

# CPSのサブスクリプション変更後のPPPoEセッションの非終了のトラブルシューティング

## 内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[問題](#)

[再生手順の発行](#)

[COAとその退職者に関して注目すべき主なポイント](#)

[解決方法](#)

## 概要

このドキュメントでは、Radiusプロトコルを使用したCisco Policy Suite(CPS)のサブスクリプション変更後にPPPoEセッションが終了しない場合のトラブルシューティング手順について説明します。

## 前提条件

### 要件

次の項目に関する知識があることが推奨されます。

- Linux
- CPS
- RADIUS プロトコル

次の特権アクセス権が必要です。

- CPS CLIへのルートアクセス
- CPS GUIへの「qns-svn」ユーザアクセス (ポリシービルダーおよびコントロールセンター)

### 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- CPS 13.1
- UCS-B

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド

キュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

## 背景説明

CPSは、Point-to-Point Protocol over Ethernet(PPPoE)加入者をサポートする認証、許可、アカウントリング(AAA)サーバ/クライアントモデルとして機能するように設計されています。CPSはASR9KまたはASR1Kデバイスと通信して、PPPoEセッションを管理します。

## 問題

PPPoEセッションは、外部プロビジョニングシステムからのSimple Object Access Protocol(SOAP)アプリケーションプログラミングインターフェイス(API)要求を介してCPSで新しいサブスクリプションが選択された後に切断および再接続されません。

CPSはアクション変更(COA)要求を生成してASR9Kデバイスに送信できますが、これらの要求は「応答タイムアウトエラーなし」でASR9Kデバイスによってタイムアウトされます。

次にエラーメッセージの例を示します。

```
dc1-1b01 dc1-1b01 2021-09-28 21:26:13,331 [pool-2-thread-1] ERROR
c.b.p.r.jms.PolicyActionJmsReceiver - Error executing RemoteAction. Returning Error Message
response
com.broadhop.exception.BroadhopException: Timeout: No Response from RADIUS Server
    at com.broadhop.radius.impl.actions.AsynchCoARequest.execute(AsynchCoARequest.java:213)
~[com.broadhop.radius.service_13.0.1.r150127.jar:na]
    at
com.broadhop.utilities.policy.remote.RemoteActionStub.execute(RemoteActionStub.java:62)
~[com.broadhop.utility_13.0.0.release.jar:na]
    at
com.broadhop.policy.remote.jms.PolicyActionJmsReceiver$RemoteActionExecutor.run(PolicyActionJmsReceiver.java:98) ~[com.broadhop.policy.remote.jms_13.0.0.release.jar:na]
    at
com.broadhop.utilities.policy.async.PolicyRemoteAsyncActionRunnable.run(PolicyRemoteAsyncActionRunnable.java:24) [com.broadhop.utility_13.0.0.release.jar:na]
    at java.util.concurrent.Executors$RunnableAdapter.call(Executors.java:511) [na:1.8.0_72]
    at java.util.concurrent.FutureTask.run(FutureTask.java:266) [na:1.8.0_72]
    at
com.broadhop.utilities.policy.async.AsyncPolicyActionExecutionManager$GenericThread.run(AsyncPolicyActionExecutionManager.java:301) [com.broadhop.utility_13.0.0.release.jar:na]
Caused by: net.jradius.exception.TimeoutException: Timeout: No Response from RADIUS Server
    at net.jradius.client.RadiusClientTransport.sendReceive(RadiusClientTransport.java:112)
~[na:na]
    at net.jradius.client.RadiusClient.changeOfAuth(RadiusClient.java:383) ~[na:na]
    at com.broadhop.radius.impl.actions.AsynchCoARequest.execute(AsynchCoARequest.java:205)
~[com.broadhop.radius.service_13.0.1.r150127.jar:na]
    ... 6 common frames omitted
```

## 再生手順の発行

ステップ1:ASR9KまたはASR1KデバイスからPPPoEセッションを開始し、Control Center経由でCPSでこれらのセッションを確認します。

ステップ2:SOAP API要求を開始して、サブスライバに関連付けられているサービスのサブスクリプションを更新します。

The screenshot shows a Wireshark capture of a network packet. The packet list pane shows three frames: 2665 (TCP), 2666 (HTTP/XML), and 2667 (TCP). The packet details pane for frame 2666 shows the following structure:

- Frame 2666: 1348 bytes on wire (10784 bits), 1348 bytes captured (10784 bits)
- Linux cooked capture v1
- Internet Protocol Version 4, Src: [redacted], Dst: [redacted]
- Transmission Control Protocol, Src Port: 32928, Dst Port: 8080, Seq: 2897, Ack: 1, Len: 1280
- [2 Reassembled TCP Segments (4176 bytes): #2665(2896), #2666(1280)]
- Hypertext Transfer Protocol
- eXtensible Markup Language
  - <?xml
  - <SOAP-ENV:Envelope
    - xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"
    - xmlns:ns1="http://broadhop.com/unifiedapi/soap/types"
    - <SOAP-ENV:Body>
      - <ns1:UpdateSubscriberRequest>
        - <ns1:subscriber>
          - <ns1:id>
          - <ns1:name>
          - <ns1:credential>
          - <ns1:status>
          - <ns1:avp>
          - <ns1:avp>
          - <ns1:avp>
          - <ns1:version>
          - <ns1:subAccount>
          - <ns1:subAccount>
          - </ns1:subscriber>

ステップ3:CPSはASR9KまたはASR1Kに対するCOA要求を開始します。CPSが同じCOAの重複した要求を使用して同じ要求の再試行を実行していることがわかります。

The screenshot shows a Wireshark capture of RADIUS CoA requests. The packet list pane shows four frames: 2675 (RADIUS), 2757 (RADIUS), 2899 (RADIUS), and 2985 (RADIUS). The packet details pane for frame 2675 shows the following structure:

- Frame 2675: 134 bytes on wire (1072 bits), 134 bytes captured (1072 bits)
- Linux cooked capture v1
- Internet Protocol Version 4, Src: [redacted], Dst: [redacted]
- User Datagram Protocol, Src Port: 34761, Dst Port: 1700
- RADIUS Protocol
  - Code: CoA-Request (43)
  - Packet identifier: 0x4d (77)
  - Length: 90
  - Authenticator: dfdbe5861de70c1a39d5b0fb9350b1d0
  - Attribute Value Pairs
    - AVP: t=Vendor-Specific(26) l=41 vnd=ciscoSystems(9)
    - AVP: t=Acct-Session-Id(44) l=10 val=0477a980
    - AVP: t=User-Name(1) l=19 val=[redacted]

注：最初のパケットはピアデバイス(ASR9K)によって確認応答されないため、CPSの内部ロジックによって再試行メカニズムがトリガーされ、重複する要求が送信されます。

ステップ4：最初のセッションCOA要求とその再試行に対する応答がないため、CPSは他のすべてのセッション更新アクションをドロップします。

これにより、ASR9KでPPPoEセッションが引き続きアクティブであり、セッション更新のためにCPSに対してセッション切断要求が送信されていないことがわかります。CPSは、COA要求に関してASR9KからのAccounting Stop要求を想定しています。

## COAとその退職者に関して注目すべき主なポイント

1. CPSは、特定のサブスクリバのデータベース内のすべてのセッションのアクティブ/存在要求を開始します。
2. CPSは、特定のCOA要求に対するACKまたはNACKを受信しない場合、ポリシービルダーの設定に基づいて再試行メカニズムを開始します。
3. 再試行の回数と間隔は設定可能です。

The screenshot shows the configuration page for a Generic RADIUS Device Pool. The 'General Selection' tab is active. The configuration includes fields for Name, Description, Default Shared Secret, Default CoA Shared Secret, CoA Port (1700), CoA Retries (3), CoA Timeout Seconds (3), Access Request Guard Timer (0), Correlation Key (AccountSessionId), Coa Disconnect Template, Disconnect Template, Proxy Access Accept Filter, Dup Check With Framed Ip, Dup Check With Mac Address, Radius Network Session Correlation, and Control Session Lifecycle (checked). The CoA Retries and CoA Timeout Seconds fields are highlighted in yellow.

再試行設定の例

## 解決方法

この問題を解決するには、さらにASR9Kに対する分析を拡張し、COA要求とその再試行に対するCPSへの応答がない理由を調べる必要があります。

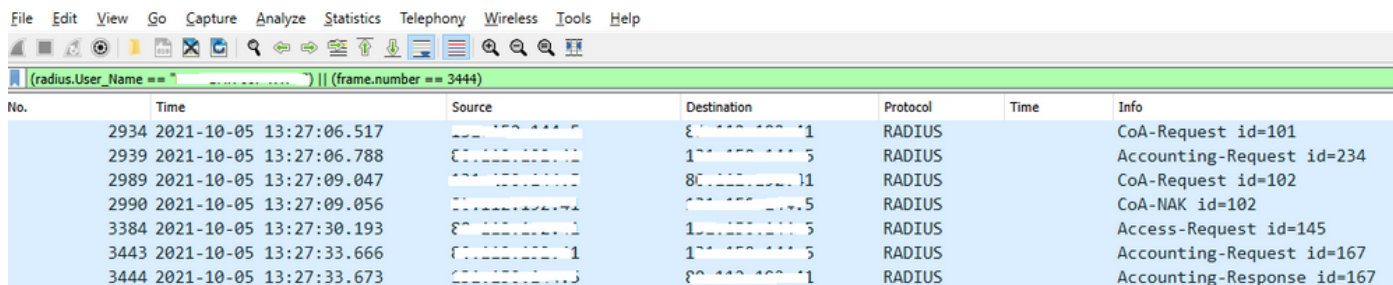
スニファトレースでは、CPSのロードバランサ(LB01)が<IP-1>からCOAを発信し、デフォルトルートであるeth1経由でパケットをルーティングしていることがわかります。

もう1つのロードバランサ(LB02)は<IP-2>からCOAを発信し、eth2経由の特定のルートを使用します。

ASR9Kには、COAが<IP-1>からではなく<IP-2>から送信された場合にのみ、COAを受け入れるアクセスリスト(ACL)があります。

そのため、CPSのLB01のルートテーブルを修正して、適切な送信元IP (特定のルートを経由する<IP-2>)を使用してCOAを送信する必要があります。

サブスクリプションの変更に関する正常なエンドツーエンドRADIUSトランザクションを確認できます。CPS LBルートテーブルで必要な修正を投稿してください。



The image shows a Wireshark network traffic capture window. The title bar includes menu items: File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help. The filter bar contains the expression: (radius.User\_Name == " ") || (frame.number == 3444). The main display area shows a list of captured packets with the following columns: No., Time, Source, Destination, Protocol, Time, and Info. The packets listed are RADIUS transactions with various IDs.

No.	Time	Source	Destination	Protocol	Time	Info
2934	2021-10-05 13:27:06.517	...	...	RADIUS		CoA-Request id=101
2939	2021-10-05 13:27:06.788	...	...	RADIUS		Accounting-Request id=234
2989	2021-10-05 13:27:09.047	...	...	RADIUS		CoA-Request id=102
2990	2021-10-05 13:27:09.056	...	...	RADIUS		CoA-NAK id=102
3384	2021-10-05 13:27:30.193	...	...	RADIUS		Access-Request id=145
3443	2021-10-05 13:27:33.666	...	...	RADIUS		Accounting-Request id=167
3444	2021-10-05 13:27:33.673	...	...	RADIUS		Accounting-Response id=167