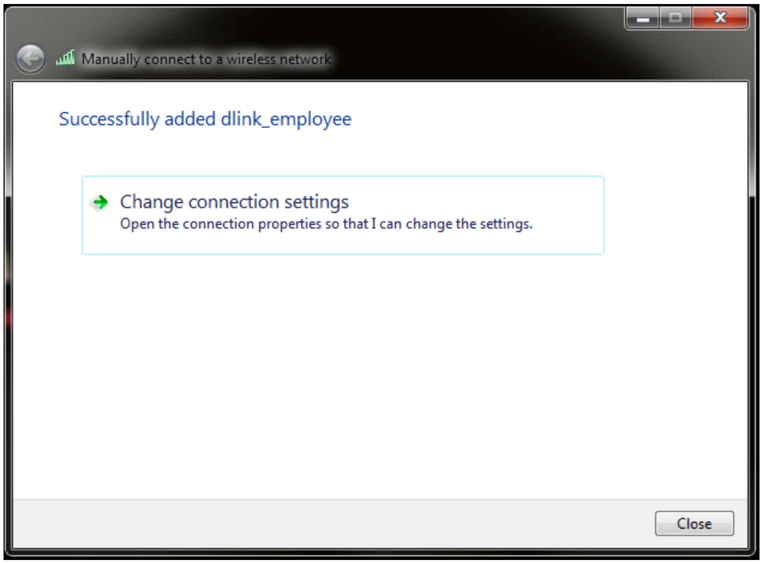
□ Hide characters

☑ Start this connection automatically

□ Connect even if the network is not broadcasting

Warning: If you select this option, your computer's privacy might be at risk.

1-3. Click "Change connection settings".



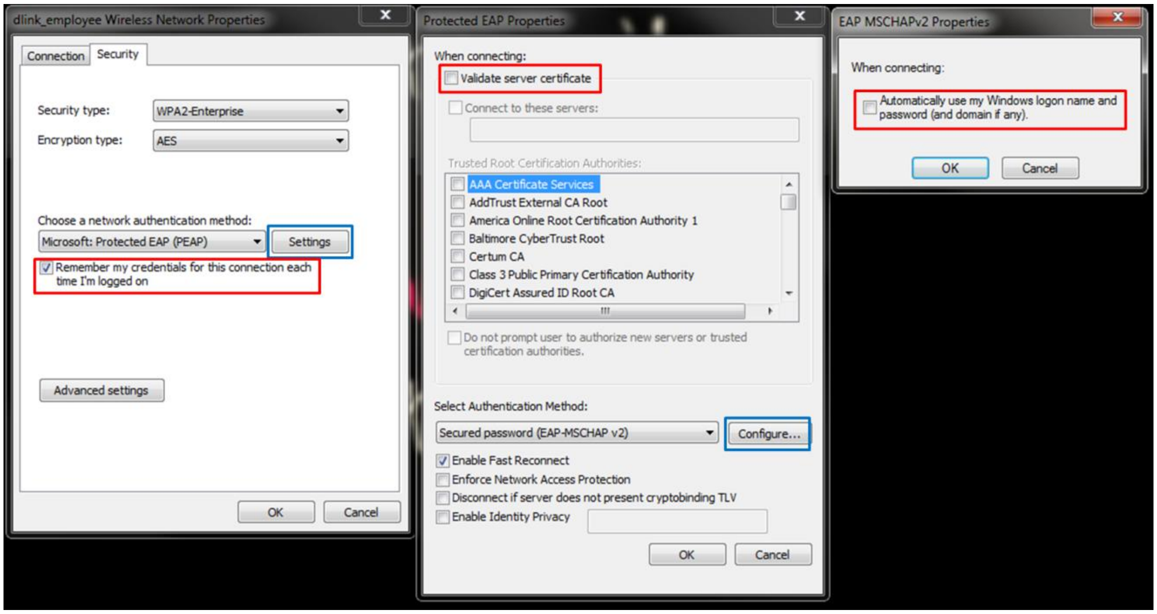
Successfully added dlink_employee

Change connection settings
Open the connection properties so that I can change the settings.

1-3-1. Click tab "Security". (Option) Tick "Remember my credentials for the connection each time I'm logged on" to keep the username/ password information in the computer.

1-3-2. Click "Settings" of "Choose a network authentication method". Un-check "Validate server certification".

1-3-3. Click "Configure.." of Select Authentication Method". (Option) Un-check "Automatically use my Windows logon name and password (and domain if any)" if the username/ password is not the same as Windows logon information.



dlink_employee Wireless Network Properties

Connection | Security

Security type: WPA2-Enterprise

Encryption type: AES

Choose a network authentication method:

Microsoft: Protected EAP (PEAP) | Settings

☑ Remember my credentials for this connection each time I'm logged on

Advanced settings

OK | Cancel

Protected EAP Properties

When connecting:

□ Validate server certificate

□ Connect to these servers:

Trusted Root Certification Authorities:

□ AAA Certificate Services
□ AddTrust External CA Root
□ America Online Root Certification Authority 1
□ Baltimore CyberTrust Root
□ Certum CA
□ Class 3 Public Primary Certification Authority
□ DigiCert Assured ID Root CA

□ Do not prompt user to authorize new servers or trusted certification authorities.

Select Authentication Method:

Secured password (EAP-MSCHAP v2) | Configure...

☑ Enable Fast Reconnect
□ Enforce Network Access Protection
□ Disconnect if server does not present cryptobinding TLV
□ Enable Identity Privacy

OK | Cancel

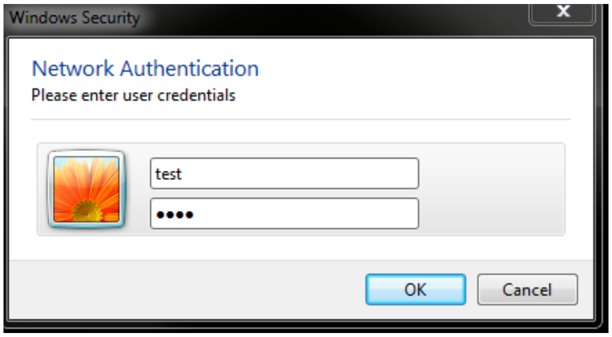
EAP MSCHAPv2 Properties

When connecting:

□ Automatically use my Windows logon name and password (and domain if any).

OK | Cancel

2. Connect the wireless. Insert the username and password.



Windows Security

Network Authentication

Please enter user credentials

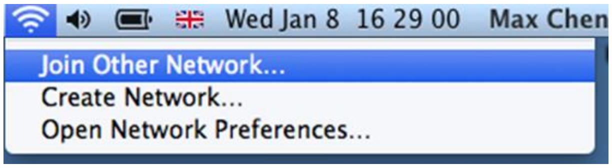
test

••••

OK | Cancel

Configuration Steps (Notebook, Apple/ iOS10)

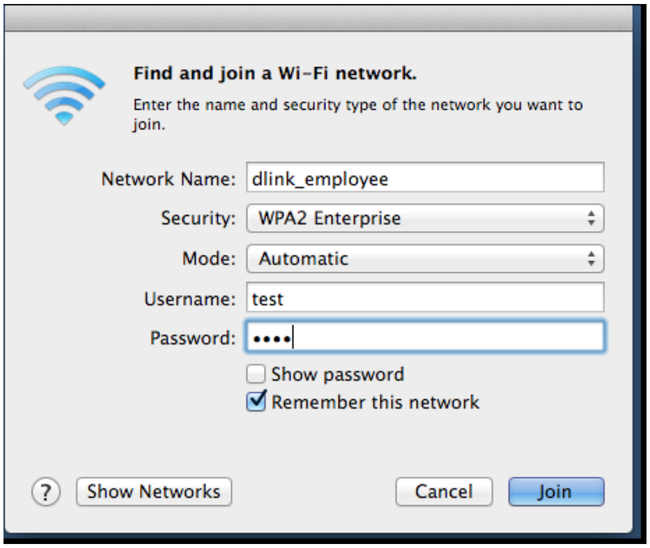
1. Set up wireless security. Click WiFi and select "Join Other Network...".



Wed Jan 8 16 29 00   Max Chen

Join Other Network...
Create Network...
Open Network Preferences...

2. Fill in the network name. Select security type as WPA2-Enterprise. Click “Join”.



Find and join a Wi-Fi network.

Enter the name and security type of the network you want to join.

Network Name: dlink_employee

Security: WPA2 Enterprise

Mode: Automatic

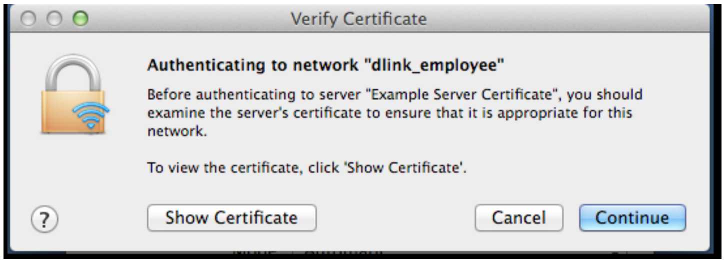
Username: test

Password: ••••

□ Show password

☑ Remember this network

3. Click “Cancel” on Verify Certificate.



Verify Certificate

Authenticating to network "dlink_employee"

Before authenticating to server "Example Server Certificate", you should examine the server's certificate to ensure that it is appropriate for this network.

To view the certificate, click 'Show Certificate'.

Proof of Concept

The NB with MAC 08:11:96:71, which is the corporate-provided device, is assigned VLAN2 after pass the authentication. The NB would get IP address of VLAN2 subnet (for example, 192.168.0.x). It can access resources on VLAN2, for example, printer and internet.

The NB with MAC 00:13:02:69:7F:E9, which is the private device, even use the same username/ password, as the MAC address doesn’t match with the database, it is assigned VLAN3 after pass authentication and get IP address of VLAN3 subnet (for example, 192.168.1.x). It can access resources on VLAN3, for example, internet.

D-Link®

www.dlink.com