Understand and Troubleshoot RADIUS CoA and Disconnect Messages

TAC **Document ID: 119397**

Contributed by Tomasz Dudarski and Maciej Poszywak, Cisco TAC Engineers.
Dec 17, 2015

Contents

Introduction

This document describes RADIUS disconnect messages (DMs).

Definition of RADIUS CoA Messages

A Change of Authorization (CoA) message is used in order to change attributes and the data filters associated with a user session. The system supports CoA messages from the Authentication, Authorization, and Accounting (AAA) server to change data filters associated with a subscriber session.

Note: The filters in filter-id attributes (if present in the request) should be configured in the ASR 5000 for application to the user traffic. This is the form of Access Control Lists (ACLs) and is configured in the ASR 5000 with **ip access-list** commands.

The CoA request message should contain attributes to identify the user session; attributes and the data filters need to be applied to the user session. The filter-id attribute (attribute id 11) contains the names of the filters. If the ASR 5000 successfully executes the CoA request, a CoA ACK is sent back to the RADIUS server and the new attributes and data filters are applied to the user session. Otherwise, a CoA NAK is sent with proper reason as an error-code attribute without making any changes to the user session.

RADIUS DM

The DM message is used in order to disconnect user sessions in the ASR 5000 from a RADIUS server. The DM request message should contain necessary attributes in order to identify the user session. If the system successfully disconnects the user session, DM ACK is sent back to the RADIUS server. Otherwise, DM-NAK is sent with proper error reasons.

As mentioned previously, it is possible that the NAS cannot honor Disconnect-Request or CoA-Request messages for some reason. The Error-Cause Attribute provides more detail on the cause of the problem. It CAN be included within Disconnect-ACK, Disconnect-NAK, and CoA-NAK messages.

The Value field is four octets, which contains an integer that specifies the cause of the error.

- Values **0-199** and **300-399** are reserved.
- Values **200-299** represent successful completion, so that these values might only be sent within Disconnect-ACK or CoA-ACK message and MUST NOT be sent within a Disconnect-NAK or CoA-NAK.
- Values **400-499** represent fatal errors committed by the RADIUS server, so that they CAN be sent within CoA-NAK or Disconnect-NAK messages and MUST NOT be sent within CoA-ACK or Disconnect-ACK messages.
- Values **500-599** represent fatal errors that occur on a NAS or RADIUS proxy, so that they CAN be sent within CoA-NAK and Disconnect-NAK messages, and MUST NOT be sent within CoA-ACK or Disconnect-ACK messages. Error-Cause values SHOULD be logged by the RADIUS server.

Error-Code values (expressed in decimal) include:

```
#     Value
---   -----
201   Residual Session Context Removed>
202   Invalid EAP Packet (Ignored)
401   Unsupported Attribute
402   Missing Attribute
403   NAS Identification Mismatch
404   Invalid Request
405   Unsupported Service
406   Unsupported Extension
501   Administratively Prohibited
502   Request Not Routable (Proxy)
503   Session Context Not Found
504   Session Context Not Removable
505   Other Proxy Processing Error
506   Resources Unavailable
507   Request Initiated
```

Attributes for Session Identification

For identification of the ASR 5000, one of these methods can be used:

- NAS-IP-Address: NAS IP address if present in the COA/DM request should match with the ASR 5000 NAS IP address.
- NAS-Identifier: If this attribute is present, its value should match to the nas-identifier generated for the user session.
  This is a mandatory attribute for session identification, if the ASR 5000 is configured with NAS-Identifier.

For identification of the user session, either one of these methods is used:

- Acct-Session-ID: If this attribute is present, its value should match to the acct-session-id for the user session.

- Framed-IP-Address: If this attribute is present, its values should match to the framed IP address of the session.
- Username: If this attribute is present, its values should match to the username of the session.
- Calling-Station-ID: This is the International Mobile Subscriber Identity (IMSI) of the user.

Configuration of RADIUS DMs

Configuration of a RADIUS DM is quite easy. All the lines needs to be configured in destination context (the one with the RADIUS configuration).

radius change-authorize-nas-ip *ip_address* **[encrypted] key** *value* **[port** *port* **]**
[eventtimestamp-window *window* **] [no-nas-identification-check]**
[no-reverse-path-forward-check][mpls-label input *in_label_value* **| output** *out_label_value1*
[*out_label_value2* **]**

Note: The "radius change-authorize-nas-ip" should be your local context's AAA interface address. This CLI command is sometimes a source of confusion.

Sample Configuration

```
radius change-authorize-nas-ip 192.168.88.40 encrypted key <key value>
 no-reverse-path-forward-check
no-nas-identification-check
```

Failure Scenario Examples

No DM Messages Received on the ASR 5000 Side

It is possible that the socket is not ready for UDP port 3799. (In accordance with RFC 3756, the RADIUS Disconnect-Request packet is sent to UDP port 3799).

This behavior can be simplified. The process which handles all the CoA requests is aaamgr instance 385, which is the one on the active SMC/MIO card. This CLI command needs to be executed in the destination context.

```
#cli test-commands password <xx> #show radius info radius group all instance 385
```

Such output looks like:

```
# show radius info radius group all instance 385 AAAMGR instance 385:
 cb-list-en: 3 AAA Group: <>
-------------------------------------------
socket number: 19
socket state: ready
local ip address: 10.176.81.215
local udp port: 50954
flow id: 0
use med interface: no
VRF context ID: 66
```

In this example, there is no port 3799 and this is the reason for the reported behavior. If you see the same in your case, the solution is to remove and re-add the CoA configuration in order to recreate the listening socket. Additionally, you can try to kill aaamgr instance 385 if the first solution does not help.

After the described actions, you should see this output:

```
# show radius info radius group all instance 385 AAAMGR instance 385:
 cb-list-en: 3 AAA Group: <>
------------------------------------------->
socket number: 19>
socket state: ready
local ip address: 10.176.81.215
local udp port: 50954
flow id: 0
use med interface: no
VRF context ID: 66
socket number: 21   <---------------------
socket state: ready
local ip address: 10.176.81.215
local udp port: 3799 <---------------------
flow id: 0
use med interface: no
```

and the socket should be visible from the debug shell on the appropriate context/VR:

```
bash-2.05b# netstat -lun | grep 3799
udp 0 0 10.176.81.215:3799 0.0.0.0:*
```

UDP Port 3379 Has Ready Socket with No DM Messages

The UDP port 3379 has ready socket, however you still do not see the DM messages. This is probably caused by an incorrect configuration of **radius change-authorize-nas-ip**. Either the attribute values that came in the DM request message do not match the ones which were sent in an Accounting request towards RADIUS.

Accounting Request

```
Thursday August 06 2015
<<<<OUTBOUND
Code: 4 (Accounting-Request)
      Attribute Type: 44 (Acct-Session-Id)
                Length: 18
                Value: 42 43 37 31 44 46 32 36 BC71DF26
                       30 36 30 33 41 32 42 46 0603A2BF
      Attribute Type: 31 (Calling-Station-Id)
                Length: 14
                Value: 39 39 38 39 33 31 37 32 99893172
                       30 39 31 31             0911
      Attribute Type: 4 (NAS-IP-Address)
                Length: 6
                Value: C0 A8 58 E1             ..X.
                       (192.168.88.225)
      Attribute Type: 8 (Framed-IP-Address)
                Length: 6
                Value: 0A 55 12 21             .U.!
                       (10.85.18.33)
```

Disconnect-Request

```
Radius Protocol
    Code: Disconnect-Request (40)
    Packet identifier: 0x2 (2)
    Length: 71
    Authenticator: 4930a228f13da294550239f5187b08b9

    Attribute Value Pairs
        AVP: l=6 t=NAS-IP-Address(4): 192.168.88.225
```

```
            NAS-IP-Address: 192.168.88.225 (192.168.88.225)

        AVP: l=6 t=Framed-IP-Address(8): 10.85.18.33
            Framed-IP-Address: 10.85.18.33 (10.85.18.33)

        AVP: l=14 t=Calling-Station-Id(31): 998931720911
            Calling-Station-Id: 998931720911

        AVP: l=18 t=Acct-Session-Id(44): BC71DF260603A2BF
            Acct-Session-Id: BC71DF260603A200
```

In this example, the value of **Acct-Session-Id** which comes to the ASR 5000 is different than the one sent towards RADIUS and this is the reason for the issue. This problem can be fixed by proper changes on the RADIUS side.

The Acct-Session-Id for the active session can be verified with the command **show subscribers ggsn-only aaa-configuration active imsi <>**.

```
[local]# show subscribers ggsn-only aaa-configuration active imsi 434051801170727

Username: 998931720911@mihc1             Status: Online/Active
  Access Type: ggsn-pdp-type-ipv4        Network Type: IP
  Access Tech: WCDMA UTRAN               Access Network Peer ID: n/a
  callid: 057638b8                       imsi: 434051801170727
  3GPP2 Carrier ID: n/a
  3GPP2 ESN: n/a
  RADIUS Auth Server: 192.168.88.40  RADIUS Acct Server: n/a
  NAS IP Address: 192.168.88.225
  Acct-session-id: BC71DF260603A2BF
```

All the Attributes Match, but the ASR 5000 Sends DM NAK with the Error Message: 401 - Unsupported Attribute

At this point it is known that this kind of error message means that the issue comes from the RADIUS server. However, it is still not clear what is wrong. Here, the limitation of the ASR 5000 does not support Called-station-Id in Radius DM. Hence, if it is seen there, it answers with the highlighted error.

```
INBOUND>>>>>
RADIUS COA Rx PDU, from 192.168.1.254:38073 to 192.168.1.2:1800
Code: 40 (Disconnect-Request)
Id: 106
Length: 61
Authenticator: 8D F1 50 2E DD 79 49 39 79 A0 B5 FC 59 3E C4 51
     Attribute Type: 32 (NAS-Identifier)
               Length: 9
               Value: 73 74 61 72 65 6E 74   starent
     Attribute Type: 1 (User-Name)
               Length: 10
               Value: 74 65 73 74 75 73 65 72 testuser
     Attribute Type: 30 (Called-Station-ID)
               Length: 9
               Value: 65 63 73 2D 61 70 6E   ecs-apn
     Attribute Type: 31 (Calling-Station-Id)
               Length: 13
               Value: 36 34 32 31 31 32 33 34 64211234
                      35 36 37               567

<<<<OUTBOUND 06:57:42:683 Eventid:70902(6)
RADIUS COA Tx PDU, from 192.168.1.2:1800 to 192.168.1.254:38073
Code: 42 (Disconnect-Nak)
Id: 106
Length: 26
```

```
Authenticator: 34 2E DE B4 77 22 4A FE A5 16 93 91 0D B2 E6 3B
     Attribute Type: 101 (Error-Cause)
               Length: 6
               Value: 00 00 01 91             ....
                      (Unsupported-Attribute)
```

System Has Configured "no-nas-identification-check" in the "radius change-authorize-nas-ip" Line, "NAS-Identification-Mismatch" Error Still Returned

This happens in this configuration:

```
radius change-authorize-nas-ip 192.168.1.2 encrypted key
+A27wvxlgy06ia30pcqswmdajxd11ckg4ns88i6l92dghsqw7v77f1 port 1800
 event-timestamp-window 0 no-reverse-path-forward-check no-nas-identification-check
    aaa group default
    radius attribute nas-ip-address address 192.168.1.2
    radius server 192.168.1.128 encrypted key
 +A3ec01d8zs92ed1gz2mytddjjrf11af3u0watpyr3gd0rs8mthlzc port 1812
    radius accounting server 192.168.1.128 encrypted key
 +A24x0pj4mjgnqh0sclbnen1lm6f1d6drn2nw3yf31tmfldk9fr38e         port 1813
 #exit
```

For an active PDP context, the Disconnect Request is NAKed:

```
INBOUND>>>>>  04:27:13:898 Eventid:70901(6)
RADIUS COA Rx PDU, from 192.168.1.254:42082 to 192.168.1.2:1800 (52) PDU-dict=starent-vsa1
 Code: 40 (Disconnect-Request)
 Id: 115
 Length: 52
 Authenticator: BF 95 05 0B 87 B4 42 59 5F C6 CC 78 D7 17 77 7F
      Attribute Type: 32 (NAS-Identifier)
                Length: 9
                Value: 73 74 61 72 65 6E 74    starent
      Attribute Type: 1 (User-Name)
                Length: 10
                Value: 74 65 73 74 75 73 65 72 testuser
      Attribute Type: 31 (Calling-Station-Id)
                           Value: 36 34 32 31 31 32 33 34 64211234;     Length: 13

                       35 36 37               567

Monday October 19 2015
<<<<OUTBOUND  04:27:13:898 Eventid:70902(6)
RADIUS COA Tx PDU, from 192.168.1.2:1800 to 192.168.1.254:42082 (26) PDU-dict=starent-vsa1
 Code: 42 (Disconnect-Nak)
 Id: 115
 Length: 26
 Authenticator: 75 D1 04 3E 31 19 9C 92 B2 2E 5D 5F 98 B9 34 99
      Attribute Type: 101 (Error-Cause)
                Length: 6
                Value: 00 00 01 93             ....
                       (NAS-Identification-Mismatch)
```

However, when this line is included in the default AAA group:

```
    radius attribute nas-identifier starent
```

it starts to work:

```
Monday October 19 2015
INBOUND>>>>>  05:19:01:798 Eventid:70901(6)
```

```
RADIUS COA Rx PDU, from 192.168.1.254:55426 to 192.168.1.2:1800 (52) PDU-dict=starent-vsa1
 Code: 40 (Disconnect-Request)
 Id: 171
 Length: 52
 Authenticator: 3A 67 43 25 DC 18 5C E3 23 08 04 C0 9C 31 68 68
      NAS-Identifier = starent
      User-Name = testuser
      Calling-Station-Id = 64211234567


Monday October 19 2015
<<<<OUTBOUND  05:19:01:799 Eventid:70902(6)
RADIUS COA Tx PDU, from 192.168.1.2:1800 to 192.168.1.254:55426 (26) PDU-dict=starent-vsa1
 Code: 41 (Disconnect-Ack)
 Id: 171
 Length: 26
 Authenticator: 45 07 79 C5 E0 92 53 28 8F AD A3 E3 C4 B4 52 10
      Acct-Termination-Cause = Admin_Reset
```

Or it will also work without configuration of the nas-identifier on the AAA group, but with NAS-Identifier AVP removed from the Disconnect-Request:

```
INBOUND>>>>>  05:14:41:374 Eventid:70901(6)
RADIUS COA Rx PDU, from 192.168.1.254:54757 to 192.168.1.2:1800 (43) PDU-dict=starent-vsa1
 Code: 40 (Disconnect-Request)
 Id: 78
 Length: 43
 Authenticator: 84 5D FE 5E 90 0D C8 16 84 7A 11 67 FF 82 40 DB
      User-Name = testuser
      Calling-Station-Id = 64211234567

Monday October 19 2015
<<<<OUTBOUND  05:14:41:375 Eventid:70902(6
RADIUS COA Tx PDU, from 192.168.1.2:1800 to 192.168.1.254:54757 (26) PDU-dict=starent-vsa1
 Code: 41 (Disconnect-Ack)
 Id: 78
 Length: 26
 Authenticator: 34 84 5B 8E AF 02 1C F2 58 26 1B 0C 20 37 93 33
      Acct-Termination-Cause = Admin_Reset
```

Cisco bug ID CSCuw78786 has been submitted. This has been tested on Release 17.2.0 and Release 15.

Updated: Dec 17, 2015 Document ID: 119397