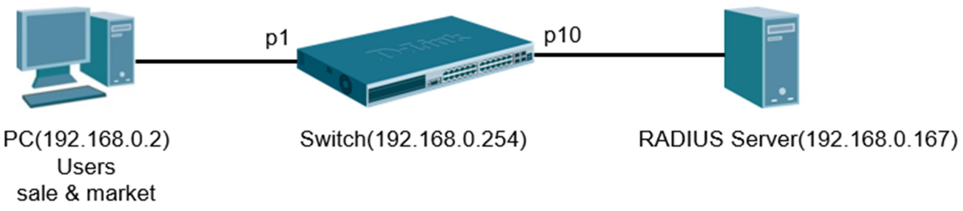
How to use 802.1x Dynamic ACL Assignments on DGS-1510

[Topology]



[Version]

PC (**Ubuntu 14.04.1 x86_64**)

Switch (**DGS-1510 FW v1.40.B24**)

Radius Server (**Ubuntu 12.04_FreeRADIUS v2.1.10**)

[Target]

There are two 802.1x users created in Radius server DB. (sale & market)

Two requirements below:

1) 802.1x user (sale) cannot use ICMP ping to any host, but can execute other actions without problem

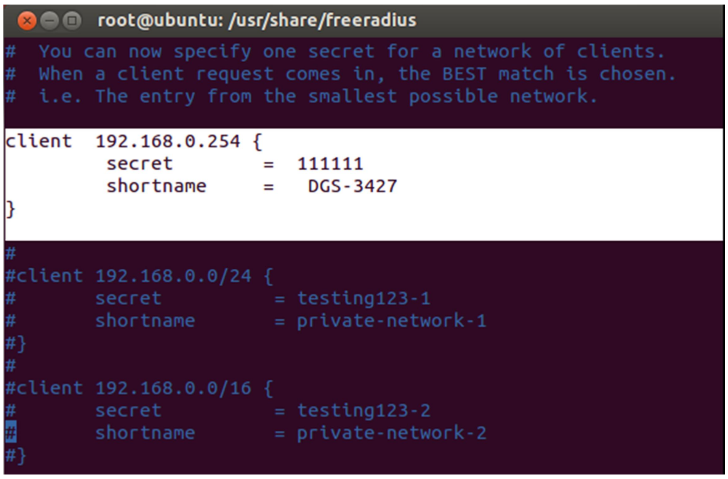
2) 802.1x user (market) cannot use TCP telnet to any host, but can execute other actions without problem.

[Configuration]

#FreeRadius:

1) Setup information of 802.1x users & client.conf on Radius DB.

vim /etc/freeradius/clients.conf



```
#  You can now specify one secret for a network of clients.
#  When a client request comes in, the BEST match is chosen.
#  i.e. The entry from the smallest possible network.

client  192.168.0.254 {
         secret         =  111111
         shortname      =   DGS-3427
}

#
#client 192.168.0.0/24 {
#       secret          = testing123-1
#       shortname       = private-network-1
#}
#
#client 192.168.0.0/16 {
#       secret          = testing123-2
#       shortname       = private-network-2
#}
```

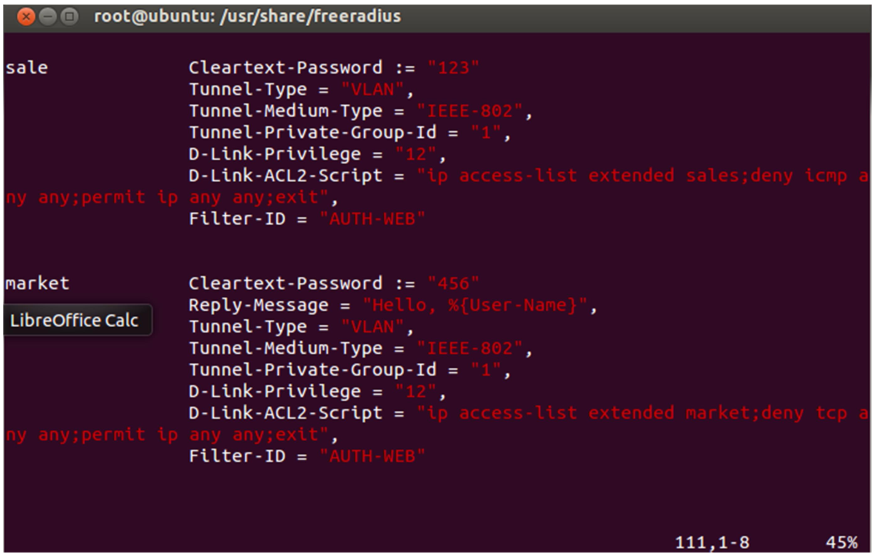
vim /etc/freeradius/users

File:

users

sale's ACL: *"ip access-list extended sales;deny icmp any any;permit ip any any;exit"*

market's ACL: "ip *access-list extended market;deny tcp any any;permit ip any any;exit"*



```
sale            Cleartext-Password := "123"
                Tunnel-Type = "VLAN",
                Tunnel-Medium-Type = "IEEE-802",
                Tunnel-Private-Group-Id = "1",
                D-Link-Privilege = "12",
                D-Link-ACL2-Script = "ip access-list extended sales;deny icmp a
ny any;permit ip any any;exit",
                Filter-ID = "AUTH-WEB"


market          Cleartext-Password := "456"
                Reply-Message = "Hello, %{User-Name}",
                Tunnel-Type = "VLAN",
                Tunnel-Medium-Type = "IEEE-802",
                Tunnel-Private-Group-Id = "1",
                D-Link-Privilege = "12",
                D-Link-ACL2-Script = "ip access-list extended market;deny tcp a
ny any;permit ip any any;exit",
                Filter-ID = "AUTH-WEB"


                                                            111,1-8       45%
```

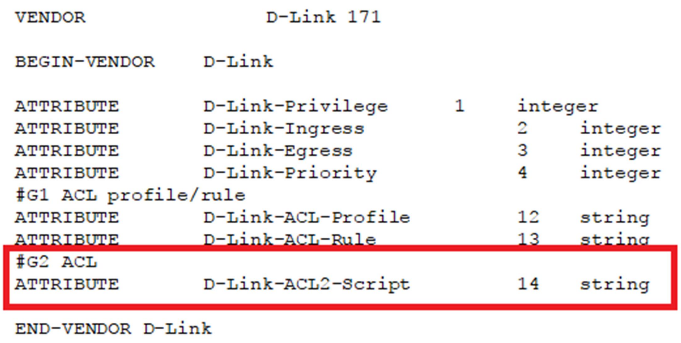
2) Put the below file "dictionary.dlink" under /usr/share/freeradius/. To proclaim vendor code 171 (D-link) and the identify attributes.

File:

dictionary.dlink

cp /home/james/Desktop/dictionary.dlink /usr/share/freeradius/

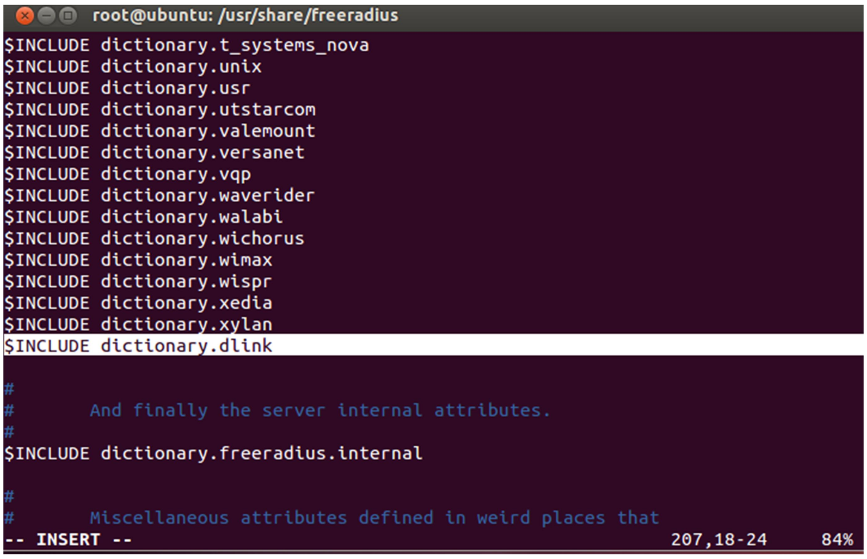
(identify attributes)



```
VENDOR                  D-Link 171

BEGIN-VENDOR     D-Link

ATTRIBUTE        D-Link-Privilege      1     integer
ATTRIBUTE        D-Link-Ingress              2     integer
ATTRIBUTE        D-Link-Egress               3     integer
ATTRIBUTE        D-Link-Priority             4     integer
#G1 ACL profile/rule
ATTRIBUTE        D-Link-ACL-Profile          12    string
ATTRIBUTE        D-Link-ACL-Rule             13    string
#G2 ACL
ATTRIBUTE        D-Link-ACL2-Script          14    string

END-VENDOR D-Link
```

3) Then, go to dictionary and add the below command:

vim /usr/share/freeradius/dictionary



root@ubuntu: /usr/share/freeradius

```
$INCLUDE dictionary.t_systems_nova
$INCLUDE dictionary.unix
$INCLUDE dictionary.usr
$INCLUDE dictionary.utstarcom
$INCLUDE dictionary.valemount
$INCLUDE dictionary.versanet
$INCLUDE dictionary.vqp
$INCLUDE dictionary.waverider
$INCLUDE dictionary.walabi
$INCLUDE dictionary.wichorus
$INCLUDE dictionary.wimax
$INCLUDE dictionary.wispr
$INCLUDE dictionary.xedia
$INCLUDE dictionary.xylan
$INCLUDE dictionary.dlink

#
#       And finally the server internal attributes.
#
$INCLUDE dictionary.freeradius.internal

#
#       Miscellaneous attributes defined in weird places that
-- INSERT --                                              207,18-24      84%
```

Or, you also can refer to the file:

dictionary

4) After finishing, enable Freeradius server on Ubuntu.

freeradius -X

#Switch:

-IP:

```
config t
interface vlan 1
ip address 192.168.0.254 255.255.255.0
exit
```

-802.1xglobal:

```
dot1x system-auth-control
```

-AAA new model:

```
aaa new-model
```

-Radius server:

```
radius-server host 192.168.0.167 key 111111
```

-802.1x port setting:

```
interface ethernet 1/0/1
dot1x pae authenticator
exit
```

-AAA group server assign:

```
aaa group server radius dot1x
server 192.168.0.167
exit
```

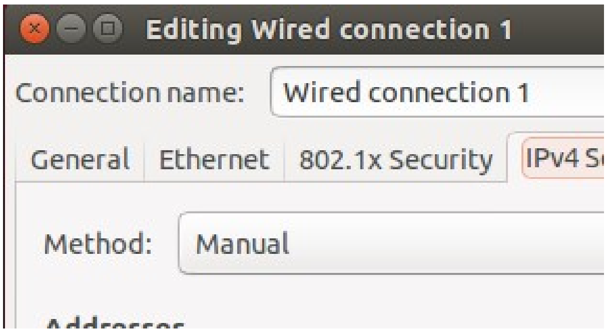
-Network Access Authentication:

```
aaa authentication dot1x default group dot1x
```

[Result]

#802.1x Client:

1) Configure PC’s ip address: 192.168.0.2/24 and Enable 802.1x MD5 authentication

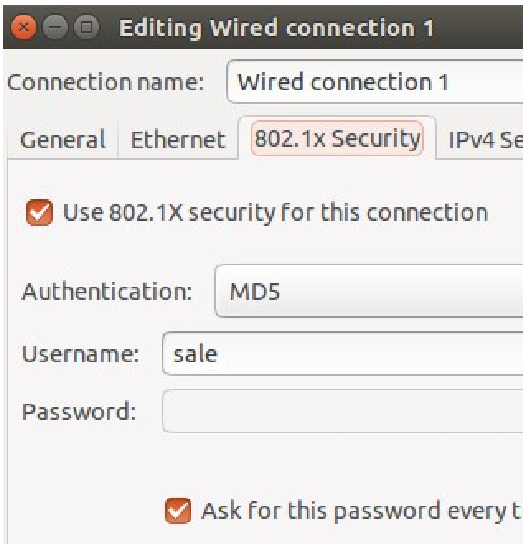


Editing Wired connection 1

Connection name: Wired connection 1

Method: Manual

2) Input username: sale /password:123



Editing Wired connection 1

Connection name: Wired connection 1

☑ Use 802.1X security for this connection

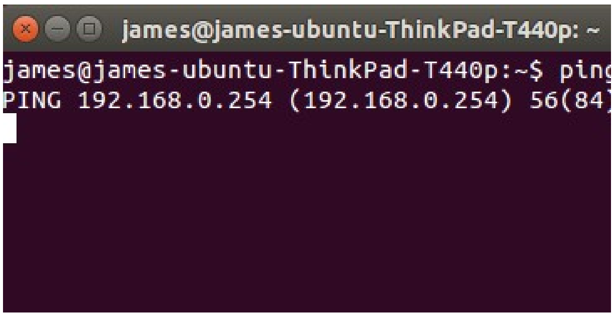
Authentication: MD5

Username: sale

Password:

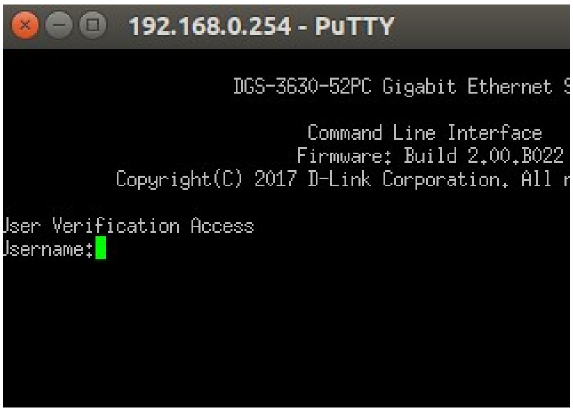
☑ Ask for this password every t

3) After pass authentication, user “sale” cannot ping to switch IP: 192.168.0.254 by ACL assigned from Radius.



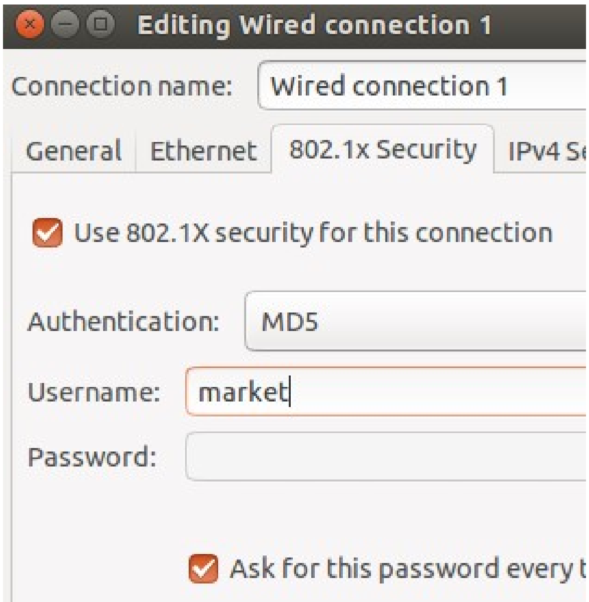
```
james@james-ubuntu-ThinkPad-T440p:~$ ping
PING 192.168.0.254 (192.168.0.254) 56(84)
```

4) After pass authentication, user "sale" can telnet to switch IP: 192.168.0.254 by ACL assigned from Radius.



```
                    DGS-3630-52PC Gigabit Ethernet S

                          Command Line Interface
                         Firmware: Build 2.00.B022
          Copyright(C) 2017 D-Link Corporation. All r

User Verification Access
Username:
```

5) Input username: market /password: 456



Connection name: Wired connection 1

☑ Use 802.1X security for this connection

Authentication: MD5

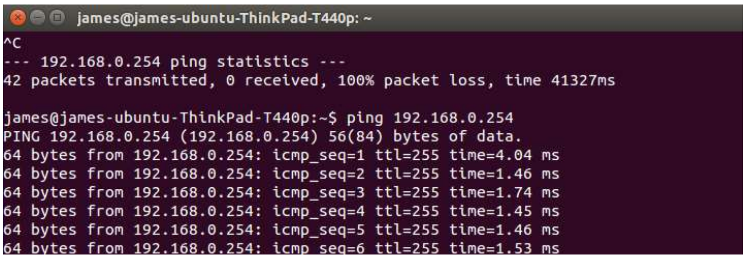
Username: market

Password:

☑ Ask for this password every t

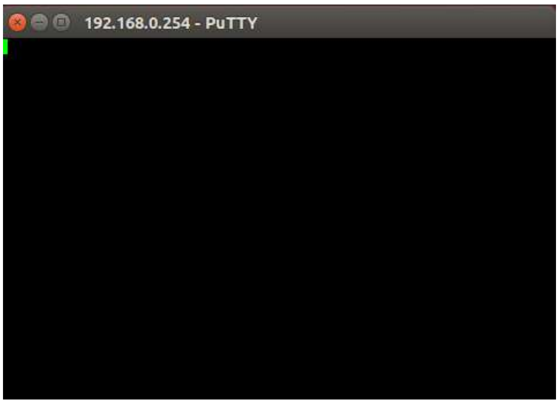
6) After pass authentication, user "market" can ping to switch IP: 192.168.0.254 by ACL

assigned from Radius.



```
james@james-ubuntu-ThinkPad-T440p: ~
^C
--- 192.168.0.254 ping statistics ---
42 packets transmitted, 0 received, 100% packet loss, time 41327ms

james@james-ubuntu-ThinkPad-T440p:~$ ping 192.168.0.254
PING 192.168.0.254 (192.168.0.254) 56(84) bytes of data.
64 bytes from 192.168.0.254: icmp_seq=1 ttl=255 time=4.04 ms
64 bytes from 192.168.0.254: icmp_seq=2 ttl=255 time=1.46 ms
64 bytes from 192.168.0.254: icmp_seq=3 ttl=255 time=1.74 ms
64 bytes from 192.168.0.254: icmp_seq=4 ttl=255 time=1.45 ms
64 bytes from 192.168.0.254: icmp_seq=5 ttl=255 time=1.46 ms
64 bytes from 192.168.0.254: icmp_seq=6 ttl=255 time=1.53 ms
```

7) After pass authentication, user “market” cannot telnet to switch IP: 192.168.0.254 by ACL assigned from Radius.

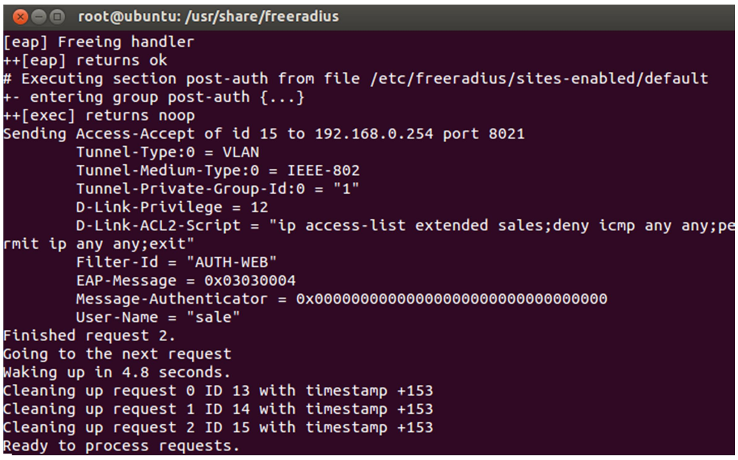


8) Also, you are able to see the log & captured packets information on Radius server:

#user “sale”:

Captured File:

sale.pcapng

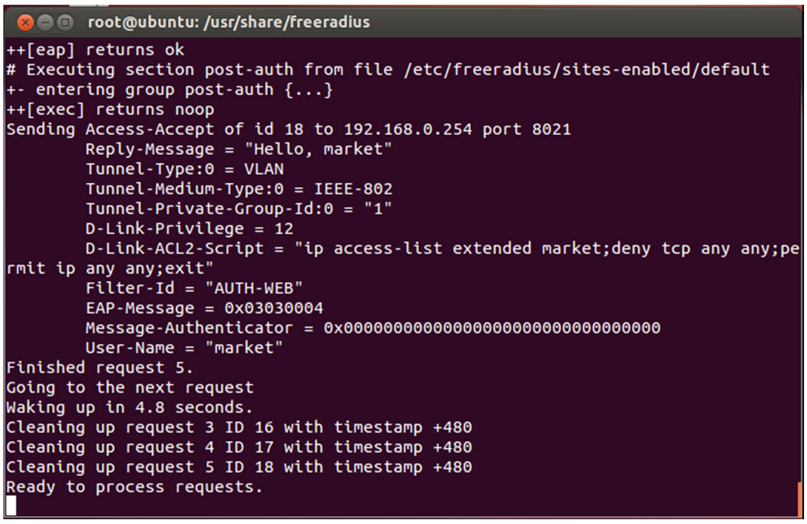


```
root@ubuntu: /usr/share/freeradius
[eap] Freeing handler
++[eap] returns ok
# Executing section post-auth from file /etc/freeradius/sites-enabled/default
+- entering group post-auth {...}
++[exec] returns noop
Sending Access-Accept of id 15 to 192.168.0.254 port 8021
        Tunnel-Type:0 = VLAN
        Tunnel-Medium-Type:0 = IEEE-802
        Tunnel-Private-Group-Id:0 = "1"
        D-Link-Privilege = 12
        D-Link-ACL2-Script = "ip access-list extended sales;deny icmp any any;pe
rmit ip any any;exit"
        Filter-Id = "AUTH-WEB"
        EAP-Message = 0x03030004
        Message-Authenticator = 0x00000000000000000000000000000000
        User-Name = "sale"
Finished request 2.
Going to the next request
Waking up in 4.8 seconds.
Cleaning up request 0 ID 13 with timestamp +153
Cleaning up request 1 ID 14 with timestamp +153
Cleaning up request 2 ID 15 with timestamp +153
Ready to process requests.
```

#user “market”:

Captured File:

market.pcapng



```
++[eap] returns ok
# Executing section post-auth from file /etc/freeradius/sites-enabled/default
+- entering group post-auth {...}
++[exec] returns noop
Sending Access-Accept of id 18 to 192.168.0.254 port 8021
        Reply-Message = "Hello, market"
        Tunnel-Type:0 = VLAN
        Tunnel-Medium-Type:0 = IEEE-802
        Tunnel-Private-Group-Id:0 = "1"
        D-Link-Privilege = 12
        D-Link-ACL2-Script = "ip access-list extended market;deny tcp any any;pe
rmit ip any any;exit"
        Filter-Id = "AUTH-WEB"
        EAP-Message = 0x03030004
        Message-Authenticator = 0x00000000000000000000000000000000
        User-Name = "market"
Finished request 5.
Going to the next request
Waking up in 4.8 seconds.
Cleaning up request 3 ID 16 with timestamp +480
Cleaning up request 4 ID 17 with timestamp +480
Cleaning up request 5 ID 18 with timestamp +480
Ready to process requests.
```