Dépanner la non-résiliation de la session PPPoE après une modification d'abonnement dans CPS

Contenu

Introduction

Ce document décrit la procédure de dépannage de la non-fin des sessions PPPoE après un changement d'abonnement dans Cisco Policy Suite (CPS) sur le protocole Radius.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Linux
- CPS
- Protocole Radius

Cisco vous recommande de disposer d'un accès privilégié :

- Accès racine à l'interface CLI CPS
- Accès utilisateur « qns-svn » aux interfaces utilisateur CPS (Policy Builder and Control Center)

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- CPS 13.1
- UCS-B

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

CPS est conçu pour fonctionner comme un modèle serveur/client AAA (Authentication, Authorization, and Accounting), pour prendre en charge les abonnés PPPoE (Point-to-Point Protocol over Ethernet). CPS interagit avec les périphériques ASR9K ou ASR1K pour gérer les sessions PPPoE.

Problème

Les sessions PPPoE ne se déconnectent pas et ne se reconnectent pas après une nouvelle sélection d'abonnement dans CPS via une requête d'interface de programmation d'application (API) SOAP (Simple Object Access Protocol) d'un système de provisionnement externe.

L'observation est que CPS est capable de générer la demande de changement d'action (COA) et de l'envoyer au périphérique ASR9K, mais ces demandes ont un délai d'attente dépassé par le périphérique ASR9K avec l'erreur « No response Timeout ».

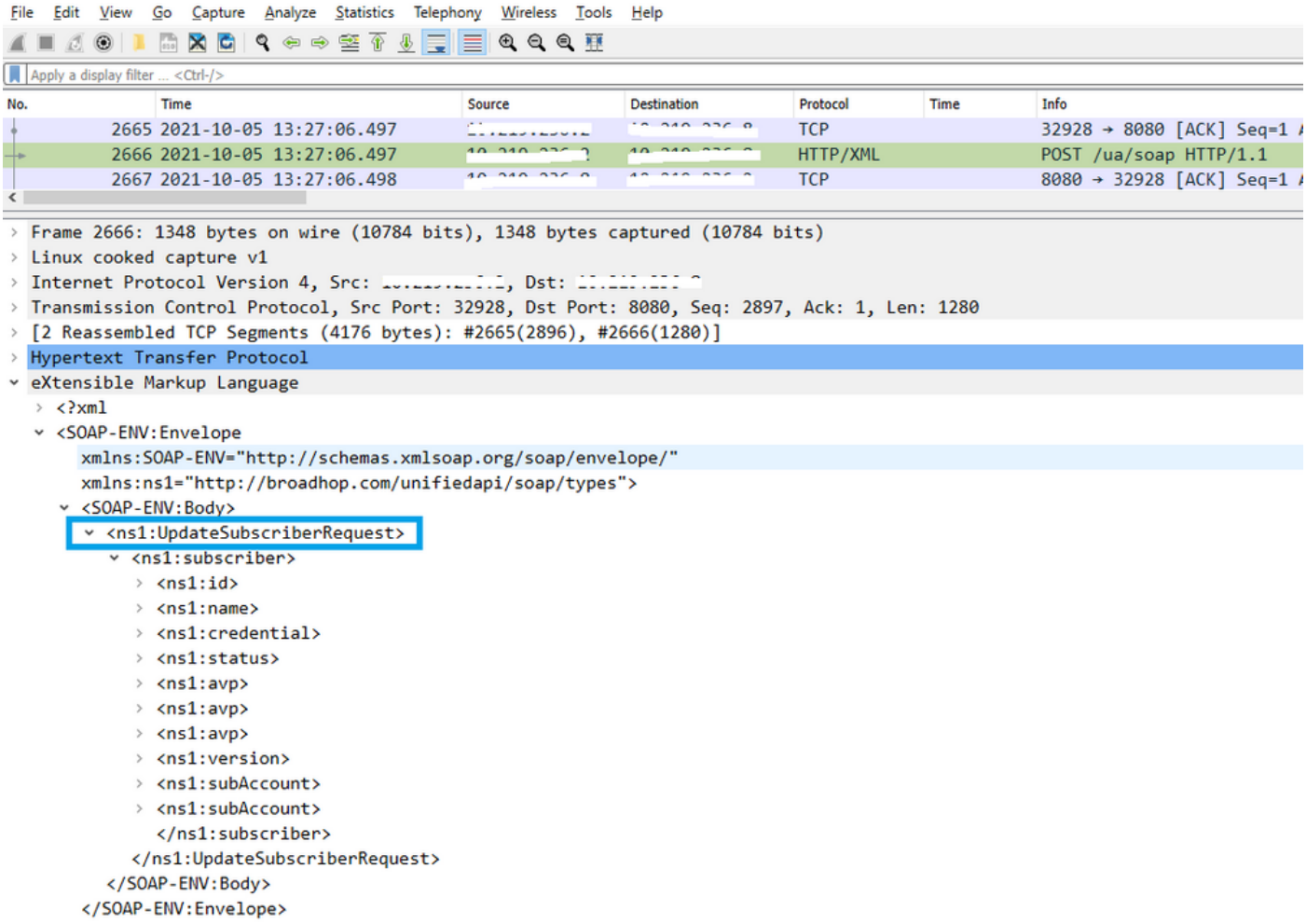
Voici un exemple de message d'erreur :

```
dc1-lb01  dc1-lb01 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$RemoteActionExecutor.run(PolicyActionJmsR
eceiver.java:98) ~[com.broadhop.policy.remote.jms_13.0.0.release.jar:na]
       at
com.broadhop.utilities.policy.async.PolicyRemoteAsyncActionRunnable.run(PolicyRemoteAsyncActionR
unnable.java:24) [com.broadhop.utility_13.0.0.release.jar:na]
       at java.util.concurrent.Executors$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$GenericThead.run(AsyncPoli
cyActionExecutionManager.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
```

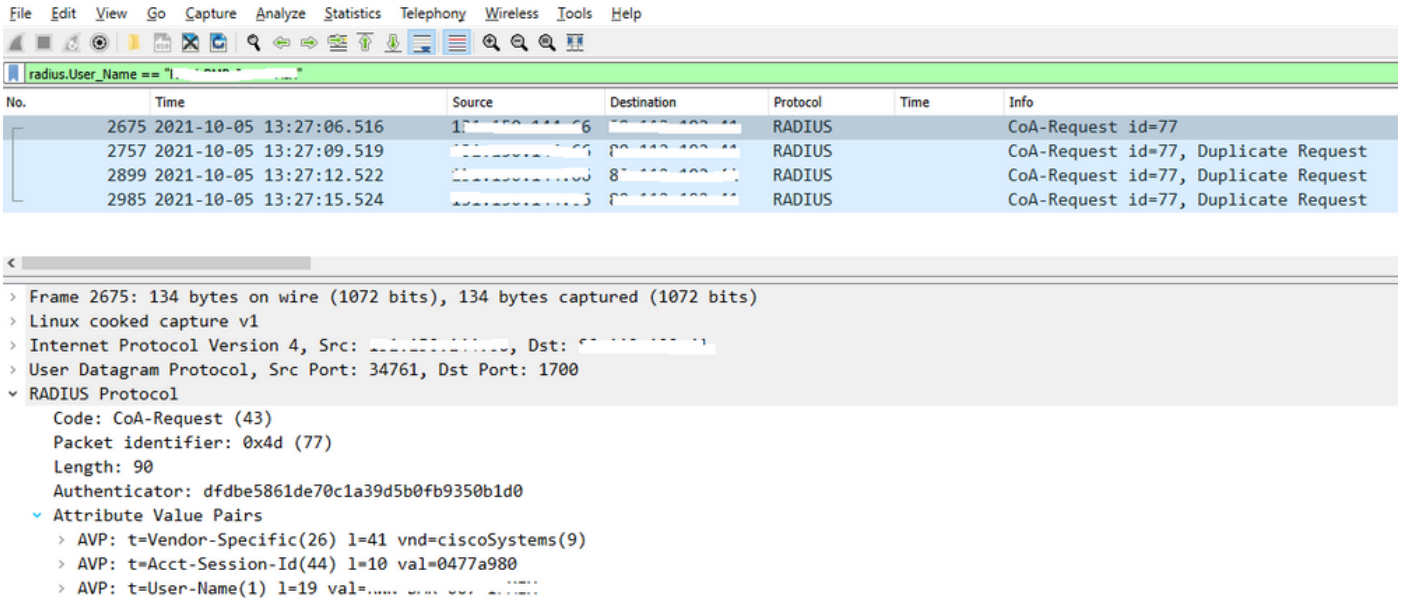
Étapes de reproduction du problème

Étape 1. Lancez des sessions PPPoE à partir de périphériques ASR9K ou ASR1K, assurez-vous que ces sessions s'affichent dans CPS via Control Center.

Étape 2. Lancer une demande d'API SOAP pour mettre à jour l'abonnement de services associé à l'abonné.



Étape 3. CPS démarre les demandes de certificat d'authenticité vers ASR9K ou ASR1K. Vous pouvez observer que CPS effectue une nouvelle tentative de la même demande avec la demande dupliquée du même certificat d'authenticité.



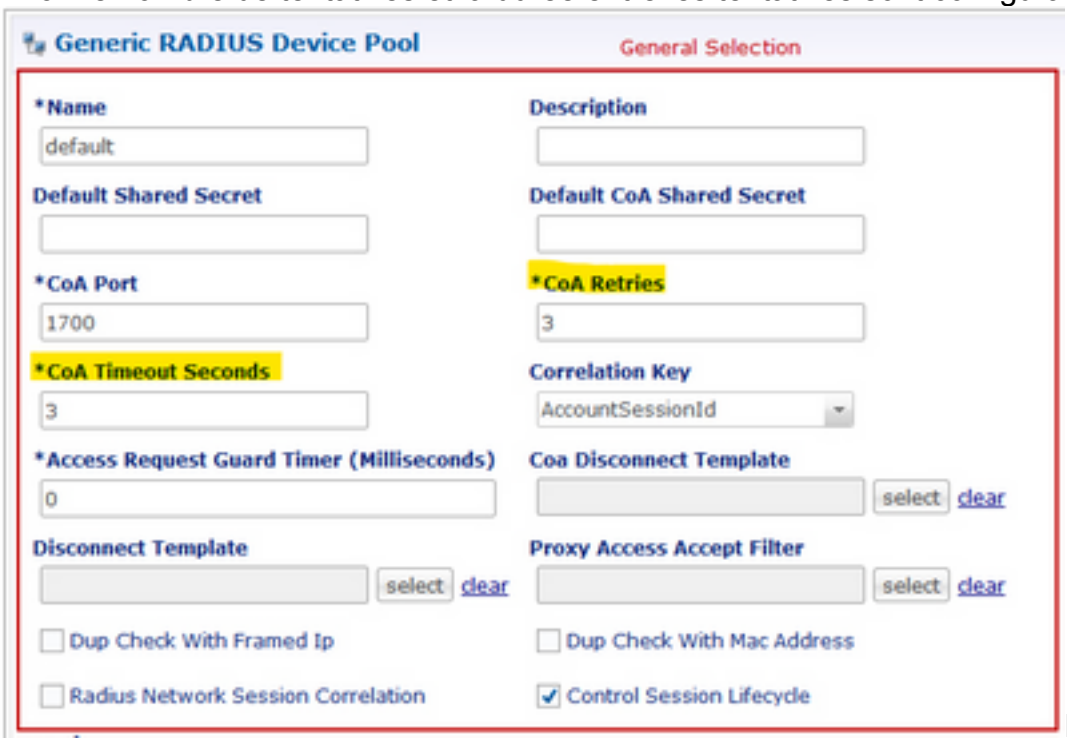
Note: Le premier paquet est reçu sans accusé de réception par le périphérique homologue (ASR9K), d'où la logique interne dans CPS qui déclenche un mécanisme de nouvelle tentative et envoie des requêtes en double.

Étape 4. L'observation est que CPS abandonne toute autre action de mise à jour de session, car il n'y a aucune réponse pour la première demande d'COA de session et ses nouvelles tentatives.

Avec cela, vous pouvez voir que la session PPPoE est toujours active à ASR9K et qu'aucune demande de déconnexion de session n'a été envoyée à CPS pour l'actualisation de la session. CPS attend une demande d'arrêt de comptabilité de ASR9K en ce qui concerne la demande de certificat d'authenticité.

Principaux points à relever en ce qui concerne le certificat d'authenticité et ses départs

1. CPS lance des demandes d'ACO pour toutes les sessions actives/existantes dans sa base de données pour un abonné particulier.
2. Si CPS ne reçoit pas ACK ou NACK pour une demande de certificat d'authenticité particulière, il lance un mécanisme de nouvelle tentative basé sur la configuration dans le générateur de stratégies.
3. Le nombre de tentatives et la durée entre les tentatives sont configurables.



Exemple de configuration de nouvelle tentative

Solution

Pour résoudre ce problème, vous devez approfondir l'analyse vers ASR9K et trouver la raison pour laquelle aucune réponse n'a été apportée au CPS pour la demande de certificat d'authenticité et ses nouvelles tentatives.

Vous pouvez voir dans les traces de l'analyseur que l'équilibreur de charge (LB01) de CPS source

le certificat d'authenticité à partir de <IP-1> et achemine les paquets sur eth1, qui est la route par défaut.

L'autre équilibreur de charge (LB02) source le certificat d'authenticité à partir de <IP-2> et emprunte une route spécifique via eth2.

ASR9K possède la liste de contrôle d'accès (ACL) pour accepter le certificat d'authenticité uniquement s'il provient de <IP-2> et non de <IP-1>.

Vous devez donc corriger la table de routage à LB01 de CPS pour envoyer le certificat d'authenticité avec l'adresse IP source appropriée, c'est-à-dire <IP-2> via une route spécifique.

Vous pouvez voir ici la transaction RADIUS de bout en bout réussie pour un changement d'abonnement, après correction nécessaire à la table de routage CPS LB.