How to test Change of Authorization with FreeRadius

[Topology]

PC---(**p21**)DUT---RADIUS Server

DUT IP is 10.90.90.90

RADIUS is 10.90.90.254

[DUT settings]

#802.1x setting

```
config t
dot1x system-auth-control
aaa new-model
radius-server host 10.90.90.254 key testing123
interface ethernet 1/0/21
dot1x pae authenticator
exit
aaa group server radius dot1x
server 10.90.90.254
exit
aaa authentication dot1x default group dot1x
```

#COA setting

```
aaa server radius dynamic-author
client 10.90.90.254 server-key testing123
port 3799
exit
no authentication command bounce-port ignore
no authentication command disable-port ignore
```

[Test Procedure]

#CoA Test

Before Test, we need to understand the below behavior about COA design. “disable-host-port” & “bounce-host-port”

RADIUS CoA is used to change client authorizations in the following use cases:

Session termination with port shutdown---port linkdown, to block host

The RADIUS server CoA disable port command administratively shuts down the authentication port that is hosting a session, resulting in session termination. This command is useful when a host is known to cause problems on the network and network access needs to be immediately blocked for the host. To restore network access on the port, re-enable it using a non-RADIUS mechanism.

This command is carried in a standard CoA-Request message that has this new vendor-specific attribute (VSA):

Dlink-AV-Pair = disable-host-port

Session termination with port bounce--port lindown/up,to let device get ip address again.

When a CoA message is used to change the VLAN for an authenticated host, end devices such as printers do not have a mechanism to detect the VLAN change, so they do not renew the lease for their DHCP address in the new VLAN. The port bounce feature can be used to force the end device to initiate DHCP re-negotiation by causing a link flap on the authenticated port.

The port is bounced if the following VSA attribute-value pair is received in the CoA message from the RADIUS server:

Dlink-AV-Pair = bounce-host-port

#TEST by “disable-host-port”

1) On Ubuntu Radius Server, we need to add the below attribute in the dictionary. dlink

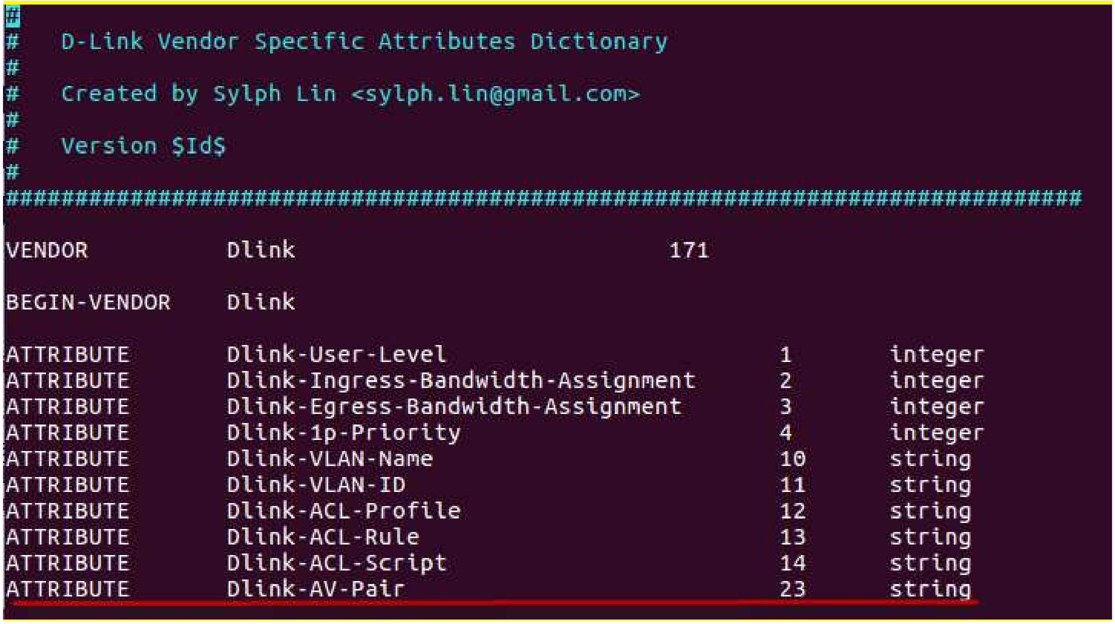
   Dictionary.dlink

   Attribute Name: Dlink-AV-Pair

   Vendor type : 23

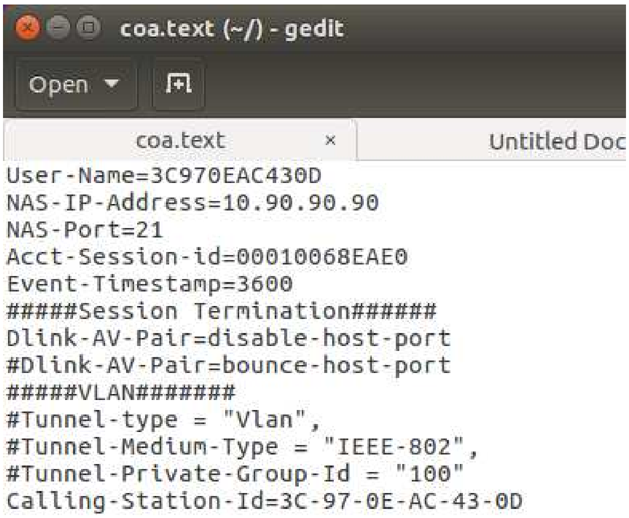
   Type:String

   =>vim /usr/share/freeradius/dictionary.dlink



```
#
#   D-Link Vendor Specific Attributes Dictionary
#
#   Created by Sylph Lin <sylph.lin@gmail.com>
#
#   Version $Id$
#
##############################################################################

VENDOR          Dlink                           171

BEGIN-VENDOR    Dlink

ATTRIBUTE       Dlink-User-Level                        1       integer
ATTRIBUTE       Dlink-Ingress-Bandwidth-Assignment      2       integer
ATTRIBUTE       Dlink-Egress-Bandwidth-Assignment       3       integer
ATTRIBUTE       Dlink-1p-Priority                       4       integer
ATTRIBUTE       Dlink-VLAN-Name                         10      string
ATTRIBUTE       Dlink-VLAN-ID                           11      string
ATTRIBUTE       Dlink-ACL-Profile                       12      string
ATTRIBUTE       Dlink-ACL-Rule                          13      string
ATTRIBUTE       Dlink-ACL-Script                        14      string
ATTRIBUTE       Dlink-AV-Pair                           23      string
```

2) Create a text file, Ex: coa.txt (Note: Attribute value should base on your test enviroment, and base on what attribute you used)



```
User-Name=3C970EAC430D
NAS-IP-Address=10.90.90.90
NAS-Port=21
Acct-Session-id=00010068EAE0
Event-Timestamp=3600
#####Session Termination######
Dlink-AV-Pair=disable-host-port
#Dlink-AV-Pair=bounce-host-port
#####VLAN#######
#Tunnel-type = "Vlan",
#Tunnel-Medium-Type = "IEEE-802",
#Tunnel-Private-Group-Id = "100"
Calling-Station-Id=3C-97-0E-AC-43-0D
```

Note:

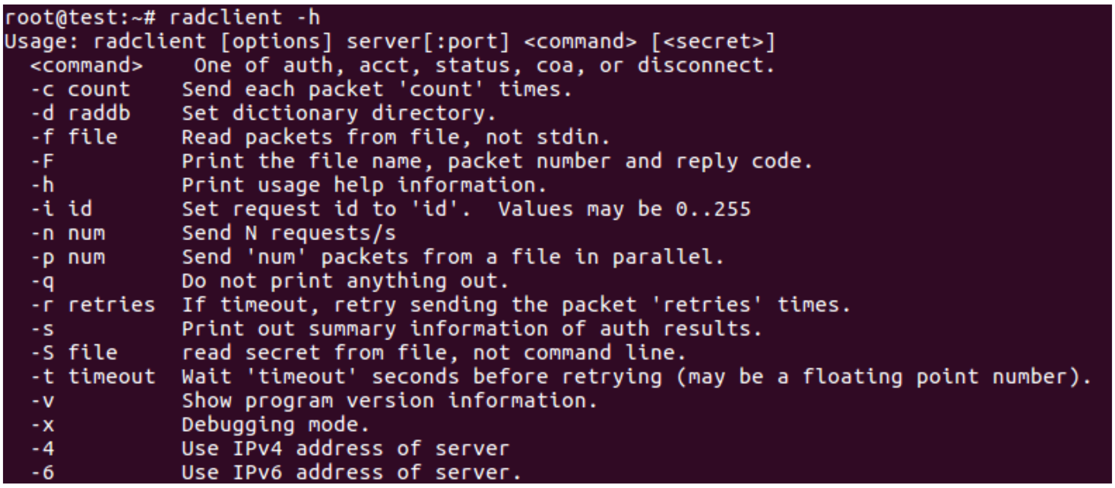
1) **Acct-Session-id should base on host session ID of user's real enviroment. On DUT , we can also use command "show authentication session" to check host session ID**
2) **Uncomment the "diable-host-port" means that switch will diable authenticated host's port number when Administrator issue the command on Radius Server**

3) Copy this coa.text to /usr/bin , Ex:

```
cd Desktop
cp coa.txt /usr/bin
```

4) Use "radclient" command to simulate CoA Request.

   We can firstly use "radclient –h" to check possible order

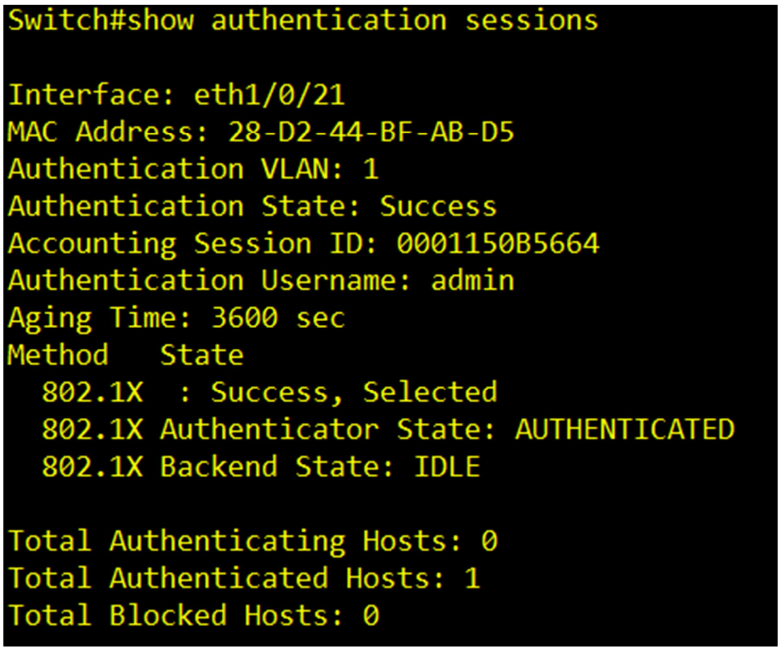


```
root@test:~# radclient -h
Usage: radclient [options] server[:port] <command> [<secret>]
  <command>    One of auth, acct, status, coa, or disconnect.
  -c count     Send each packet 'count' times.
  -d raddb     Set dictionary directory.
  -f file      Read packets from file, not stdin.
  -F           Print the file name, packet number and reply code.
  -h           Print usage help information.
  -i id        Set request id to 'id'.  Values may be 0..255
  -n num       Send N requests/s
  -p num       Send 'num' packets from a file in parallel.
  -q           Do not print anything out.
  -r retries   If timeout, retry sending the packet 'retries' times.
  -s           Print out summary information of auth results.
  -S file      read secret from file, not command line.
  -t timeout   Wait 'timeout' seconds before retrying (may be a floating point number).
  -v           Show program version information.
  -x           Debugging mode.
  -4           Use IPv4 address of server
  -6           Use IPv6 address of server.
```

5) Take below enviroment for example.

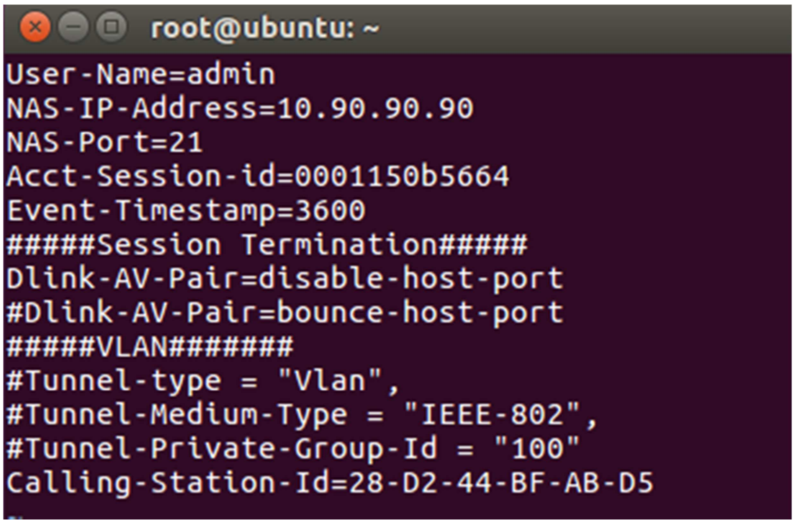
##Suppose that PC already passed 802.1x auth on port 21##

a. Check **accouting session id** by “show authen session” command on switch

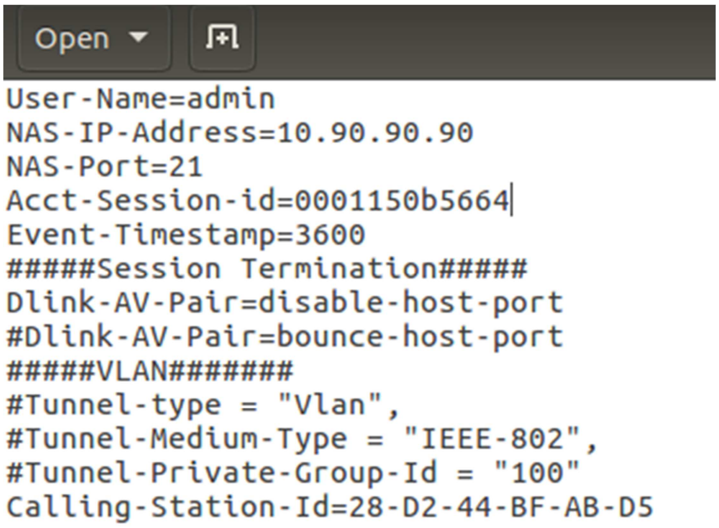


```
Switch#show authentication sessions

Interface: eth1/0/21
MAC Address: 28-D2-44-BF-AB-D5
Authentication VLAN: 1
Authentication State: Success
Accounting Session ID: 0001150B5664
Authentication Username: admin
Aging Time: 3600 sec
Method   State
  802.1X  : Success, Selected
  802.1X Authenticator State: AUTHENTICATED
  802.1X Backend State: IDLE

Total Authenticating Hosts: 0
Total Authenticated Hosts: 1
Total Blocked Hosts: 0
```

b. Modify the acct-session-id on coa.txt file on /home/james/Desktop/coa.txt & /usr/bin usr/ coa.txt to make the acct-session-id match with current session.
And, uncomment “disable-host-port”

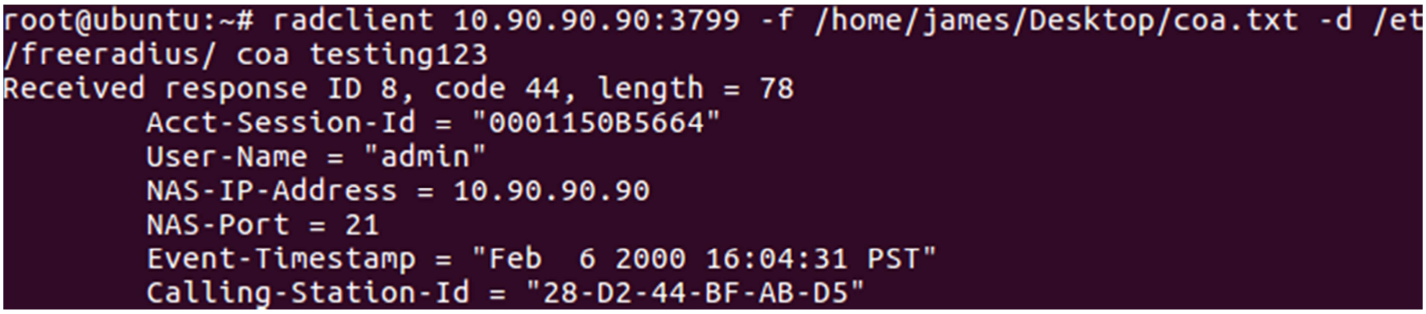


```
User-Name=admin
NAS-IP-Address=10.90.90.90
NAS-Port=21
Acct-Session-id=0001150b5664
Event-Timestamp=3600
#####Session Termination#####
Dlink-AV-Pair=disable-host-port
#Dlink-AV-Pair=bounce-host-port
#####VLAN#######
#Tunnel-type = "Vlan",
#Tunnel-Medium-Type = "IEEE-802",
#Tunnel-Private-Group-Id = "100"
Calling-Station-Id=28-D2-44-BF-AB-D5
```



```
User-Name=admin
NAS-IP-Address=10.90.90.90
NAS-Port=21
Acct-Session-id=0001150b5664
Event-Timestamp=3600
#####Session Termination#####
Dlink-AV-Pair=disable-host-port
#Dlink-AV-Pair=bounce-host-port
#####VLAN#######
#Tunnel-type = "Vlan",
#Tunnel-Medium-Type = "IEEE-802",
#Tunnel-Private-Group-Id = "100"
Calling-Station-Id=28-D2-44-BF-AB-D5
```

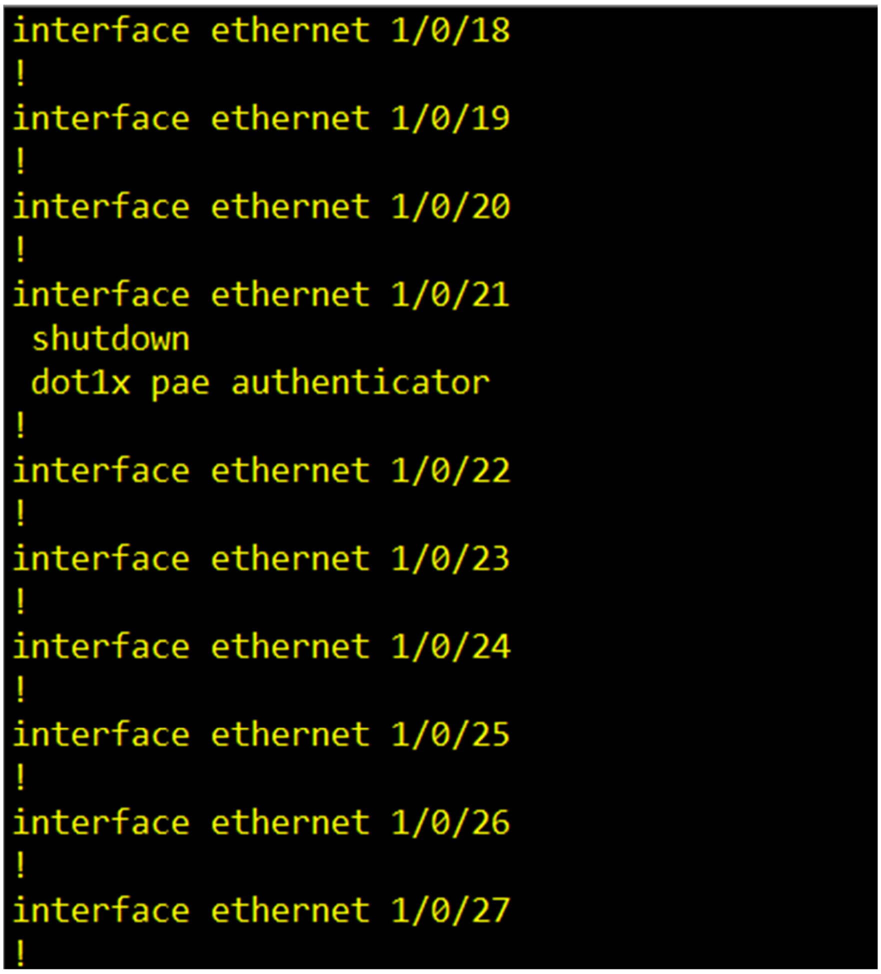
c. If Administrator expect RADIUS sending **CoA-Request** , please use below command
radclient 10.90.90.90:3799 -f /home/james/Desktop/coa.txt -d /etc/freeradius/ **coa** **testing123**



```
root@ubuntu:~# radclient 10.90.90.90:3799 -f /home/james/Desktop/coa.txt -d /et
/freeradius/ coa testing123
Received response ID 8, code 44, length = 78
        Acct-Session-Id = "0001150B5664"
        User-Name = "admin"
        NAS-IP-Address = 10.90.90.90
        NAS-Port = 21
        Event-Timestamp = "Feb  6 2000 16:04:31 PST"
        Calling-Station-Id = "28-D2-44-BF-AB-D5"
```

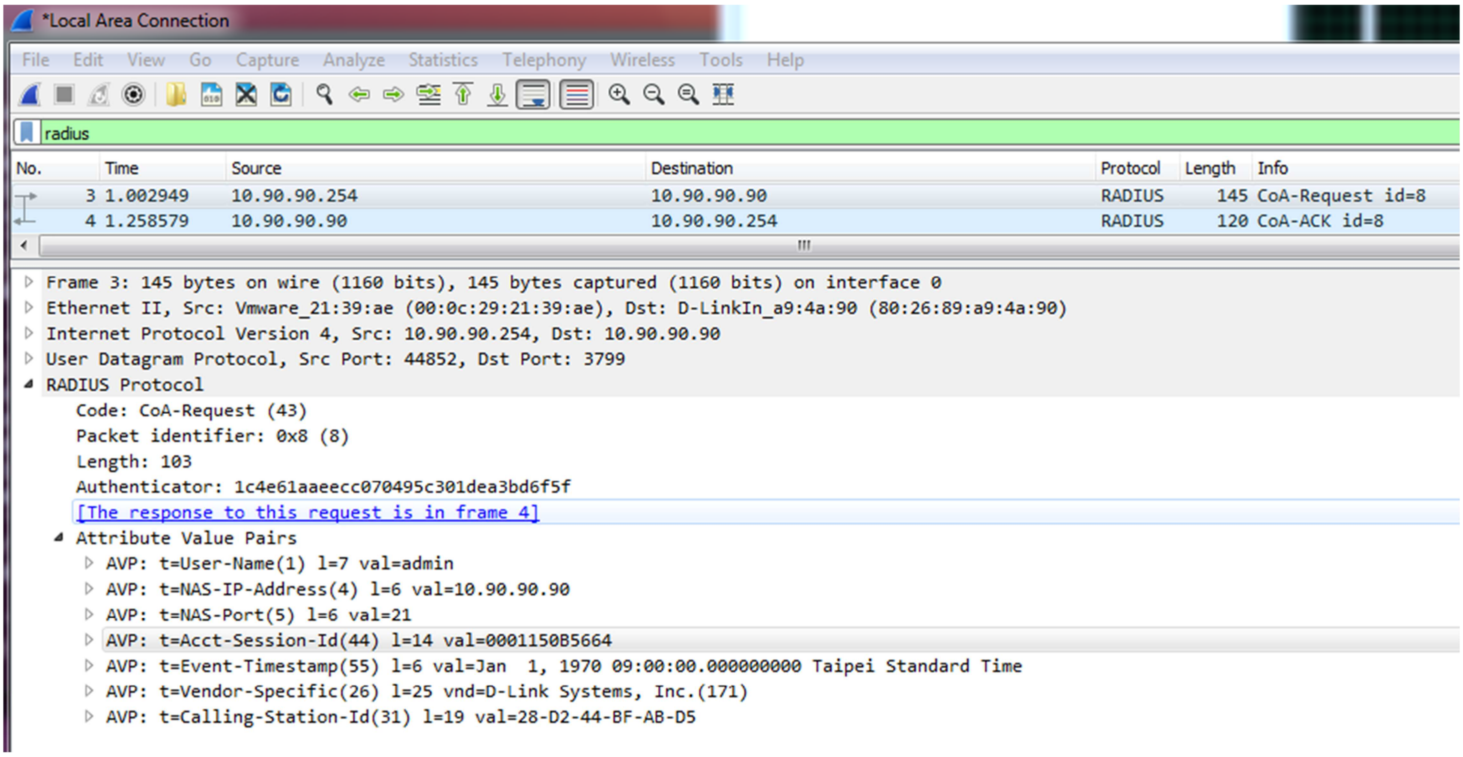
NOTE: You should check the complete output as above screenshot.

d. Then, check running-config file of switch, you will see the port21 is admin-shutdowned by switch since it is triggered by “diable-host port” of COA.



```
interface ethernet 1/0/18
!
interface ethernet 1/0/19
!
interface ethernet 1/0/20
!
interface ethernet 1/0/21
 shutdown
 dot1x pae authenticator
!
interface ethernet 1/0/22
!
interface ethernet 1/0/23
!
interface ethernet 1/0/24
!
interface ethernet 1/0/25
!
interface ethernet 1/0/26
!
interface ethernet 1/0/27
!
```

e. Attached is captured packet file, CoA request from Radius Server will tag the vendor attribute of D-Link



*Local Area Connection
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
radius

```
No.   Time       Source                Destination            Protocol  Length  Info
    3 1.002949   10.90.90.254          10.90.90.90            RADIUS      145 CoA-Request id=8
    4 1.258579   10.90.90.90           10.90.90.254           RADIUS      120 CoA-ACK id=8
```

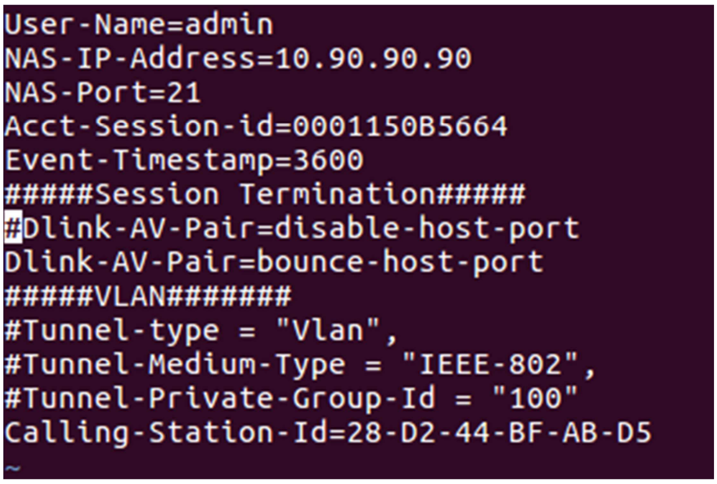
```
▷ Frame 3: 145 bytes on wire (1160 bits), 145 bytes captured (1160 bits) on interface 0
▷ Ethernet II, Src: Vmware_21:39:ae (00:0c:29:21:39:ae), Dst: D-LinkIn_a9:4a:90 (80:26:89:a9:4a:90)
▷ Internet Protocol Version 4, Src: 10.90.90.254, Dst: 10.90.90.90
▷ User Datagram Protocol, Src Port: 44852, Dst Port: 3799
◢ RADIUS Protocol
    Code: CoA-Request (43)
    Packet identifier: 0x8 (8)
    Length: 103
    Authenticator: 1c4e61aaeecc070495c301dea3bd6f5f
    [The response to this request is in frame 4]
  ◢ Attribute Value Pairs
    ▷ AVP: t=User-Name(1) l=7 val=admin
    ▷ AVP: t=NAS-IP-Address(4) l=6 val=10.90.90.90
    ▷ AVP: t=NAS-Port(5) l=6 val=21
    ▷ AVP: t=Acct-Session-Id(44) l=14 val=0001150B5664
    ▷ AVP: t=Event-Timestamp(55) l=6 val=Jan  1, 1970 09:00:00.000000000 Taipei Standard Time
    ▷ AVP: t=Vendor-Specific(26) l=25 vnd=D-Link Systems, Inc.(171)
    ▷ AVP: t=Calling-Station-Id(31) l=19 val=28-D2-44-BF-AB-D5
```

COA_disable port.pcapng

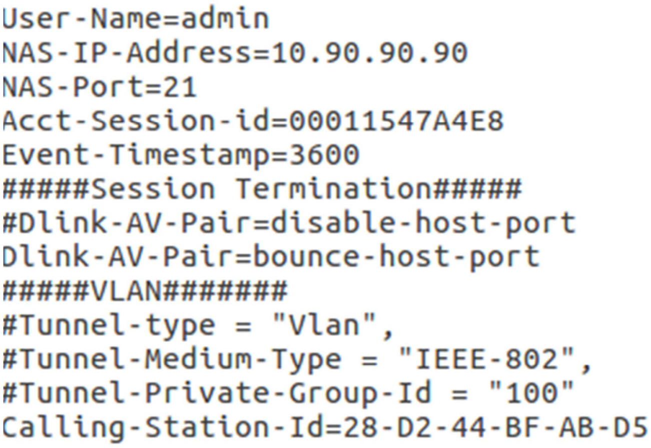
#TEST by “bounce-host-port ”

a. Modify the acct-session-id on coa.txt file on /home/james/Desktop/coa.txt & /usr/bin usr/ coa.txt to make the acct-session-id match with current session.

   NOTE: Uncomment “bounce-host-port”



```
User-Name=admin
NAS-IP-Address=10.90.90.90
NAS-Port=21
Acct-Session-id=0001150B5664
Event-Timestamp=3600
#####Session Termination#####
#Dlink-AV-Pair=disable-host-port
Dlink-AV-Pair=bounce-host-port
#####VLAN#######
#Tunnel-type = "Vlan",
#Tunnel-Medium-Type = "IEEE-802",
#Tunnel-Private-Group-Id = "100"
Calling-Station-Id=28-D2-44-BF-AB-D5
~
```



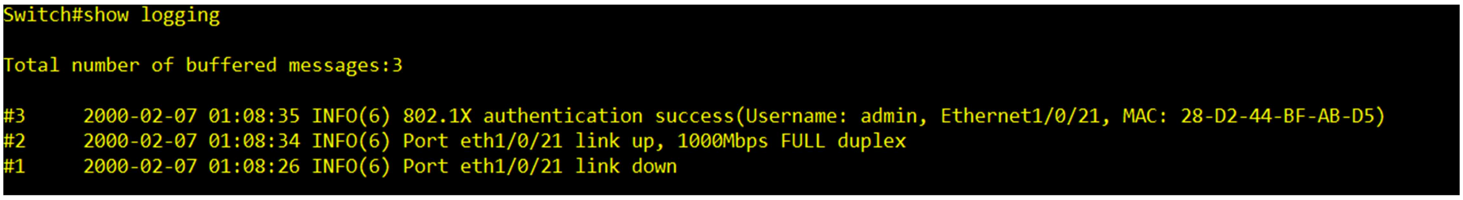
```
User-Name=admin
NAS-IP-Address=10.90.90.90
NAS-Port=21
Acct-Session-id=00011547A4E8
Event-Timestamp=3600
#####Session Termination#####
#Dlink-AV-Pair=disable-host-port
Dlink-AV-Pair=bounce-host-port
#####VLAN#######
#Tunnel-type = "Vlan",
#Tunnel-Medium-Type = "IEEE-802",
#Tunnel-Private-Group-Id = "100"
Calling-Station-Id=28-D2-44-BF-AB-D5
```

b. ##Suppose that PC already passed 802.1x auth on port 21##

   If Administrator expect RADIUS sending **CoA-Request** , please use below command

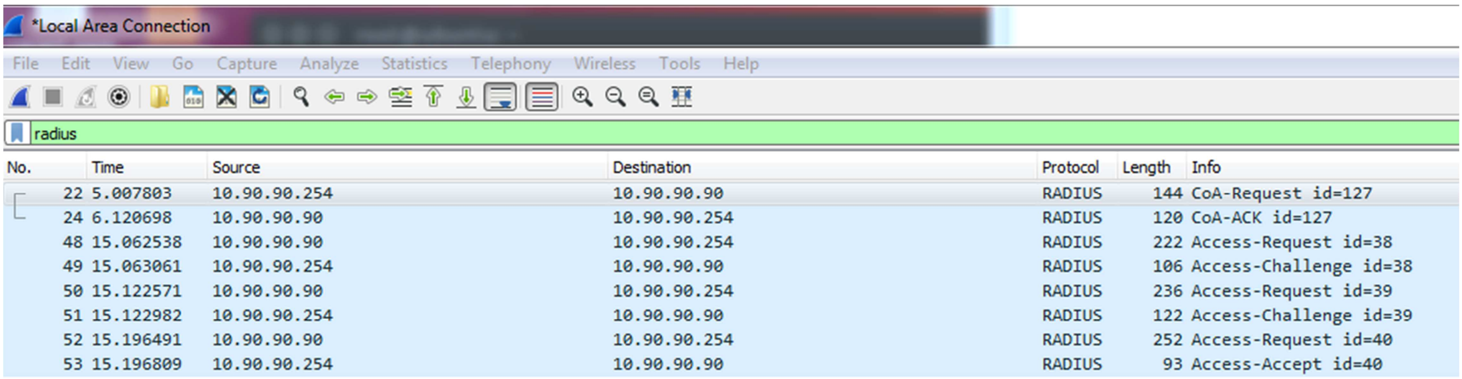
   radclient 10.90.90.90:3799 -f /home/james/Desktop/coa.txt -d /etc/freeradius/ coa **testing123**

c. Then, check the syslog of switch, you will see the port21 is flapped by the attribute of “bounce-host-port”.



```
Switch#show logging

Total number of buffered messages:3

#3     2000-02-07 01:08:35 INFO(6) 802.1X authentication success(Username: admin, Ethernet1/0/21, MAC: 28-D2-44-BF-AB-D5)
#2     2000-02-07 01:08:34 INFO(6) Port eth1/0/21 link up, 1000Mbps FULL duplex
#1     2000-02-07 01:08:26 INFO(6) Port eth1/0/21 link down
```

d. Attched is captured pakcet file, you can see that the host will be re-authenticated after CoA ACK is sending to Radius Server


*Local Area Connection [redacted]
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
radius

```
No.  Time       Source        Destination   Protocol Length Info
  22 5.007803   10.90.90.254  10.90.90.90   RADIUS    144 CoA-Request id=127
  24 6.120698   10.90.90.90   10.90.90.254  RADIUS    120 CoA-ACK id=127
  48 15.062538  10.90.90.90   10.90.90.254  RADIUS    222 Access-Request id=38
  49 15.063061  10.90.90.254  10.90.90.90   RADIUS    106 Access-Challenge id=38
  50 15.122571  10.90.90.90   10.90.90.254  RADIUS    236 Access-Request id=39
  51 15.122982  10.90.90.254  10.90.90.90   RADIUS    122 Access-Challenge id=39
  52 15.196491  10.90.90.90   10.90.90.254  RADIUS    252 Access-Request id=40
  53 15.196809  10.90.90.254  10.90.90.90   RADIUS     93 Access-Accept id=40
```

COA_bounce port.pcapng

#DM Test (Disconnected Message)

The DM message is used to disconnect subscriber sessions in the system from a RADIUS server. The DM request message should contain necessary attributes to identify the subscriber session. If the system successfully disconnects the subscriber session, a DM-ACK message is sent back to the RADIUS server, otherwise, a DM-NAK message is sent with proper error reasons.

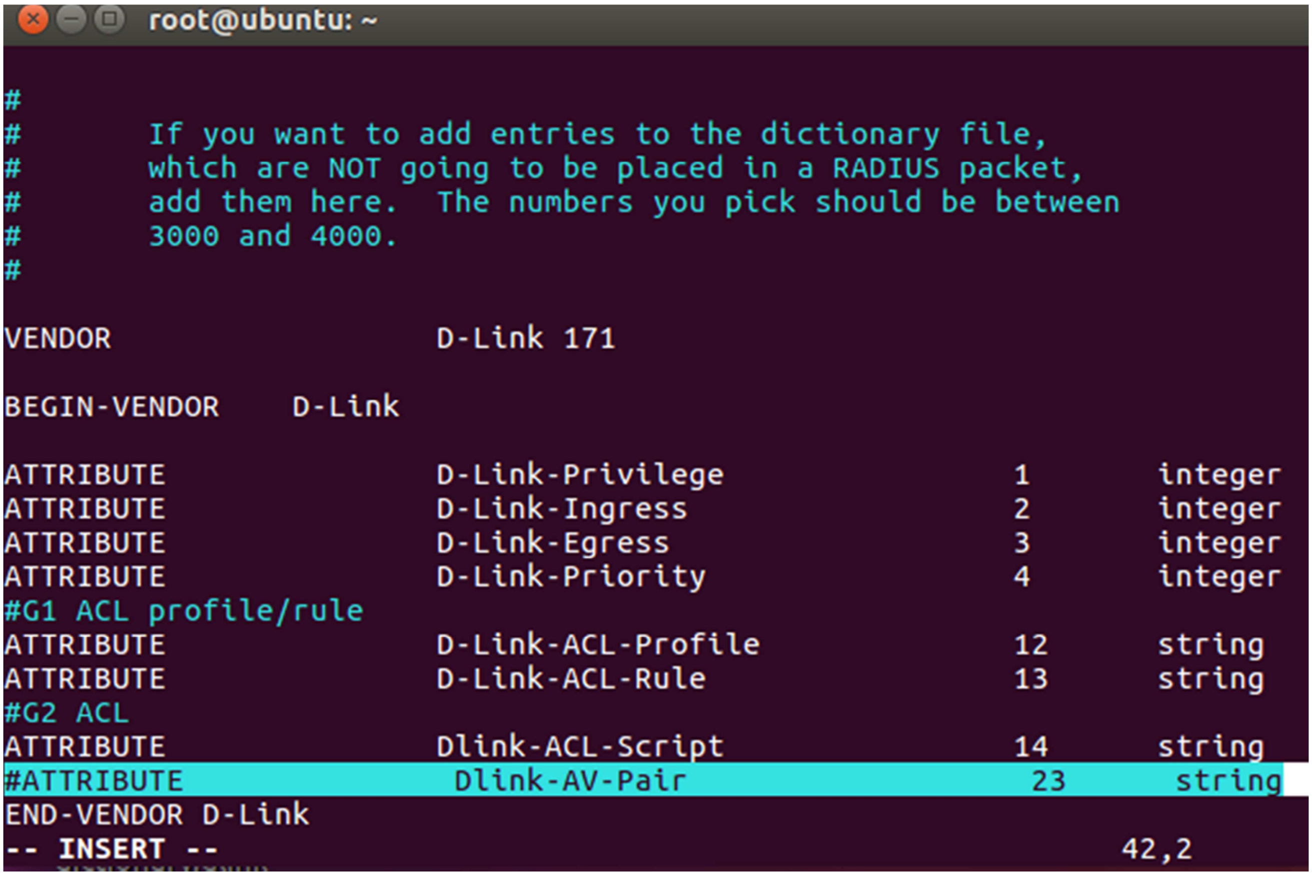
NOTE:
Based on RFC-5176
A Disconnect-Request MUST contain only NAS and session identification attributes. If other attributes are included in a Disconnect-Request, implementations MUST send a Disconnect-NAK; an Error-Cause Attribute with value "Unsupported Attribute" MAY be included. *

So, we need to remove the attribute: dlink-av-pair from Radius Server.

1) On Ubuntu Radius Server, comment the attribute of D-Link

Dictionary.dlink
Attribute Name: Dlink-AV-Pair
Vendor type : 23
Type:String

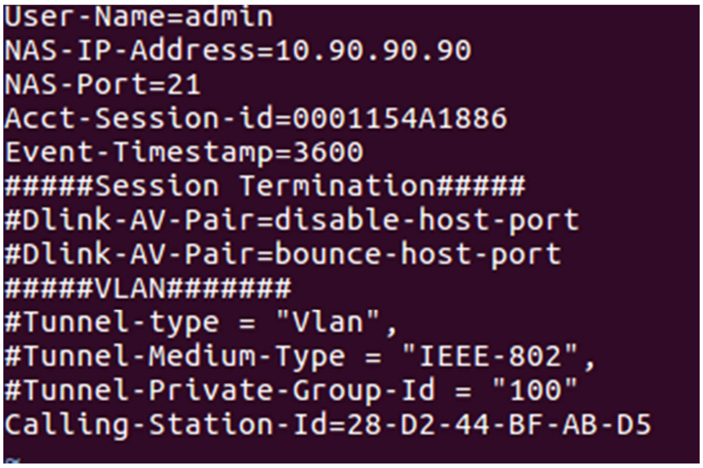
=>vim /usr/share/freeradius/dictionary.dlink



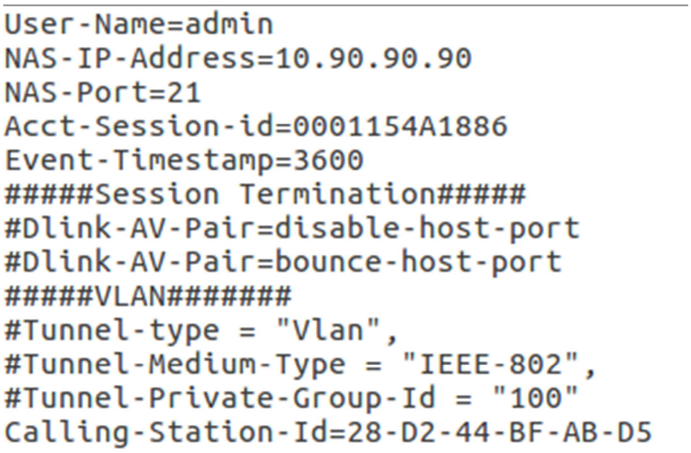
```
#
#       If you want to add entries to the dictionary file,
#       which are NOT going to be placed in a RADIUS packet,
#       add them here.  The numbers you pick should be between
#       3000 and 4000.
#

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               Dlink-ACL-Script                14      string
#ATTRIBUTE               Dlink-AV-Pair                   23      string
END-VENDOR D-Link
-- INSERT --                                                  42,2
```

2) Modify the acct-session-id on coa.txt file on /home/james/Desktop/coa.txt & /usr/bin usr/ coa.txt to make the acct-session-id match with current session.

And, comment all attributes from the list



```
User-Name=admin
NAS-IP-Address=10.90.90.90
NAS-Port=21
Acct-Session-id=0001154A1886
Event-Timestamp=3600
#####Session Termination#####
#Dlink-AV-Pair=disable-host-port
#Dlink-AV-Pair=bounce-host-port
#####VLAN#######
#Tunnel-type = "Vlan",
#Tunnel-Medium-Type = "IEEE-802",
#Tunnel-Private-Group-Id = "100"
Calling-Station-Id=28-D2-44-BF-AB-D5
```



```
User-Name=admin
NAS-IP-Address=10.90.90.90
NAS-Port=21
Acct-Session-id=0001154A1886
Event-Timestamp=3600
#####Session Termination#####
#Dlink-AV-Pair=disable-host-port
#Dlink-AV-Pair=bounce-host-port
#####VLAN#######
#Tunnel-type = "Vlan",
#Tunnel-Medium-Type = "IEEE-802",
#Tunnel-Private-Group-Id = "100"
Calling-Station-Id=28-D2-44-BF-AB-D5
```

2) ##Suppose that PC already passed 802.1x auth on port 21##

If Administrator expect RADIUS sending **Disconnect-Request** , please use below command

```
radclient 10.90.90.90:3799 -f Desktop/coa.text -d /etc/freeradius/ disconnect 123456
```

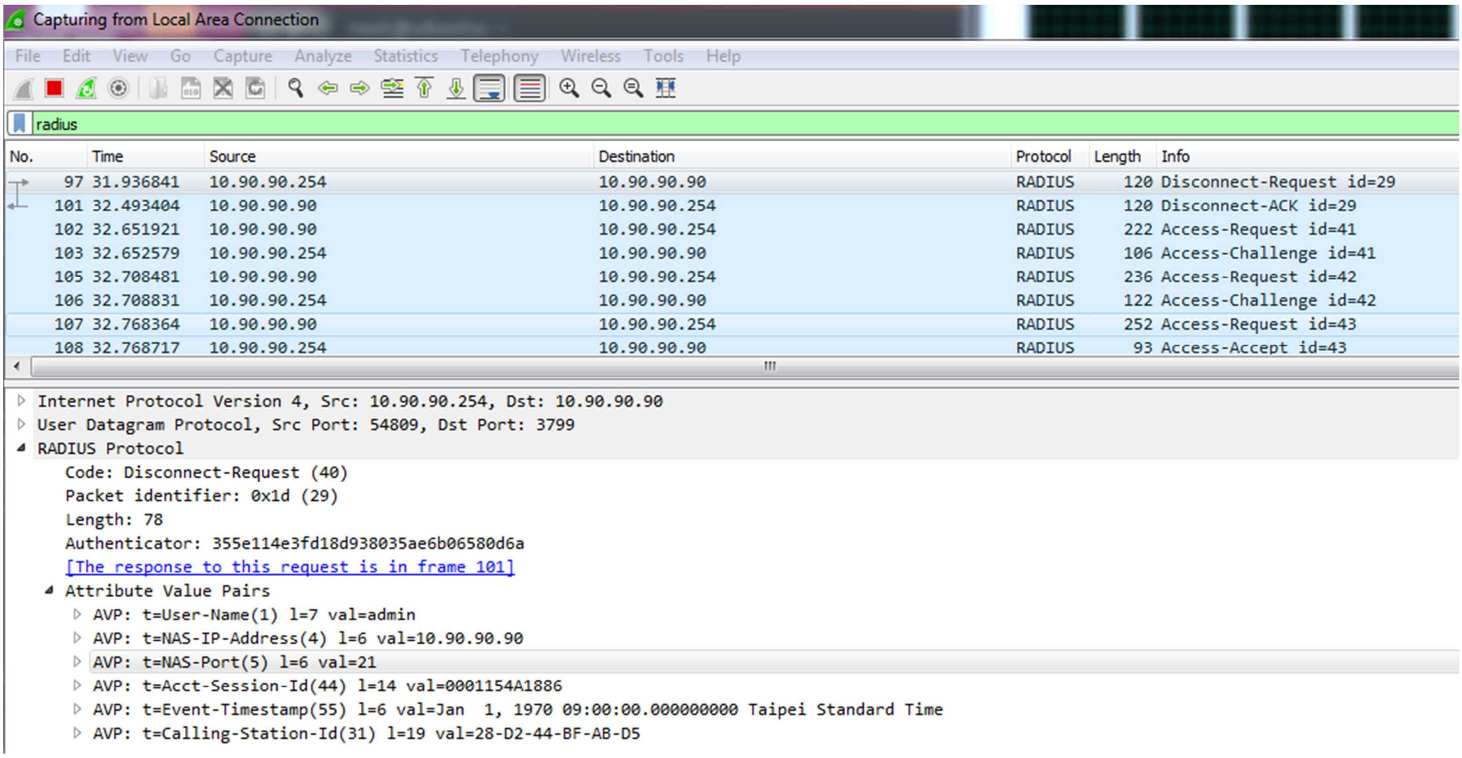
3) Attched is captured pakcet file, you can see that the host will be re-authenticated after Disconnect ACK is sending to Radius Serve.

Please be noted, DM just makes the authenticated host re-authenticated only,

Do NOT the below two actions as CoA

bounce-host-port

disable-host-port



radius

```
No.   Time        Source        Destination   Protocol  Length Info
   97 31.936841   10.90.90.254  10.90.90.90   RADIUS       120 Disconnect-Request id=29
  101 32.493404   10.90.90.90   10.90.90.254  RADIUS       120 Disconnect-ACK id=29
  102 32.651921   10.90.90.90   10.90.90.254  RADIUS       222 Access-Request id=41
  103 32.652579   10.90.90.254  10.90.90.90   RADIUS       106 Access-Challenge id=41
  105 32.708481   10.90.90.90   10.90.90.254  RADIUS       236 Access-Request id=42
  106 32.708831   10.90.90.254  10.90.90.90   RADIUS       122 Access-Challenge id=42
  107 32.768364   10.90.90.90   10.90.90.254  RADIUS       252 Access-Request id=43
  108 32.768717   10.90.90.254  10.90.90.90   RADIUS        93 Access-Accept id=43
```

```
▷ Internet Protocol Version 4, Src: 10.90.90.254, Dst: 10.90.90.90
▷ User Datagram Protocol, Src Port: 54809, Dst Port: 3799
◢ RADIUS Protocol
    Code: Disconnect-Request (40)
    Packet identifier: 0x1d (29)
    Length: 78
    Authenticator: 355e114e3fd18d938035ae6b06580d6a
    [The response to this request is in frame 101]
  ◢ Attribute Value Pairs
    ▷ AVP: t=User-Name(1) l=7 val=admin
    ▷ AVP: t=NAS-IP-Address(4) l=6 val=10.90.90.90
    ▷ AVP: t=NAS-Port(5) l=6 val=21
    ▷ AVP: t=Acct-Session-Id(44) l=14 val=0001154A1886
    ▷ AVP: t=Event-Timestamp(55) l=6 val=Jan  1, 1970 09:00:00.000000000 Taipei Standard Time
    ▷ AVP: t=Calling-Station-Id(31) l=19 val=28-D2-44-BF-AB-D5
```

DM.pcapng