

# CPAR AAA Configuration

## Contents

[Introduction](#)

[Background Information](#)

[CPAR Configuration](#)

[Global Configuration](#)

[Client Configuration](#)

[Fast Rules Configuration](#)

[Services Configuration](#)

[Remote Servers Configuration](#)

[Session Manager](#)

[Resource Manager](#)

[Scripts](#)

[CPAR Logging Configuration](#)

[Timeout Values](#)

[Diameter Packet Size](#)

[Manage Sessions in CPAR](#)

[Attributes \(AVP\) Cached at CPAR AAA for Subscriber Sessions](#)

[Verify](#)

[Troubleshoot](#)

## Introduction

This document describes the procedure on Cisco Prime Access Registrar's (CPAR) Authentication, Authorization and Accounting (AAA) Configuration.

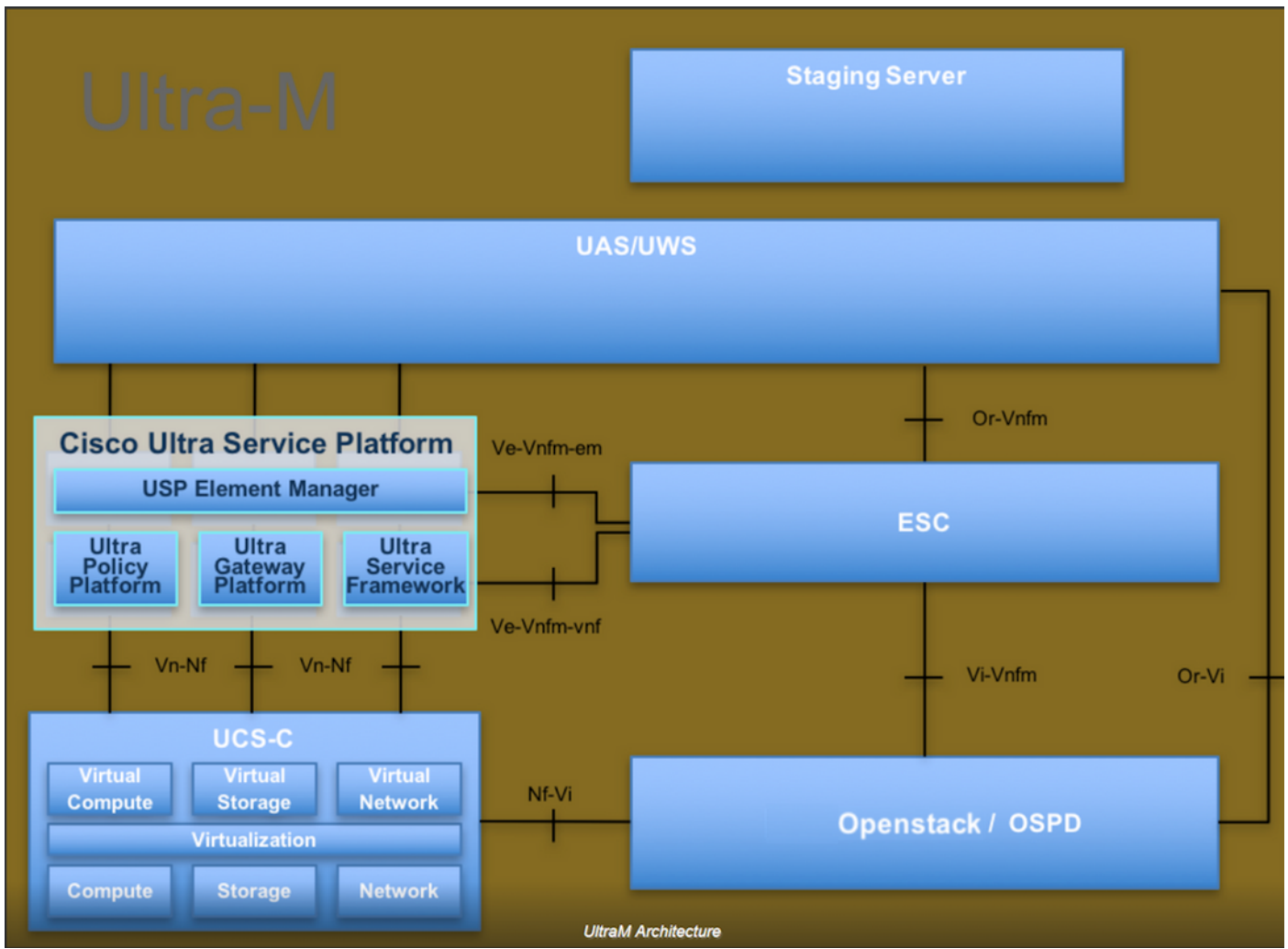
This procedure applies for an Openstack environment using NEWTON version where ESC is not managing CPAR and CPAR is installed directly on the VM deployed on Openstack.

## Background Information

Ultra-M is a pre-packaged and validated virtualized mobile packet core solution that is designed in order to simplify the deployment of VNFs. OpenStack is the Virtualized Infrastructure Manager (VIM) for Ultra-M and consists of these node types:

- Compute
- Object Storage Disk - Compute (OSD - Compute)
- Controller
- OpenStack Platform - Director (OSPD)

The high-level architecture of Ultra-M and the components involved are depicted in this image:



This document is intended for Cisco personnel who are familiar with Cisco Ultra-M platform and it details the steps required to be carried out at OpenStack and Redhat OS.

**Note:** Ultra M 5.1.x release is considered in order to define the procedures in this document.

## CPAR Configuration

### Global Configuration

The Diameter Global configuration is to be configured with appropriate values, like the Application-ID's and the origin Host IP-Address, Realm, etc.,

```
Cd /Radius/Advanced/Diameter/
Diameter/
```

```
IsDiameterEnabled = TRUE
General/
  Product = CPAR
  Version = 7.3.0.3
  AuthApplicationIdList = 1:5:16777264:16777265:16777272:16777250
  AcctApplicationIdList = 3
TransportManagement/
  Identity = aaa01.aaa.epc.mncxx.mccxx.3gppnetwork.org
  Realm = epc.mncxx.mccxx.3gppnetwork.org
  WatchdogTimeout = 500
```

```
ValidateIncomingMessages = FALSE
ValidateOutgoingMessages = TRUE
MaximumNumberOfDiameterPackets = 8192
ReserveDiameterPacketPool = 0
DiameterPacketSize = 4096
AdvertisedHostName/
    1. aaa01.aaa.epc.mncxx.mccxx.3gppnetwork.org
```

/etc/hosts has to be updated with the corresponding IP-Address to be resolved for the AAA Identity Fully Qualified Domain Name (FQDN) used in Transport management and Hostname to be resolved

## Client Configuration

The client configuration is to be configured with the Diameter peers where the traffic is received, in this case DRA.

```
Cd /Radius/Clients/
DRA01/
    Name = DRA01
    Description =
    Protocol = diameter
    HostName = x.x.x.x
    PeerPort = 3868
    Vendor =
    IncomingScript~ =
    OutgoingScript~ =
    AdvertisedHostName =
    UserLogEnabled = FALSE
    AdvertisedRealm =
    InitialTimeout = 3000
    MaxIncomingRequestRate = 0
    KeepAliveTime = 0
    AuthSessionStateInASR = No-State-Maintained
    SCTP-Enabled = FALSE
    TLS-Enabled = FALSE
```

## Fast Rules Configuration

FastRules is used to map the corresponding service in runtime based on certain condition, the condition is based on the Attributed Value Pairs (AVP) and its values present in the diameter message, if no fast rules matched it selects the Default service.

```
Cd /Radius/FastRules/
FastRules/
    RuleDefinitions/
        Entries 1 to 5 from 5 total entries
        Current filter: <all>
        r1/
            Name = r1
            Description = Used for HSS initiated Flows
            Protocol = diameter
```

```
Condition = "1 OR 2"
Success = author(3gpp-reverse)
Failure = Rule(r2)
Attributes/
    Entries 1 to 2 from 2 total entries
    Current filter: <all>

    1/
        Name = 1
        Description =
        Dictionary = environment
        Attribute = Diameter-Command-Code
        Value = 304
    2/
        Name = 2
        Description =
        Dictionary = environment
        Attribute = Diameter-Command-Code
        Value = 305
r2/
Name = r2
Description = Used for PGW Update procedure over S6b
Protocol = diameter
Condition = "1 AND 2"
Success = author(s6b)
Failure = Rule(r3)
Attributes/
    Entries 1 to 2 from 2 total entries
    Current filter: <all>

    1/
        Name = 1
        Description =
        Dictionary = Request
        Attribute = Auth-Application-Id
        Value = 16777272
    2/
        Name = 2
        Description =
        Dictionary = request
        Attribute = Diameter-Command-Code
        Value = 265
r3/
Name = r3
Description = OPTIONAL used for PGW Termination procedure
Protocol = diameter
Condition = "1 and 2"
Success = author(null)
Failure = Rule(r4)
Attributes/
    Entries 1 to 2 from 2 total entries
    Current filter: <all>

    1/
        Name = 1
        Description =
        Dictionary = Request
        Attribute = Auth-Application-Id
        Value = 16777272
    2/
        Name = 2
        Description =
        Dictionary = environment
        Attribute = Diameter-Command-Code
```

```

Value = 275
r4/
Name = r4
Description = Used for SWm Termination procedure
Protocol = diameter
Condition = "1 and 2"
Success = author(3gpp-auth)
Failure = Rule(r5)
Attributes/
  Entries 1 to 2 from 2 total entries
  Current filter: <all>
  1/
    Name = 1
    Description =
    Dictionary = request
    Attribute = Auth-Application-Id
    Value = 16777264
  2/
    Name = 2
    Description =
    Dictionary = environment
    Attribute = Diameter-Command-Code
    Value = 275
r5/
Name = r5
Description = Used for SWm ReAuthorization
Protocol = diameter
Condition = "1 and 2"
Success = Query(query)
Failure =
Attributes/
  Entries 1 to 2 from 2 total entries
  Current filter: <all>
  1/
    Name = 1
    Description =
    Dictionary = environment
    Attribute = Diameter-Command-Code
    Value = 265
  2/
    Name = 2
    Description =
    Dictionary = request
    Attribute = Auth-Application-Id
    Value = 16777264
Order/
  Radius/
  Diameter/
    1. r1
  Tacacs/

```

If none of the above FastRules matched, the packet is processed as per Default Service.

```

Cd /Radius/
DefaultAuthenticationService~ = encrypted-imsi-service
DefaultAuthorizationService~ = 3gpp-auth

```

## Services Configuration

Service Configuration is where service are defined as per authentication, authorization requirement:

## Cd /Radius/Services/

Encrypted-IMSI-Service is used for EAP-AKA authentications and with IMSI encrypted for Apple devices. If not required, set the EncryptedIMSI parameter to **False**

```
encrypted-imsi-service/  
    Name = encrypted-imsi-service  
    Description =  
    Type = eap-aka  
    NumberOfQuintets = 1  
    AlwaysRequestIdentity = True  
    EnableIdentityPrivacy = False  
    EnableRollingPseudonymSecret = False  
    PseudonymSecret = <encrypted>  
    PseudonymRenewtime = "24 Hours"  
    PseudonymLifetime = Forever  
    NotificationService =  
    Generate3GPPCompliantPseudonym = False  
    EnableReauthentication = False  
    UseOutagePolicyForReauth = False  
    MaximumReauthentications = 16  
    ReauthenticationTimeout = 3600  
    ReauthenticationRealm =  
    EnableEncryptedIMSI = True  
    EncryptedIMSIDelimiter = NULL  
    EncryptedIMSIKeyIdDelimiter = ,  
    DefaultPrivateKey = xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx  
    QuintetCacheTimeout = 0  
    AuthenticationTimeout = 120  
    QuintetGenerationScript~ =  
    UseProtectedResults = False  
    SendReAuthIDInAccept = False  
    Subscriber_DBLookup = DiameterDB  
    DiameterInterface = SWx  
    ProxyService = dia-proxy
```

The 3GPP service is used for Registration/Profiledownload from HSS over SWx;

```
3gpp-auth/  
    Name = 3gpp-auth  
    Description =  
    Type = 3gpp-authorization  
    Protocol = diameter  
    IncomingScript~ =  
    OutgoingScript~ = removeuserdata  
    SessionManager = sm1  
    DiameterProxyService = dia-proxy  
    FetchLocationInformation = False
```

The dia-proxy service is used to select the remoteserver and can define peer policy, the GroupFailover option is used as MultiplePeerPolicy, when there are multiple remote peers and wants to group the same. Also, define the GroupTimeOutPolicy to Failover to multiple groups

```
dia-proxy/
```

```

Name = dia-proxy
Description =
Type = diameter
IncomingScript~ = rmserver
OutgoingScript~ =
MultiplePeersPolicy = GroupFailover
GroupTimeOutPolicy = FailOver
ServerGroups/
    Entries 1 to 2 from 2 total entries
    Current filter: <all>

    Group_Primary_DRA/
        Name = Group_Primary_DRA
        Metric = 0
        IsActive = TRUE
    Group_Secondary_DRA/
        Name = Group_Secondary_DRA
        Metric = 1
        IsActive = TRUE

```

The above mentioned ServerGroups are defined in **/Radius/GroupServers/**

```
GroupServers/
```

```

Entries 1 to 2 from 2 total entries
Current filter: <all>

```

```
Group_Primary_DRA/
```

```

Name = Group_Primary_DRA
Description =
MultiplePeersPolicy = RoundRobin
PeerTimeOutPolicy = FailOver
DiaRemoteServers/
    Entries 1 to 2 from 2 total entries
    Current filter: <all>

```

```
DRA01/
```

```

Name = DRA01
Metric = 0
Weight = 0
IsActive = TRUE

```

```
DRA02/
```

```

Name = DRA02
Metric = 1
Weight = 0
IsActive = TRUE

```

```
Group_Secondary_DRA/
```

```

Name = Group_Secondary_DRA
Description =
MultiplePeersPolicy = RoundRobin
PeerTimeOutPolicy = FailOver
DiaRemoteServers/
    Entries 1 to 4 from 4 total entries
    Current filter: <all>

```

```
DRA03/
```

```

Name = DRA03
Metric = 0
Weight = 0
IsActive = TRUE

```

```
DRA04/
```

```
Name = DRA04
```

```

Metric = 2
Weight = 0
IsActive = TRUE

DRA05/

Name = DRA05
Metric = 1
Weight = 0
IsActive = TRUE
```

The S6b service is used to process the PGW Update procedure over S6b.

```
s6b/

Name = s6b
Description =
Type = 3gpp-authorization
Protocol = diameter
IncomingScript~ =
OutgoingScript~ =
SessionManager =
DiameterProxyService = dia-proxy
FetchLocationInformation = False
```

The 3gpp-reverse is used for HSS initiated messages to be processed.

```
3gpp-reverse/

Name = 3gpp-reverse
Description =
Type = 3gpp-reverse-authorization
IncomingScript~ = AAARTRCheck
OutgoingScript~ =
SessionManager = sm1
TranslationService =
```

The query service is used during the Re-Authorization procedure where to directly get the updated profile from cache based on the PPR received from HSS.

```
query/

Name = query
Description =
Type = diameter-query
IncomingScript~ =
OutgoingScript~ = removeuserdataquery
UpdateSessionLastAccessTime = False
SessionManagersToBeQueried/
    1. sm1
AttributesToBeReturned/
    1. Non-3GPP-User-Data
    2. Service-Selection
```

The null service is to just reply with a success for S6b Termination process as there is no session cached over S6b.

```
null/

Name = null
Description =
Type = null
IncomingScript~ =
OutgoingScript~ =
```



## Remote Servers Configuration

Remoteservers are defined with remote peer to which packets are sent from AAA like the HSS. If DRA is used, then define the same DRA info in both Clients and RemoteServers;

```
RemoteServers/
```

```
    DRA01/
```

```
        Name = DRA01
        Description =
        Protocol = diameter
        HostName = 10.169.48.235
        DestinationPort = 3868
        DestinationRealm = epc.mnc300.mcc310.3gppnetwork.org
        ReactivateTimerInterval = 300000
        Vendor =
        IncomingScript~ = AAAReplaceResultCode
        OutgoingScript~ = rmdh
        MaxTries = 3
        MaxTPSLimit = 0
        MaxSessionLimit = 0
        InitialTimeout = 3000
        LimitOutstandingRequests = FALSE
        MaxPendingPackets = 0
        MaxOutstandingRequests = 0
        DWatchDogTimeout = 2500
        SCTP-Enabled = FALSE
        TLS-Enabled = FALSE
        AdvertiseHostName =
        AdvertiseRealm =
```

## Session Manager

Session Manager is to define about the session caching, it works conjunction with Resource manager. The session manager is referred in 3gpp-auth, 3gpp-reverse and query services;

```
Cd /Radius/SessionManagers/
```

```
sm1/
```

```
    Name = sm1
    Description =
    Type = local
    EnableDiameter = True
    IncomingScript =
    OutgoingScript =
    AllowAccountingStartToCreateSession = FALSE
    SessionTimeOut =
    PhantomSessionTimeOut =
    SessionKey = User-Name:Session-Id
    SessionCreationCmdList = 268||305
    SessionDeletionCmdList = 275
    SessionRestorationTimeOut = 24h
    ResourceManagers/
        1. 3gpp
```

2. swmcache
3. per-user

## Resource Manager

Resource managers are defined to allocate the resources and mapped to session managers.

These three resource managers are used.

```
Cd /Radius/ResourceManagers/
ResourceManagers/
    3gpp/
        Name = 3gpp
        Description =
        Type = 3gpp
        EnableRegistrationFlow = TRUE
        EnableSessionTermination = false
        ReuseExistingSession = True
        HSSProxyService = dia-proxy

Per-User/
        Name = Per-User
        Description =
        Type = user-session-limit
        UserSessionLimit = 0

swmcache/
        Name = swmcache
        Description =
        Type = session-cache
        OverwriteAttributes = FALSE
        QueryKey = Session-Id
        PendingRemovalDelay = 10
        AttributesToBeCached/
            1. Non-3GPP-User-Data
            2. Service-Selection
        QueryMappings/
```

## Scripts

This table displays all the scripts used during the packets processing.

Name	Script file	Entry Point	Description
Clid	test.tcl	clid	Looks for the Application-Id 16777264 and the Diameter-Command Code 268, gets the username value, and copies it into the calling-station-ID attribute from the arriving request. This script is referred in Radius Incoming scriptpoint
rmserver	test.tcl	rm_server	Looks for the Server-Assignment-Type attribute, if it exists removes Remote-Server field from the incoming request. This script is referred in dia-proxy service Incoming scriptpoint
removeuserdata	libremoveuserdata.so	removeUserData	Rex script is used to first check the received info from HSS especially the

'Non-3GPP-IP-Access' and 'Non-3GPP-IP-Access-APN' both should be having the value 'NON\_3GPP\_SUBSCRIPTION\_ALLOWED (0)' and 'Non\_3GPP\_APNS\_ENABLE (0)' else it will fail the authorization.

Followed by a simple comparison of APN name received from SWm DER message(service-selection AVP) with the APN configuration downloaded from HSS, if there is a match it copies only the specific APN details and remove the unwanted AVPs and prepare the final DEA towards the ePDG. If there is no match authorization fails and if there is no service-selection AVP in DER all the APN info is sent but as outer AVP.

This script is referred in 3gpp-auth Outgoing scriptinpoint Rex script is used to first check the received info from HSS especially the **Non-3GPP-IP-Access** and **Non-3GPP-IP-Access-APN** both should be having the value

**NON\_3GPP\_SUBSCRIPTION\_ALLOWED (0)** and

**Non\_3GPP\_APNS\_ENABLE (0)**

else it fails the authorization.

Followed by a simple comparison of APN name received from SWm DER message (service-selection AVP) with the APN configuration downloaded from HSS, if there is a match it copies only the specific APN details and remove the unwanted AVPs and prepare the final DEA towards the ePDG. If there is no match authorization fails and if there is no service-selection AVP in DER all the APN info is sent but as outer AVP.

This script is referred in query serviceOutgoing scriptinpoint Dia proxy service incoming script – used to unset the sticky for the messages which are already processed. For ex; if MAR/MAA is received from DRA1, the subsequent user SAR will use the same DRA1 and if it's not available and sticky is

removeuserdataquery libremoveuserdataquery removeUserData  
.so

out

test.tcl

newsessionState

rmdh	test.tcl	rmdh	maintained, it does not failover. In-order to failover to alternate DRA this sticky is to be removed. The script is used to remove the Visited-Network-Identifier towards S6b SAR(PGW_update) HSS. Removes DestinationHost AVP in packets with DiameterCode 301 and 303.
rmvnid	test.tcl	rmvnid	Removes Visited-Network-Identifier AVP in packets with DiameterCode 256 and the Server-Assignment-Type is 13.
AAAReplaceResultCode	test.tcl	replaceResultCode	Replace Result-Code AVP with "Test" in packets with DiameterCode 274 and Result-Code "Diameter-Unknown-Session-Id"
AAARTRCheck	librexblockRTR.so	AAARTRCheck	When multiple RTR are received for same session, duplicate ones will be deleted and logged.

Some of the scripts may not be required in higher version, the scripts listed out is to be used in CPAR version 7.3.0.3

All the scripts are located in the path `/opt/CSCOAr/scripts/radius/`.

## CPAR Logging Configuration

The folder `/opt/CSCOAr/logs` stores all the application logs. The file `name_radius_1_log` registers all dropped and rejected requests, so it is important to store this file for troubleshooting purposes.

CPAR allows a very flexible configuration to store this log according to your needs. Based on the requirement this value can be defined, here the latest 20 log files are kept, each file with a size of 5 Mb.

To enable this specific logging 2 parameters must be configured in the aregcmd mode:

`/Radius/Advanced`

`LogFileSize = "5 Megabytes"`

`LogFileCount = 20`

Log naming convention follows the rule specified in this table:

Description	Name of the log file
Latest log	<code>name_radius_1_log</code>
2nd to latest log	<code>name_radius_1_log.01</code>
3rd to latest log	<code>name_radius_1_log.02</code>

....  
20th to latest log

....  
name\_radius\_1\_log.19

## Table 2 Log Numbering.

# Timeout Values

CPAR has server configurable timeouts. The current setup has these configuration:

General timeouts located in /Radius/Advanced

- **DiameterStaleConnectionDeletionTimeOut** 300000 (ms) This timer indicated how long a diameter connection can be inactive before CPAR mark it as down.

Client timeouts located in /Radius/Clients/<client\_name>

- **InitialTimeout** 3000 (ms) Time waited for a reply from DRA before CPAR considers it unreachable.

Remote Server timeouts located in /Radius/RemoteServers/<remote\_server\_name>

- **InitialTimeout** 3000 (ms) Time waited for a reply from DRA before CPAR considers it unreachable.
- **DWatchDogTimeout** 2500 (ms) Time waited for a replay from DRA for DiameterWatchDog packet before CPAR considers it unreachable.
- **ReactivateTimerInterval** 300000 (ms) Time that CPAR will wait until retrying to establish a connection with a diameter peer.

# Diameter Packet Size

This document addresses the meaning of the Diameter Packet size command and the reasons that drove you to maintain this parameter to the value 4096.

<b>DiameterPacketSize</b>	<b>Required; the Diameter packet size that can be processed.</b> <b>An incoming Diameter packet with a packet size more than the value set in this field will be dropped.</b>
---------------------------	--

As explained in the above image, the maximum diameter packet size that CPAR expects to receive is 4096 bytes. This value is configured under **DiameterPacketSize** variable located in /Radius/Advanced/Diameter/TransportManagement directory. All the packets that do not comply with this value will be dropped. The total packet size is obtained after adding the size of session cached attributes plus the size of the diameter packet received.

For example, let us consider a PPR packet size of 4000 bytes and within that message Non-3GPP-User-Data has size of 3800 bytes. If the session has already cached some attributes and cached data size is 297 bytes, the session size exceeds 4096 bytes and the message is dropped by CPAR.

During the project and analysis of packets larger than 4096 was carried out. The results indicate that in average 36 packets (SAA) larger than 4096 arrive to each CPAR instance per day. These number of packets are not meaningful as it is very small.

This parameter is configurable and can be increased if needed. However, the value is increased beyond 4096 entails some drawbacks:

- If the DiameterPacketSize is increased to 5KB, CPAR will accept SAA packets larger than 4096 bytes. However, if PPR is initiated for the same user session, since the size of Non-3GPP-User-Data is 4260 bytes, the session update fails and leads to User Deregistration.
- DiameterPacketSize affects directly the startup memory allocated to the radius process. The larger the DiameterPacketSize the larger the amount of RES memory allocated to the Radius process at CPAR startup.

This image shows an example of the output of top command in an instance where DiameterPacketSize is configured to 4096:

```
[root@snqaaa07 ~]# top
top - 21:29:25 up 49 days, 20:21, 1 user, load average: 0.81, 0.28, 0.14
Tasks: 348 total, 1 running, 347 sleeping, 0 stopped, 0 zombie
%cpu(s): 2.8 us, 0.0 sy, 0.0 ni, 97.2 id, 0.0 wa, 0.0 hi, 0.0 si, 0.0 st
KiB Mem: 3277520 total, 5219052 used, 27558468 free, 1328 buffers
KiB Swap: 30408700 total, 0 used, 30408700 free. 2354304 cached Mem

  PID USER      PR  NI  VIRT  RES  SHR S %CPU %MEM    TIME+  COMMAND
16721 root        20   0 18.726g 174648 10608 S 100.1  0.5   1:07.34 radius
```

If the DiameterPackerSize parameter is increased to 6000 the output of the top command looks like this:

```
top - 22:57:50 up 49 days, 21:49, 1 user, load average: 1.00, 1.01, 1.00
Tasks: 348 total, 1 running, 347 sleeping, 0 stopped, 0 zombie
%cpu(s): 2.8 us, 0.0 sy, 0.0 ni, 97.2 id, 0.0 wa, 0.0 hi, 0.0 si, 0.0 st
KiB Mem: 3277520 total, 5383328 used, 27394192 free, 1328 buffers
KiB Swap: 30408700 total, 0 used, 30408700 free. 2355000 cached Mem

  PID USER      PR  NI  VIRT  RES  SHR S %CPU %MEM    TIME+  COMMAND
18455 root        20   0 18.741g 210788 10756 S 100.1  0.6   87:00.67 radius
```

- Besides to the startup memory allocation, once the system is in use, there is an internal dynamic memory buffer that grows in relation to how many packets are hitting CPAR. If for example 1000 packets hit CPAR at one point, CPAR allocates internally in the buffer 1000 \* DiameterPacketSize worth of memory, regardless of the size of the individual packets (CPAR knows that the DiameterPacketSize indicates the maximum packet size). This internal memory buffer allocates more memory if DiameterPacketSize is incremented and less memory if it is decremented.

It is recommended to maintain this parameter as 4096, as it was decided that the number of packets larger than 4096 are negligible and the drawbacks would pose unwanted behavior.

## Manage Sessions in CPAR

The only mechanism that exists in CPAR to monitor the number of sessions is through the method

explained in this document. There is no OID than can be retrieved via SNMP that contains this information.

CPAR is capable of managing sessions, enter the CPAR CLI with `/opt/CSCOAr/bin/aregcmd` and login with administrator credentials.

With the command `count-sessions /r all` CPAR shows all the sessions attached to it at that moment.

```
--> count-sessions /r all
Total 3 session(s) in /Radius/SessionManagers
```

To see more information of the session(s) CPAR has the command `query-sessions /r all` which gives the information of all the sessions attached to CPAR.

```
--> query-sessions /r all
Sessions for /Radius:
Sessions For /Radius/SessionManagers/sml:
S5 Key: 310310990007655@nat.epc.mcc310.mcc310.3gppnetwork.org:epgchi01.03.epdg.epc.mnc300.mcc310.3gppnetwork.org:1522864003;537746744;100, NAS: 10.169.48.75, NAS-Port: 0, User-Name: 310310990007655, Time: 00:28:10, USL: 1, Session-Id: epgchi01.03.epdg.epc.mnc300.mcc310.3gppnetwork.org:1522864003;537746744;100, Auth-Application-Id: 16777264, Service-Selection: ims, User-Name: 310310990007655@nat.epc.mnc310.mcc310.3gppnetwork.org, Origin-Realm: epc.mnc300.mcc310.3gppnetwork.org, Origin-Host: epgchi01.03.epdg.epc.mnc300.mcc310.3gppnetwork.org
S6 Key: 310310990007618@nat.epc.mnc310.mcc310.3gppnetwork.org:epgchi01.06.epdg.epc.mnc300.mcc310.3gppnetwork.org:1522864820;940397039;100, NAS: 10.169.48.238, NAS-Port: 0, User-Name: 310310990007618, Time: 00:14:34, USL: 1, Session-Id: epgchi01.06.epdg.epc.mnc300.mcc310.3gppnetwork.org:1522864820;940397039;100, Auth-Application-Id: 16777264, Service-Selection: ims, User-Name: 310310990007618@nat.epc.mnc310.mcc310.3gppnetwork.org, Origin-Realm: epc.mnc300.mcc310.3gppnetwork.org, Origin-Host: epgchi01.06.epdg.epc.mnc300.mcc310.3gppnetwork.org
S7 Key: 310310990007547@nat.epc.mnc310.mcc310.3gppnetwork.org:epgchi21.epdg.epc.mnc300.mcc310.3gppnetwork.org:1495425783;2890;08002a36040180010100000000, NAS: 10.169.48.78, NAS-Port: 0, User-Name: 310310990007547, Time: 00:07:04, USL: 1, Session-Id: epgchi21.epdg.epc.mnc300.mcc310.3gppnetwork.org:1495425783;2890;08002a36040180010100000000, Auth-Application-Id: 16777264, Service-Selection: ims, User-Name: 310310990007547@nat.epc.mnc310.mcc310.3gppnetwork.org, Origin-Realm: epc.mnc300.mcc310.3gppnetwork.org, Origin-Host: epgchi21.epdg.epc.mnc300.mcc310.3gppnetwork.org
S11 Key: 310310990005644@nat.epc.mnc310.mcc310.3gppnetwork.org:epgchi21.epdg.epc.mnc300.mcc310.3gppnetwork.org:1495425783;2894;08008a10501800101000000000, NAS: 10.169.48.235, NAS-Port: 0, User-Name: 310310990005644, Time: 00:01:16, USL: 1, Session-Id: epgchi21.epdg.epc.mnc300.mcc310.3gppnetwork.org:1495425783;2894;08008a10501800101000000000, Auth-Application-Id: 16777264, Service-Selection: ims, User-Name: 310310990005644@nat.epc.mnc310.mcc310.3gppnetwork.org, Origin-Realm: epc.mnc300.mcc310.3gppnetwork.org, Origin-Host: epgchi21.epdg.epc.mnc300.mcc310.3gppnetwork.org
```

To just show the information of a specific session, the command can be changed and use the USER value, i.e.: `query-sessions /r with-User 310310990007655`

```
--> query-sessions /r with-user 310310990007655
Sessions with-user 310310990007655 for /Radius:
Sessions For /Radius/SessionManagers/sml:
S5 Key: 310310990007655@nat.epc.mnc310.mcc310.3gppnetwork.org:epgchi01.03.epdg.epc.mnc300.mcc310.3gppnetwork.org:1522864003;537746744;100, NAS: 10.169.48.75, NAS-Port: 0, User-Name: 310310990007655, Time: 00:30:22, USL: 1, Session-Id: epgchi01.03.epdg.epc.mnc300.mcc310.3gppnetwork.org:1522864003;537746744;100, Auth-Application-Id: 16777264, Service-Selection: ims, User-Name: 310310990007655@nat.epc.mnc310.mcc310.3gppnetwork.org, Origin-Realm: epc.mnc300.mcc310.3gppnetwork.org, Origin-Host: epgchi01.03.epdg.epc.mnc300.mcc310.3gppnetwork.org
```

This list contains all the possible filters for `query-sessions` command:

- All
- with-ID
- with-NAS
- with-User
- with-Key
- with-Age+
- with-Attribute.

Finally, to detach sessions from CPAR, use the command `release-sessions /r all`, and all the sessions attached to that moment are detached.

```
--> release-sessions /r all
Released 4 session(s) in /Radius/SessionManagers
```

A filter can be applied to detach a specific session.

## Attributes (AVP) Cached at CPAR AAA for Subscriber Sessions

Prime Access Registrar supports attribute caching at Session Managers that can be used to query data. This Diameter-query service contains a list of session managers to be queried from and a list of (cached) attributes to be returned in the Access-Accept packet in response to a DIAMETER Query request. This is initiated through an extension point script or through the Rule and Policy Engine by setting it to a new environment variable named Query-Service.

The DIAMETER Query service should be selected through an extension point script or through the Rule and Policy Engine by setting it to a new environment variable named Query-Service. The reason for this is that the DIAMETER Query request comes in as an Access-Request and the server has no way of knowing whether it is a DIAMETER Query request or normal authentication request. Setting the Query-Service environment variable tells the Prime Access Registrar server that the request is a DIAMETER Query request so the Prime Access Registrar server can process the request with the diameter-query service set in the Query-Service environment variable.

When a DIAMETER Query service is selected to process an Access-Request, it queries the configured list of Session Managers for a matching record using the QueryKey value configured in the session-cache Resource Manager referenced under these Session Managers as key. If a matching record is found, an Access-Accept containing a list of cached attributes present (based on the configuration) in the matched record is sent back to the client. If the session cache contains a multivalued attribute, all values of that attribute are returned in the response as a multivalued attribute. If there is no matching record, an Access-Reject packet is sent to the client.

Prime Access Registrar introduces scripting points at the Session Manager level along with automated programmable interfaces (APIs) to access cached information present in the session record. You can use these scripting points and APIs to write extension point scripts to modify the cached information.

At this moment, our deployment has no written scripts or makes use of programmable APIs to access such data but the option is there.

The attributes that our session manager stores at the moment are:

Hardcoded at /radius/resourcemanagers/swmcache/AttributesToBeCached:

- Non-3GPP-User-Data
- Service-Selection

By Default:

- User-Name (IMSI)
- Origin-Host
- Auth-Application-Id
- Origin-Realm
- Session-Id



Such attributes are visible per session when this command **query-sessions** is used on CLI.

## **Verify**

There is currently no verification procedure available for this configuration.

## **Troubleshoot**

There is currently no specific troubleshooting information available for this configuration.