

# 排除AAAAccSrvUnreachable和AAAAuthSrvUnreachable陷阱故障

## 目錄

[簡介](#)

[陷阱觸發器](#)

[aaamgr流程方法中的連續故障](#)

[Keepalive方法](#)

[故障排除命令/方法](#)

[Radius組態基本資訊](#)

[show task resources facility aaamgr all](#)

[show radius counters {all |伺服器}](#)

[show session subsystem facility {aaamgr | sessmgr} {all |例項](#)

[ping](#)

[traceroute](#)

[radius測試例項x auth {radius group](#)

[radius測試例項x記帳{radius組](#)

[show radius info \[radius group](#)

[監控使用者](#)

[封包擷取](#)

[補救](#)

[最終示例](#)

[相關思科支援社群討論](#)

SNMPAAAAccSrvUnreachableAAAAuthSrvUnreachable(RADIUS)

RESULTradius//

IP

//radius

## aaamgr

aaamgraaamgrradiusradiusaaamgrsessmgrshow task resourcesaaamgraaamgrradiusaaamgr — show radius countersAccess-Request Timeout

Access-Request Current Consequential Failures in a mgrshow radius countersshow radius accounting(or authentication)servers detailradiusActiveNot RespondingSNMP radius

[source]PDSN> show radius accounting servers detail  
Friday November 28 23:23:34 UTC 2008

```
+-----Type:          (A) - Authentication   (a) - Accounting
|                    (C) - Charging       (c) - Charging Accounting
|                    (M) - Mediation      (m) - Mediation Accounting
|
|+-----Preference:  (P) - Primary           (S) - Secondary
||
||+----State:        (A) - Active           (N) - Not Responding
|||                 (D) - Down             (W) - Waiting Accounting-On
|||                 (I) - Initializing    (w) - Waiting Accounting-Off
|||                 (a) - Active Pending  (U) - Unknown
|||
|||+--Admin          (E) - Enabled           (D) - Disabled
|||  Status:
|||
|||+--Admin
|||  status          (O) - Overridden      (.) - Not Overridden
|||  Overridden:
|||
vvvvv IP              PORT GROUP
-----
PNE. 198.51.100.1    1813 default
```

Event History:  
2008-Nov-28+23:18:36 Active  
2008-Nov-28+23:18:57 Not Responding  
2008-Nov-28+23:19:12 Active  
2008-Nov-28+23:19:30 Not Responding  
2008-Nov-28+23:19:36 Active  
2008-Nov-28+23:20:57 Not Responding  
2008-Nov-28+23:21:12 Active  
2008-Nov-28+23:22:31 Not Responding  
2008-Nov-28+23:22:36 Active  
2008-Nov-28+23:23:30 Not Responding

如果此計數器達到配置的值（預設值= 4），並且從未被重置，則按可配置方式：(請注意，方括弧[]用於表示可選的限定符，並在這些情況下捕獲故障排除記帳（如果未指定記帳，則預設使用身份驗證）

radius [accounting] detect-dead-server consecutive-failures 4

然後此伺服器在配置的時間（分鐘）內標籤為「關閉」：

radius [accounting] deadtime 10

SNMP陷阱和日誌也會被觸發，例如分別用於身份驗證和/或記帳：

```
Fri Jan 30 06:17:19 2009 Internal trap notification 39 (AAAASvrUnreachable) server 2 ip
address 172.28.221.178
Fri Jan 30 06:22:19 2009 Internal trap notification 40 (AAAASvrReachable) server 2 ip address
172.28.221.178

Fri Nov 28 21:59:12 2008 Internal trap notification 42 (AAAASvrUnreachable) server 6 ip
address 172.28.221.178
Fri Nov 28 22:28:29 2008 Internal trap notification 43 (AAAASvrReachable) server 6 ip address
172.28.221.178
```

```
2008-Nov-28+21:59:12.899 [radius-acct 24006 warning] [8/0/518 <aaamgr:231> aaamgr_config.c:1060]
[context: source, contextID: 2] [software internal security config user critical-info] Server
172.28.221.178:1813 unreachable
```

```
2008-Nov-28+22:28:29.280 [radius-acct 24007 info] [8/0/518 <aaamgr:231> aaamgr_config.c:1068]
[context: source, contextID: 2] [software internal security config user critical-info] Server
172.28.221.178:1813 reachable
```

陷阱指示無法訪問伺服器。注意任何模式。例如，它是在一台伺服器、另一台伺服器還是在所有伺服器上發生？彈跳的頻率是多少？是連續發生還是偶爾發生？

另請注意，觸發此陷阱只需一台管理器發生故障，因此，此陷阱的棘手之處在於它並不指示問題的程度。它可能非常廣泛或非常微小——由操作員來確定，本文討論了如何找出這種方法。

show snmp trap statistics將報告自啟動以來觸發的次數，即使較舊的陷阱早已刪除。此範例顯示無法到達記帳的問題：

```
[source]PDSN> show snmp trap statistics | grep -i aaa
Wednesday September 10 08:38:19 UTC 2014
```

Trap Name	#Gen	#Disc	Disable	Last Generated
AAAAccSvrUnreachable	833	0	0	2014:09:10:08:36:54
AAAAccSvrReachable	839	0	0	2014:09:10:08:37:00

請注意，上述示例中報告的aaamgr為#231。這是位於系統管理卡(SMC)上的ASR 5000上的管理管理器。此輸出中的欺騙性在於，當單個aaamgr或aaamgr遇到可訪問性問題時，日誌中報告的例項編號是管理aaamgr例項，而不是遇到問題的特定例項。這是因為如果許多例項遇到可訪問性問題，那麼如果所有例項都這樣報告，則日誌記錄將很快填滿，因此設計是泛泛地報告管理例項，如果不知道這一點，則無疑將是欺騙性的。在故障排除部分中，將提供有關如何確定哪些aamr發生故障的詳細資訊。從StarOS 17和v18+的某些版本開始，此行為已更改，因此具有連線問題的對應的aaamgr例項編號（如SNMP陷阱中報告的）在使用特定ID(Cisco CDETS CSCum84773)的日誌中報告，儘管仍然只報告第一次出現此情況（跨多個陣列）。

管理aamgr是最大sessmgr例項編號+ 1，因此，在ASR 5500中，資料處理卡(DPC)為385，而DPC 2為1153。

作為說明，管理管理員負責處理操作員/管理員登入，以及處理從RADIUS伺服器本身發起的授權請求更改。

繼續操作時，「show radius accounting(or authentication)servers detail」命令將指示與陷阱/日誌對應的狀態更改為「關閉」的時間戳(提醒：先前定義的「未響應」僅是一個管理器獲得超時，而「關閉」則是一個管理器獲得每個配置的足夠連續超時來觸發「關閉」)

```
vvvvv IP          PORT GROUP
-----
asDE. 172.28.221.178 1813 default
```

```
Event History:
2008-Nov-28+21:59:12      Down
2008-Nov-28+22:28:29      Active
2008-Nov-28+22:28:57      Not Responding
2008-Nov-28+22:32:12      Down
2008-Nov-28+23:01:57      Active
2008-Nov-28+23:02:12      Not Responding
```

2008-Nov-28+23:05:12	Down
2008-Nov-28+23:19:29	Active
2008-Nov-28+23:19:57	Not Responding
2008-Nov-28+23:22:12	Down

如果只配置了一個伺服器，則不會將其標籤為關閉，因為這對呼叫設定成功至關重要。

值得一提的是，detect-dead-server config line中可以配置另一個名為「response-timeout」的引數。如果指定，則僅當滿足連續失敗和響應超時條件時，才會將伺服器標籤為關閉。response-timeout指定了一段時間，在此時間段內不會收到對傳送到特定伺服器的所有請求的響應。（請注意，收到響應後，此計時器將持續重置。）當伺服器或網路連線完全關閉（而不是部分受損/降級）時，會出現這種情況。

這種情況的使用情形是流量突發導致連續故障觸發，但並不希望立即將伺服器標籤為關閉。相反，只有在經過特定時間段後伺服器才會被降級，此時不會收到任何響應，這實際上表示伺服器確實無法訪問。

剛剛討論的控制radius狀態機更改的方法依賴於檢視所有aamgr進程並查詢觸發了失敗重試條件的進程。該方法在一定程度上受故障隨機性的影響，可能不是理想的故障檢測演算法。但它特別擅長找到損壞的垃圾桶，而其他垃圾桶工作正常。

## Keepalive方法

檢測radius伺服器可達性的另一種方法是使用假的keepalive測試消息。這涉及持續傳送虛假radius訊息，而不是監控即時流量。此方法的另一個優點是它始終處於活動狀態，而與aamgr方法中的連續故障相比，AAMGR方法中可能存在不傳送radius流量的時段，因此無法知道這些時段期間是否存在問題，從而導致嘗試開始時的延遲檢測。此外，當伺服器被標籤為關閉時，也會繼續傳送這些keepalive資料包，以便伺服器可以儘快進行標籤。此方法的缺點在於它遺漏了與特定aaamgr例項相關的問題，這些例項可能遇到問題，因為它將管理aaamgr例項用於測試消息。

以下是與此方法相關的各種可設定專案：

```
radius (accounting) detect-dead-server keepalive
radius (accounting) keepalive interval 30
radius (accounting) keepalive retries 3
radius (accounting) keepalive timeout 3
radius (accounting) keepalive consecutive-response 1
radius (accounting) keepalive username Test-Username
radius keepalive encrypted password 2ec59b3188f07d9b49f5ea4cc44d9586
radius (accounting) keepalive calling-station-id 0000000000000000
radius keepalive valid-response access-accept
```

命令「radius(accounting)detect-dead-server keepalive」開啟keep-alive方法，而不是使用aamgr方法連續失敗。在上方範例中，系統每30秒傳送一則使用者名為Test-Username且密碼為Test-Username的測試訊息，如果沒有收到回應，則每3秒重試一次，最多重試3次，之後將伺服器標籤為關閉。一旦收到第一封回信，它會再次將它標籤出來。

以下是上述設定的身份驗證請求/響應示例：

```
<<<<OUTBOUND 17:50:12:657 Eventid:23901(6)
```

```
RADIUS AUTHENTICATION Tx PDU, from 192.168.50.151:32783 to 192.168.50.200:1812 (142) PDU-
dict=starent-vsai
```

```
Code: 1 (Access-Request)
Id: 16
Length: 142
Authenticator: 51 6D B2 7D 6A C6 9A 96 0C AB 44 19 66 2C 12 0A
  User-Name = Test-Username
  User-Password = B7 23 1F D1 86 46 4D 7F 8F E0 2A EF 17 A1 F3 BF
  Calling-Station-Id = 0000000000000000
  Service-Type = Framed
  Framed-Protocol = PPP
  NAS-IP-Address = 192.168.50.151
  Acct-Session-Id = 00000000
  NAS-Port-Type = HRPD
  3GPP2-MIP-HA-Address = 255.255.255.255
  3GPP2-Correlation-Id = 00000000
  NAS-Port = 4294967295
  Called-Station-ID = 00
```

```
INBOUND>>>> 17:50:12:676 Eventid:23900(6)
RADIUS AUTHENTICATION Rx PDU, from 192.168.50.200:1812 to 192.168.50.151:32783 (34) PDU-
dict=starent-vsai
```

```
Code: 2 (Access-Accept)
Id: 16
Length: 34
Authenticator: 21 99 F4 4C F8 5D F8 28 99 C6 B8 D9 F9 9F 42 70
  User-Password = testpassword
```

與aamgr方法中的連續故障一樣，使用相同的SNMP陷阱來表示無法到達/關閉以及可到達/開啟radius狀態：

```
Fri Feb 27 17:54:55 2009 Internal trap notification 39 (AAAAuthSvrUnreachable) server 1 ip
address 192.168.50.200
Fri Feb 27 17:57:04 2009 Internal trap notification 40 (AAAAuthSvrReachable) server 1 ip address
192.168.50.200
```

「show radius counters all」包含用於跟蹤身份驗證和記帳的keepalive請求的部分 — 以下是身份驗證計數器：

```
Server-specific Keepalive Auth Counters
-----
Keepalive Access-Request Sent: 33
Keepalive Access-Request Retried: 3
Keepalive Access-Request Timeouts: 4
Keepalive Access-Accept Received: 29
Keepalive Access-Reject Received: 0
Keepalive Access-Response Bad Authenticator Received: 0
Keepalive Access-Response Malformed Received: 0
Keepalive Access-Response Malformed Attribute Received: 0
Keepalive Access-Response Unknown Type Received: 0
Keepalive Access-Response Dropped: 0
```

## 故障排除命令/方法

現在已解釋了AAA無法到達陷阱的觸發因素，下一步是瞭解各種故障排除命令，用於確定影響並嘗試找出根本原因。「無法到達」是一個非常寬泛的術語。它沒有說明不可達性在網路、伺服器或ASR上的位置。例如，是否知道最初是否傳送了這些請求？伺服器是否收到請求？它是否對這些請求作出了回應。響應是否返回到ASR，如果是，它們是在內部路徑上處理或丟棄的（即流）。本節

嘗試介紹如何回答這些問題。

## Radius組態基本資訊

首先需要熟悉一些有關RADIUS配置的基礎知識。RADIUS的大部分配置都位於一個指定的組中，並且所有情景都有一個預設組，該組可如下配置。很多情況下，配置將只有一個組，即預設組。

```
[local]CSE2# config
[local]CSE2(config)# context aaa_ctx
[aaa_ctx]ASR5000(config-ctx)# aaa group default
[aaa_ctx]ASR5000(config-aaa-group)#
```

如果使用特定的命名aaa組，則使用者配置檔案或應用點名稱(APN) ( 取決於呼叫控制技術 ) 中配置的以下語句會指向這些組，例如：

```
subscriber name <subscriber name>
  aaa group <group name>
```

附註：系統首先檢查分配給訂戶的特定aaa組，然後檢查aaa組預設值以查詢未在特定組中定義的其他可配置項。

以下是總結分配給各種aaa組配置中的所有配置項的所有值的有用命令。這允許快速檢視包括預設值在內的所有可配置項，而無需手動檢查配置，可能有助於避免在設定某些設定時出錯。這些命令報告所有上下文：

```
show aaa group all
show aaa group name <group name>
```

當然，最重要的可設定是radius存取和記帳伺服器本身。以下是範例：

```
radius server 209.165.201.1 key testtesttesttest port 1645 priority 1 max-rate 5
radius server 209.165.201.2 key testtesttesttest port 1645 priority 2 max-rate 5
radius accounting server 209.165.201.1 key testtesttesttest port 1646 priority 1
radius accounting server 209.165.201.2 key testtesttesttest port 1646 priority 2
```

請注意max-rate功能，該功能限制每秒向伺服器傳送的請求數

此外，還需要定義NAS IP地址，這是從其中傳送radius請求和收到響應的情景中的介面上的IP地址。如果未定義，則不會傳送請求，並且監視器訂閱伺服器跟蹤可能無法發佈明顯的錯誤 ( 未傳送radius請求且未指示原因 ) 。

```
radius屬性nas-ip-address address 10.211.41.129
```

請注意，由於驗證和記帳通常由同一伺服器處理，因此會使用不同的連線埠號碼來區分RADIUS伺服器上的驗證和記帳流量。對於ASR5K端，未指定UDP源埠號，由機箱根據管理員選擇 ( 稍後將對此進行詳細說明 ) 。

通常為冗餘目的指定多個訪問和記帳伺服器。可以配置輪詢或優先順序：

```
radius [accounting]演算法{first-server |循環配置資源}
```

第一個伺服器選項會將ALL請求傳送到優先順序最低的伺服器。只有在發生重試失敗或更嚴重的情

況下，伺服器被標籤為關閉時，才會嘗試具有下一個優先順序的伺服器。有關下面的詳細資訊。

當傳送radius ( 記帳或訪問 ) 請求時，需要回覆。在超時時間內 ( 秒 ) 未收到回覆時：

```
radius [accounting] timeout 3
```

重新傳送請求至指定的次數：

```
radius [accounting] max-retries 5
```

這表示在嘗試的特定radius伺服器上，要求放棄之前，可以傳送合共max-retries + 1次的請求。這時，它會依序嘗試相同序列到下一個radius伺服器。如果每個伺服器已嘗試了max-retries + 1次，但沒有響應，則呼叫將被拒絕，假設到目前為止沒有其他故障原因。

例如，即使身份驗證和記帳由於所有伺服器超時而失敗，使用者也可以通過配置進行訪問，儘管商業部署不太可能實現以下功能：

```
radius allow [accounting] authentication-down
```

此外，還有可配置項，可限制特定請求在所有已配置伺服器中的絕對傳輸總數，這些項預設處於禁用狀態：

```
radius [accounting] max-transmissions 256
```

例如，如果設定為= 1，則即使有輔助伺服器，也不會嘗試它，因為只嘗試過一次特定使用者設定。

## show task resources facility aaamgr all

每個aaamgr進程與關聯的sessmgr進程 ( 負責整體呼叫處理 ) 配對並「適用於」，且位於不同的資料包服務卡(PSC)或資料處理卡(DPC)上，但使用相同的例項ID。此外，在此示例輸出中，請注意在ASR 5000的系統管理卡(SMC)上運行的特殊aamgr例項231(或ASR 5500(MIO)的管理輸入輸出卡)，該例項不會處理使用者請求，但不會用於radius測試命令 ( 有關更多詳細資訊，請參閱下一節 ) 和操作員CLI登入處理。

在此代碼片段中，位於PSC 13上的aamgr 107負責處理PSC 1上的配對sessmgr 107的所有RADIUS處理。aamgr 107的可達性問題會影響sessmgr 107上的呼叫。

```
      task  cputime      memory      files      sessions
cpu facility  inst used allc   used alloc used allc used allc S status
-----
1/0 sessmgr   107 1.6% 100% 119.6M 155.0M   26 500   83 6600 I   good
13/1 aaamgr   107 0.3% 94%  30.8M 77.0M    18 500   --  --  -   good
8/0 aaamgr   231 0.1% 30%  11.6M 25.0M    19 500   --  --  -   good
```

在以下示例中，請注意，與會話計數相關的其他會話相比，aamgr 92的問題正在影響配對sessmgr，這一點很容易看到：

```
      task  cputime      memory      files      sessions
cpu facility  inst used allc   used alloc used allc used allc S status
-----
12/0 sessmgr   92 1.2% 100% 451.5M 1220M    43 500   643 21120 I   good
16/0 aaamgr   92 0.0% 95%  119.0M 315.0M    20 500   --  --  -   good
12/0 sessmgr   95 6.9% 100% 477.3M 1220M    41 500  2626 21120 I   good
```

```

12/0 sessmgr      105 7.7% 100% 600.5M 1220M  45  500  2626 21120 I  good
12/0 sessmgr      126 3.4% 100% 483.0M 1220M  44  500  2625 21120 I  good
12/0 sessmgr      131 8.1% 100% 491.7M 1220M  45  500  2627 21120 I  good

```

## show radius counters { {all | server <server IP>} [instance <aamgr #>] |摘要}

熟悉的第一命令是「show radius counters」的變體

此命令會傳回許多有用的計數器以疑難排解radius問題。「show radius counters all」命令在跟蹤伺服器成功與失敗方面非常有用，瞭解構成此命令的各種計數器的含義非常重要，因為它可能並不明顯。該命令是上下文相關的，因此必須在定義aaa組的同一上下文中運行。

重要附註：在未被監視的時間段內，很難從計數器值或計數器之間的關係得出任何結論。為了做出準確的結論，最佳方法是重置計數器，並在出現故障排除問題時在一段時間內對其進行監控。

在以下輸出中，請注意「Access-Request Sent」= 1，而「Access-Request Retried」= 3。因此，對特定radius伺服器的任何給定新請求僅計數一次，所有重試均單獨計數。在本例中，共傳送了3 + 1 = 4個訪問請求。請注意，計數器"Access-Request Timeouts" = 1。只有當所有重試失敗時，才會出現單個超時。因此，在這種情況下，3次重試而沒有響應會導致1次超時（而不是4次）。所有已配置的伺服器都會發生這種情況，直到成功或所有嘗試都失敗。因此，請注意分別為每個伺服器跟蹤的計數器。以下是範例，其中：

```

radius max-retries 3
radius server 192.168.50.200 encrypted key 01abd002c82b4a2c port 1812 priority 1
radius server 192.168.50.250 encrypted key 01abd002c82b4a2c port 1812 priority 2

```

```
[destination]CSE2# show radius counters all
```

```
Server-specific Authentication Counters
```

```
-----
Authentication server address 192.168.50.200, port 1812:
```

```

Access-Request Sent: 1
Access-Request with DMU Attributes Sent: 0
Access-Request Pending: 0
Access-Request Retried: 3
Access-Request with DMU Attributes Retried: 0
Access-Challenge Received: 0
Access-Accept Received: 0
Access-Reject Received: 0
Access-Reject Received with DMU Attributes: 0
Access-Request Timeouts: 1
Access-Request Current Consecutive Failures in a mgr: 1
Access-Request Response Bad Authenticator Received: 0
Access-Request Response Malformed Received: 0
Access-Request Response Malformed Attribute Received: 0
Access-Request Response Unknown Type Received: 0
Access-Request Response Dropped: 0
Access-Request Response Last Round Trip Time: 0.0 ms
Access-Request Response Average Round Trip Time: 0.0 ms

```

```

Current Access-Request Queued: 0 ... Authentication server address 192.168.50.250, port 1812:
Access-Request Sent: 1 Access-Request with DMU Attributes Sent: 0 Access-Request Pending: 0
Access-Request Retried: 3 Access-Request with DMU Attributes Retried: 0 Access-Challenge
Received: 0 Access-Accept Received: 0 Access-Reject Received: 0 Access-Reject Received with DMU
Attributes: 0 Access-Request Timeouts: 1 Access-Request Current Consecutive Failures in a mgr: 1
Access-Request Response Bad Authenticator Received: 0 Access-Request Response Malformed
Received: 0 Access-Request Response Malformed Attribute Received: 0 Access-Request Response
Unknown Type Received: 0 Access-Request Response Dropped: 0 Access-Request Response Last Round
Trip Time: 0.0 ms Access-Request Response Average Round Trip Time: 0.0 ms
Current Access-Request Queued: 0

```



另請注意，超時不計為失敗，結果是，如果存在任何超時，接收的訪問接受和訪問拒絕的數量不會合計為傳送的訪問請求。

對這些計數器的分析可能不是完全簡單的。例如，對於移動IP(MIP)協定，由於身份驗證失敗，沒有傳送MIP註冊應答(RRP)，並且移動機會可以繼續發起新的MIP註冊請求(RRQ)，因為它沒有收到MIP RRP。每個新的MIP RRQ都會導致PDSN傳送新的身份驗證請求，該請求本身可以具有其自己的一系列重試。這可以在資料包跟蹤頂部的ID欄位中看到 — 對於每組重試而言，此欄位都是唯一的。結果是Sent、Retried和Timeout的計數器可以大大超出所接收呼叫數的預期值。有一個選項可以啟用以最小化這些額外重試次數，而且可以在外部代理(FA)中設定(但不能在Home Agent(HA)服務中設定："authentication mn-aaa <此處選擇6>optimize-retries")

其他一些有用的計數器：

「Access-Request Response Dropped」 — 在等待身份驗證請求的響應時呼叫設定失敗時發生。

「Access-Request Response Last Round Trip Time」 — 表示終端之間的任何延遲，但顯然不會表示延遲可能發生在何處。

「Access-Request Current Consecutive Failures in a mgr」與有關AAA不可達陷阱觸發器的第一節中討論的內容有關。它表示具有最高連續超時計數的aaamgr。

「Current Access/Accounting-Request Queued」表示未響應且保留在隊列中的請求（記帳允許在身份驗證不響應時無限期地建立隊列）

報告AAA無法連線時最常見的情況是也會發生存取逾時和/或回應捨棄，而存取回應跟不上要求。

如果對特權技術支援模式的訪問可用，則可在aamgr例項級別執行進一步調查，以確定一個或多個特定aamgr是否是總體「錯誤」計數增加的原因。例如，查詢位於計數較高的特定PSC/DPC上的aaamgr，或者可能查詢存在問題的單個aaamgr或隨機aamgr — 查詢模式。如果所有或大多數客戶都出現問題，則更有可能出現根本原因或機箱外部或機箱上出現大規模問題的情況。在這種情況下，應執行一般運行狀況檢查。

以下是顯示特定aamgr記帳問題的輸出範例。(事實證明，問題出在ASR5K和RADIUS伺服器之間的防火牆中存在一個錯誤，該防火牆阻止來自特定aamgr例項(114)埠的流量)。在三週內，只收到48個響應，但是已經發生了100,000多次超時（這不包括重新傳輸）。

```
[source]PDSN> show radius counters server 209.165.201.1 instance 114 | grep -E "Accounting-Request Sent|Accounting-Response Received|Accounting-Request Timeouts"
Wednesday October 01 18:12:24 UTC 2014
  Accounting-Request Sent:                14306189
  Accounting-Response Received:          14299843
  Accounting-Request Timeouts:           6342
```

```
[source]PDSN> show radius counters server 209.165.201.1 instance 114 | grep -E "Accounting server address|Accounting-Request Sent|Accounting-Response Received|Accounting-Request Timeouts"
Wednesday October 22 20:26:35 UTC 2014
  Accounting server address 209.165.201.1, port 1646:
  Accounting-Request Sent:                15105872
  Accounting-Response Received:          14299891
  Accounting-Request Timeouts:           158989
```

```
[source]PDSN> show radius counters server 209.165.201.1 instance 114 | grep Accounting
Wednesday October 22 20:33:09 UTC 2014
  Per-Context RADIUS Accounting Counters
  Accounting Response
  Server-specific Accounting Counters
  Accounting server address 209.165.201.1, port 1646:
  Accounting-Request Sent:                15106321
  Accounting-Start Sent:                  7950140
  Accounting-Stop Sent:                   7156129
```

```

Accounting-Interim Sent: 52
Accounting-On Sent: 0
Accounting-Off Sent: 0
Accounting-Request Pending: 3
Accounting-Request Retried: 283713
Accounting-Start Retried: 279341
Accounting-Stop Retried: 4372
Accounting-Interim Retried: 0
Accounting-On Retried: 0
Accounting-Off Retried: 0
Accounting-Response Received: 14299891
Accounting-Request Timeouts: 159000
Accounting-Request Current Consecutive Failures in a mgr: 11
Accounting-Response Bad Response Received: 0
Accounting-Response Malformed Received: 0
Accounting-Response Unknown Type Received: 0
Accounting-Response Dropped: 21
Accounting-Response Last Round Trip Time: 52.5 ms
Accounting-Response Average Round Trip Time: 49.0 ms
Accounting Total G1 (Acct-Output-Octets): 4870358614798
Accounting Total G2 (Acct-Input-Octets): 714140547011
Current Accounting-Request Queued: 17821

```

總之，確定哪些計數器正在遞增、哪些伺服器遞增以及遞增速度如何。

## show session subsystem facility {aaamgr | sessmgr} {all |例項<例項#>}

雖然檢查此命令的所有多餘輸出已超出本文的範圍，但有幾個示例值得一看。與任何其他故障排除一樣，比較被認為良好與不好的aaamgr例項之間的輸出通常會揭示所報告的值之間的明顯差異。這可能反映在請求總數、失敗/成功率、身份驗證取消等中。提醒一下，務必清除會話子系統（一個例項無法清除，它們都必須清除），以消除可能提供當前狀態模糊圖的任何歷史記錄。

繼續上文提到的關於單個aamgr記賬失敗的相同問題，下面是從除了不同會話例項36之外的具有同一問題的不同節點輸出的輸出。請注意失敗的aamgr的所有感興趣的欄位，以及使用該命令的兩個捕獲時這些值隨時間如何增加。同時，示出了來自例項37的輸出作為工作放大器的示例。

```
[source]PDSN> show session subsystem facility aaamgr instance 36
Wednesday September 10 08:51:18 UTC 2014
```

```

AAAMgr: Instance 36
39947440 Total aaa requests 17985 Current aaa requests
24614090 Total aaa auth requests 0 Current aaa auth requests
0 Total aaa auth probes 0 Current aaa auth probes
0 Total aaa aggregation requests
0 Current aaa aggregation requests
0 Total aaa auth keepalive 0 Current aaa auth keepalive
15171628 Total aaa acct requests 17985 Current aaa acct requests
0 Total aaa acct keepalive 0 Current aaa acct keepalive
20689536 Total aaa auth success 1322489 Total aaa auth failure
86719 Total aaa auth purged 1016 Total aaa auth cancelled
0 Total auth keepalive success 0 Total auth keepalive failure
0 Total auth keepalive purged
0 Total aaa aggregation success requests
0 Total aaa aggregation failure requests
0 Total aaa aggregation purged requests
15237 Total aaa auth DMU challenged
17985/70600 aaa request (used/max)
14 Total diameter auth responses dropped
6960270 Total Diameter auth requests 0 Current Diameter auth requests
23995 Total Diameter auth requests retried
52 Total Diameter auth requests dropped
9306676 Total radius auth requests 0 Current radius auth requests
0 Total radius auth requests retried

```

```

988 Total radius auth responses dropped
13 Total local auth requests          0 Current local auth requests
8500275 Total pseudo auth requests    0 Current pseudo auth requests
8578 Total null-username auth requests (rejected)
0 Total aggregation responses dropped
15073834 Total aaa acct completed      79763 Total aaa acct purged    <== If issue started
recently, this may not have yet started incrementing
0 Total acct keepalive success        0 Total acct keepalive timeout
0 Total acct keepalive purged
4 CLI Test aaa acct purged
0 IP Interface down aaa acct purged
0 No Radius Server found aaa acct purged
0 No Response aaa acct purged
14441090 Total acct sess alloc
14422811 Total acct sess delete
18279 Current acct sessions
0 Auth No Wait Suppressed
0 Aggr No Wait Suppressed
0 Disc No Wait Suppressed
0 Start No Wait Suppressed
0 Interim No Wait Suppressed
0 Stop No Wait Suppressed
0 Acct OnOff Custom14
0 Acct OnOff Custom67
0 Acct OnOff
0 Recovery Str Suppressed
0 Recovery Stop Suppressed
0 Med Chrg Gtpp Suppressed
0 Med Chrg Radius Suppressed
0 Radius Probe Trigger
0 Recovery Stop Acct Session Suppressed
46 Total aaa acct cancelled
0 Total Diameter acct requests        0 Current Diameter acct requests
0 Total Diameter acct requests retried
0 Total diameter acct requests dropped
0 Total diameter acct responses dropped
0 Total diameter acct cancelled
0 Total diameter acct purged
15171628 Total radius acct requests    17985 Current radius acct requests
46 Total radius acct cancelled
79763 Total radius acct purged
11173 Total radius acct requests retried
49 Total radius acct responses dropped
0 Total radius sec acct requests      0 Current radius sec acct requests
0 Total radius sec acct cancelled
0 Total radius sec acct purged
0 Total radius sec acct requests retried
0 Total gtpp acct requests            0 Current gtpp acct requests
0 Total gtpp acct cancelled          0 Total gtpp acct purged
0 Total gtpp sec acct requests        0 Total gtpp sec acct purged
0 Total null acct requests            0 Current null acct requests
16218236 Total aaa acct sessions        21473 Current aaa acct sessions
8439 Total aaa acct archived          2 Current aaa acct archived
21473 Current recovery archives       4724 Current valid recovery records
1 Total aaa sockets opened            1 Current aaa sockets opened
1 Total aaa requests pend socket opened
0 Current aaa requests pend socket open
133227 Total radius requests pend server max-outstanding
17982 Current radius requests pend server max-outstanding
0 Total radius auth req queued server max-rate
0 Max radius auth req queued server max-rate
0 Current radius auth req queued server max-rate
0 Total radius acct req queued server max-rate
0 Max radius acct req queued server max-rate

```

```

0 Current radius acct req queued server max-rate
0 Total radius charg auth req queued server max-rate
0 Max radius charg auth req queued server max-rate
0 Current radius charg auth req queued server max-rate
0 Total radius charg acct req queued server max-rate
0 Max radius charg acct req queued server max-rate
0 Current radius charg acct req queued server max-rate
0 Total aaa radius coa requests      0 Total aaa radius dm requests
0 Total aaa radius coa acks         0 Total aaa radius dm acks
0 Total aaa radius coa naks         0 Total aaa radius dm naks
0 Total radius charg auth           0 Current radius charg auth
0 Total radius charg auth success   0 Total radius charg auth failure
0 Total radius charg auth purged    0 Total radius charg auth cancelled
0 Total radius charg acct           0 Current radius charg acct
0 Total radius charg acct success   0 Total radius charg acct purged
0 Total radius charg acct cancelled
0 Total gtpm charg                  0 Current gtpm charg
0 Total gtpm charg success           0 Total gtpm charg failure
0 Total gtpm charg cancelled         0 Total gtpm charg purged
0 Total gtpm sec charg              0 Total gtpm sec charg purged
161722 Total prepaid online requests 0 Current prepaid online requests
141220 Total prepaid online success  20392 Current prepaid online failure
0 Total prepaid online retried      102 Total prepaid online cancelled
8 Current prepaid online purged

```

...

```

[source]PDSN> show session subsystem facility aaamgr instance 37
Wednesday September 10 08:51:28 UTC 2014

```

```

AAAMgr: Instance 37
39571859 Total aaa requests          0 Current aaa requests
24368622 Total aaa auth requests     0 Current aaa auth requests
0 Total aaa auth probes              0 Current aaa auth probes
0 Total aaa aggregation requests     0 Current aaa aggregation requests
0 Total aaa auth keepalive           0 Current aaa auth keepalive
15043217 Total aaa acct requests      0 Current aaa acct requests
0 Total aaa acct keepalive           0 Current aaa acct keepalive
20482618 Total aaa auth success       1309507 Total aaa auth failure
85331 Total aaa auth purged           968 Total aaa auth cancelled
0 Total auth keepalive success       0 Total auth keepalive failure
0 Total auth keepalive purged
0 Total aaa aggregation success requests
0 Total aaa aggregation failure requests
0 Total aaa aggregation purged requests
15167 Total aaa auth DMU challenged
1/70600 aaa request (used/max)
41 Total diameter auth responses dropped
6883765 Total Diameter auth requests  0 Current Diameter auth requests
23761 Total Diameter auth requests retried
37 Total Diameter auth requests dropped
9216203 Total radius auth requests    0 Current radius auth requests
0 Total radius auth requests retried
927 Total radius auth responses dropped
15 Total local auth requests         0 Current local auth requests
8420022 Total pseudo auth requests    0 Current pseudo auth requests
8637 Total null-username auth requests (rejected)
0 Total aggregation responses dropped
15043177 Total aaa acct completed      0 Total aaa acct purged
0 Total acct keepalive success       0 Total acct keepalive timeout
0 Total acct keepalive purged
0 CLI Test aaa acct purged
0 IP Interface down aaa acct purged
0 No Radius Server found aaa acct purged

```

```

0 No Response aaa acct purged
14358245 Total acct sess alloc
14356293 Total acct sess delete
1952 Current acct sessions
0 Auth No Wait Suppressed
0 Aggr No Wait Suppressed
0 Disc No Wait Suppressed
0 Start No Wait Suppressed
0 Interim No Wait Suppressed
0 Stop No Wait Suppressed
0 Acct OnOff Custom14
0 Acct OnOff Custom67
0 Acct OnOff
0 Recovery Str Suppressed
0 Recovery Stop Suppressed
0 Med Chrg Gtpp Suppressed
0 Med Chrg Radius Suppressed
0 Radius Probe Trigger
0 Recovery Stop Acct Session Suppressed
40 Total aaa acct cancelled
0 Total Diameter acct requests          0 Current Diameter acct requests
0 Total Diameter acct requests retried
0 Total diameter acct requests dropped
0 Total diameter acct responses dropped
0 Total diameter acct cancelled
0 Total diameter acct purged
15043217 Total radius acct requests          0 Current radius acct requests
40 Total radius acct cancelled
0 Total radius acct purged
476 Total radius acct requests retried
37 Total radius acct responses dropped
0 Total radius sec acct requests          0 Current radius sec acct requests
0 Total radius sec acct cancelled
0 Total radius sec acct purged
0 Total radius sec acct requests retried
0 Total gtpp acct requests          0 Current gtpp acct requests
0 Total gtpp acct cancelled          0 Total gtpp acct purged
0 Total gtpp sec acct requests          0 Total gtpp sec acct purged
0 Total null acct requests          0 Current null acct requests
16057760 Total aaa acct sessions          4253 Current aaa acct sessions
14 Total aaa acct archived          0 Current aaa acct archived
4253 Current recovery archives          4249 Current valid recovery records
1 Total aaa sockets opened          1 Current aaa sockets opened
1 Total aaa requests pend socket opened
0 Current aaa requests pend socket open
29266 Total radius requests pend server max-outstanding
0 Current radius requests pend server max-outstanding
0 Total radius auth req queued server max-rate
0 Max radius auth req queued server max-rate
0 Current radius auth req queued server max-rate
0 Total radius acct req queued server max-rate
0 Max radius acct req queued server max-rate
0 Current radius acct req queued server max-rate
0 Total radius charg auth req queued server max-rate
0 Max radius charg auth req queued server max-rate
0 Current radius charg auth req queued server max-rate
0 Total radius charg acct req queued server max-rate
0 Max radius charg acct req queued server max-rate
0 Current radius charg acct req queued server max-rate
0 Total aaa radius coa requests          0 Total aaa radius dm requests
0 Total aaa radius coa acks          0 Total aaa radius dm acks
0 Total aaa radius coa naks          0 Total aaa radius dm naks
0 Total radius charg auth          0 Current radius charg auth
0 Total radius charg auth success          0 Total radius charg auth failure

```

```

0 Total radius charg auth purged      0 Total radius charg auth cancelled
0 Total radius charg acct              0 Current radius charg acct
0 Total radius charg acct success      0 Total radius charg acct purged
0 Total radius charg acct cancelled
0 Total gtpv charg                     0 Current gtpv charg
0 Total gtpv charg success              0 Total gtpv charg failure
0 Total gtpv charg cancelled           0 Total gtpv charg purged
0 Total gtpv sec charg                 0 Total gtpv sec charg purged
160020 Total prepaid online requests   0 Current prepaid online requests
139352 Total prepaid online success    20551 Current prepaid online failure
...

```

```

[source]PDSN> show session subsystem facility aaamgr instance 36
Wednesday September 10 09:12:13 UTC 2014

```

```
AAAMgr: Instance 36
```

```

39949892 Total aaa requests              17980 Current aaa requests
24615615 Total aaa auth requests         0 Current aaa auth requests
  0 Total aaa auth probes                0 Current aaa auth probes
  0 Total aaa aggregation requests
  0 Current aaa aggregation requests
  0 Total aaa auth keepalive              0 Current aaa auth keepalive
15172543 Total aaa acct requests          17980 Current aaa acct requests
  0 Total aaa acct keepalive              0 Current aaa acct keepalive
20690768 Total aaa auth success          1322655 Total aaa auth failure
 86728 Total aaa auth purged              1016 Total aaa auth cancelled
  0 Total auth keepalive success          0 Total auth keepalive failure
  0 Total auth keepalive purged
  0 Total aaa aggregation success requests
  0 Total aaa aggregation failure requests
  0 Total aaa aggregation purged requests
 15242 Total aaa auth DMU challenged
 17981/70600 aaa request (used/max)
  14 Total diameter auth responses dropped
6960574 Total Diameter auth requests     0 Current Diameter auth requests
 23999 Total Diameter auth requests retried
  52 Total Diameter auth requests dropped
9307349 Total radius auth requests        0 Current radius auth requests
  0 Total radius auth requests retried
  988 Total radius auth responses dropped
  13 Total local auth requests            0 Current local auth requests
8500835 Total pseudo auth requests        0 Current pseudo auth requests
 8578 Total null-username auth requests (rejected)
  0 Total aggregation responses dropped
15074358 Total aaa acct completed          80159 Total aaa acct purged
  0 Total acct keepalive success          0 Total acct keepalive timeout
  0 Total acct keepalive purged
  4 CLI Test aaa acct purged
  0 IP Interface down aaa acct purged
  0 No Radius Server found aaa acct purged
  0 No Response aaa acct purged
14441768 Total acct sess alloc
14423455 Total acct sess delete
 18313 Current acct sessions
  0 Auth No Wait Suppressed
  0 Aggr No Wait Suppressed
  0 Disc No Wait Suppressed
  0 Start No Wait Suppressed
  0 Interim No Wait Suppressed
  0 Stop No Wait Suppressed
  0 Acct OnOff Customl4

```

```

0 Acct OnOff Custom67
0 Acct OnOff
0 Recovery Str Suppressed
0 Recovery Stop Suppressed
0 Med Chrg Gtpp Suppressed
0 Med Chrg Radius Suppressed
0 Radius Probe Trigger
0 Recovery Stop Acct Session Suppressed
46 Total aaa acct cancelled
0 Total Diameter acct requests          0 Current Diameter acct requests
0 Total Diameter acct requests retried
0 Total diameter acct requests dropped
0 Total diameter acct responses dropped
0 Total diameter acct cancelled
0 Total diameter acct purged
15172543 Total radius acct requests      17980 Current radius acct requests
46 Total radius acct cancelled
80159 Total radius acct purged
11317 Total radius acct requests retried
49 Total radius acct responses dropped
0 Total radius sec acct requests        0 Current radius sec acct requests
0 Total radius sec acct cancelled
0 Total radius sec acct purged
0 Total radius sec acct requests retried
0 Total gtpp acct requests              0 Current gtpp acct requests
0 Total gtpp acct cancelled             0 Total gtpp acct purged
0 Total gtpp sec acct requests          0 Total gtpp sec acct purged
0 Total null acct requests              0 Current null acct requests
16219251 Total aaa acct sessions          21515 Current aaa acct sessions
8496 Total aaa acct archived             0 Current aaa acct archived
21515 Current recovery archives          4785 Current valid recovery records
1 Total aaa sockets opened              1 Current aaa sockets opened
1 Total aaa requests pend socket opened
0 Current aaa requests pend socket open
133639 Total radius requests pend server max-outstanding
17977 Current radius requests pend server max-outstanding
...

```

您還應該運行show task resources以檢查所有會話中是否有任何不均衡的會話計數（已用列）。如果找到任何作業階段，請透過此指令檢查這些作業階段的配對磁標，看看是否有超出範圍的欄位——如果問題是由RADIUS所導致，那麼就很有可能找到問題。

在前一節的show task resources示例中，sessmgr 92上的會話計數顯著降低，該計數與aamgr 92配對。show session subsystem的輸出顯示，最大未處理和aaa auth清除計數以及當前最大未處理計數顯著增加。您可以使用機箱和/或記事本上的grep功能或其他強大++搜尋編輯器快速分析資料。多次運行該命令，以檢視哪些值正在增加或保持提升狀態：

```

[Ingress]PGW# show session subsystem facility aaamgr all
Tuesday January 10 04:42:29 UTC 2012
4695 Total aaa auth purged
4673 Total radius auth requests          16 Current radius auth requests
4167 Total radius requests pend server max-outstanding
76 Current radius requests pend server max-outstanding

[Ingress]PGW# show session subsystem facility aaamgr all | grep "max-outstanding"
Tuesday January 10 04:51:00 UTC 2012
4773 Total radius requests pend server max-outstanding
67 Current radius requests pend server max-outstanding

[Ingress]PGW# show session subsystem facility aaamgr all | grep "max-outstanding"
Tuesday January 10 04:56:10 UTC 2012
5124 Total radius requests pend server max-outstanding

```

```
81 Current radius requests pend server max-outstanding
```

```
[Ingress]PGW# show session subsystem facility aaamgr instance 92  
Tuesday January 10 04:57:03 UTC 2012
```

```
5869 Total aaa auth purged  
5843 Total radius auth requests          12 Current radius auth requests  
5170 Total radius requests pend server max-outstanding  
71 Current radius requests pend server max-outstanding
```

```
[Ingress]PGW# show session subsystem facility aaamgr instance 92  
Tuesday January 10 05:10:05 UTC 2012
```

```
6849 Total aaa auth purged  
6819 Total radius auth requests          6 Current radius auth requests  
5981 Total radius requests pend server max-outstanding  
68 Current radius requests pend server max-outstanding
```

```
[Ingress]PGW# show session subsystem facility aaamgr all | grep "max-outstanding"  
Tuesday January 10 05:44:22 UTC 2012
```

```
71 Total radius requests pend server max-outstanding  
0 Current radius requests pend server max-outstanding  
61 Total radius requests pend server max-outstanding  
0 Current radius requests pend server max-outstanding
```

```
7364 Total radius requests pend server max-outstanding  <== instance #92  
68 Current radius requests pend server max-outstanding
```

```
89 Total radius requests pend server max-outstanding  
0 Current radius requests pend server max-outstanding  
74 Total radius requests pend server max-outstanding  
0 Current radius requests pend server max-outstanding
```

```
[Ingress]PGW#radius test instance 92 auth server 65.175.1.10 port 1645 test test  
Tuesday January 10 06:13:38 UTC 2012
```

```
Authentication from authentication server 65.175.1.10, port 1645  
Communication Failure: No response received
```

## ping

## traceroute

ICMP Ping會測試基本連通性，以確定是否可以到達AAA伺服器。ping可能需要使用src關鍵字作為來源，具體取決於網路，並且需要從AAA上下文執行才能有值。如果對伺服器執行ping失敗，則嘗試ping中間元素，包括上下文中的下一跳地址，並確認如果ping失敗，則下一跳地址中有一個ARP條目。Traceroute也能協助解決路由問題。

```
[source]CSE2# ping 192.168.50.200  
PING 192.168.50.200 (192.168.50.200) 56(84) bytes of data.  
64 bytes from 192.168.50.200: icmp_seq=1 ttl=64 time=0.411 ms  
64 bytes from 192.168.50.200: icmp_seq=2 ttl=64 time=0.350 ms  
64 bytes from 192.168.50.200: icmp_seq=3 ttl=64 time=0.353 ms  
64 bytes from 192.168.50.200: icmp_seq=4 ttl=64 time=0.321 ms  
64 bytes from 192.168.50.200: icmp_seq=5 ttl=64 time=0.354 ms
```

```
--- 192.168.50.200 ping statistics ---  
5 packets transmitted, 5 received, 0% packet loss, time 4000ms  
rtt min/avg/max/mdev = 0.321/0.357/0.411/0.037 ms
```

**radius測試例項x auth {radius group <group> |全部 |伺服器<IP>埠<埠>} <使用者名稱>  
> <密碼>**



## radius測試例項x記帳{radius group <group name> |全部 |伺服器<IP>埠<埠>}

透過存取Tech Support Test指令，您可以進一步測試特定管理員是否可存取任何RADIUS伺服器。對於獨立於任何特定aamgr例項的基本RADIUS連線測試，使用此命令的通用版本，該版本不指定任何特定例項#，但在預設情況下使用管理例項。如果此操作失敗，則它可能指向一個獨立於具體例項的更廣泛的問題。

此命令傳送基本身份驗證請求或記帳start和stop請求並等待響應。要進行身份驗證，請使用任何使用者名稱和密碼，在這種情況下，應收到拒絕響應，確認RADIUS正在按照設計工作，或者可以使用已知的工作使用者名稱/密碼，在這種情況下，應收到接受響應

以下是在實驗室機箱上運行監控協定及驗證版本命令的示例輸出：

```
[source]CSE2# radius test authentication server 192.168.50.200 port 1812 test test
```

```
Authentication from authentication server 192.168.50.200, port 1812
Authentication Success: Access-Accept received
Round-trip time for response was 12.3 ms
```

```
<<<<OUTBOUND 14:53:49:202 Eventid:23901(6)
RADIUS AUTHENTICATION Tx PDU, from 192.168.50.151:32783 to 192.168.50.200:1812 (58) PDU-
dict=starent-vsai
Code: 1 (Access-Request)
Id: 5
Length: 58
Authenticator: 56 97 57 9C 51 EF A4 08 20 E1 14 89 40 DE 0B 62
    User-Name = test
    User-Password = 49 B0 92 4D DC 64 49 BA B0 0E 18 36 3F B6 1B 37
    NAS-IP-Address = 192.168.50.151
    NAS-Identifier = source
```

```
INBOUND>>>> 14:53:49:214 Eventid:23900(6)
RADIUS AUTHENTICATION Rx PDU, from 192.168.50.200:1812 to 192.168.50.151:32783 (34) PDU-
dict=starent-vsai
Code: 2 (Access-Accept)
Id: 5
Length: 34
Authenticator: D7 94 1F 18 CA FE B4 27 17 75 5C 99 9F A8 61 78
    User-Password = testpassword
```

以下是來自活動機箱的示例：

```
<<<<OUTBOUND 12:45:49:869 Eventid:23901(6)
RADIUS AUTHENTICATION Tx PDU, from 10.209.28.200:33156 to 209.165.201.1:1645 (72) PDU-
dict=custom150
Code: 1 (Access-Request)
Id: 6
Length: 72
Authenticator: 67 C2 2B 3E 29 5E A5 28 2D FB 85 CA 0E 9F A4 17
    User-Name = test
    User-Password = 8D 95 3B 31 99 E2 6A 24 1F 81 13 00 3C 73 BC 53
    NAS-IP-Address = 10.209.28.200
    NAS-Identifier = source
    3GPP2-Session-Term-Capability = Both_Dynamic_Auth_And_Reg_Revocation_in_MIP
```

```
INBOUND>>>> 12:45:49:968 Eventid:23900(6)
RADIUS AUTHENTICATION Rx PDU, from 209.165.201.1:1645 to 10.209.28.200:33156 (50) PDU-
dict=custom150
Code: 3 (Access-Reject)
Id: 6
Length: 50
Authenticator: 99 2E EC DA ED AD 18 A9 86 D4 93 52 57 4C 2F 84
```

Reply-Message = Invalid username or password

以下是運行命令的記帳版本的示例輸出。不需要密碼。

```
[source]CSE2# radius test accounting server 192.168.50.200 port 1813 test
RADIUS Start to accounting server 192.168.50.200, port 1813
Accounting Success: response received
Round-trip time for response was 7.9 ms
```

```
RADIUS Stop to accounting server 192.168.50.200, port 1813
Accounting Success: response received
Round-trip time for response was 15.4 ms
```

```
<<<<OUTBOUND 15:23:14:974 Eventid:24901(6)
RADIUS ACCOUNTING Tx PDU, from 192.168.50.151:32783 to 192.168.50.200:1813 (62) PDU-
dict=starent-vsai
Code: 4 (Accounting-Request)
Id: 8
Length: 62
Authenticator: DA 0F A8 11 7B FE 4B 1A 56 EB 0D 49 8C 17 BD F6
  User-Name = test
  NAS-IP-Address = 192.168.50.151
  Acct-Status-Type = Start
  Acct-Session-Id = 00000000
  NAS-Identifier = source
  Acct-Session-Time = 0
```

```
INBOUND>>>> 15:23:14:981 Eventid:24900(6) RADIUS ACCOUNTING Rx PDU, from 192.168.50.200:1813 to
192.168.50.151:32783 (20) PDU-dict=starent-vsai Code: 5 (Accounting-Response) Id: 8 Length: 20
Authenticator: 05 E2 82 29 45 FC BC D6 6C 48 63 AA 14 9D 47 5B <<<<OUTBOUND 15:23:14:983
Eventid:24901(6) RADIUS ACCOUNTING Tx PDU, from 192.168.50.151:32783 to 192.168.50.200:1813 (62)
PDU-dict=starent-vsai Code: 4 (Accounting-Request) Id: 9 Length: 62 Authenticator: 29 DB F1 0B
EC CE 68 DB C7 4D 60 E4 7F A2 D0 3A User-Name = test NAS-IP-Address = 192.168.50.151 Acct-
Status-Type = Stop Acct-Session-Id = 00000000 NAS-Identifier = source Acct-Session-Time = 0
INBOUND>>>> 15:23:14:998 Eventid:24900(6) RADIUS ACCOUNTING Rx PDU, from 192.168.50.200:1813 to
192.168.50.151:32783 (20) PDU-dict=starent-vsai Code: 5 (Accounting-Response) Id: 9 Length: 20
Authenticator: D8 3D EF 67 EA 75 E0 31 A5 31 7F E8 7E 69 73 DC
```

以下輸出適用於剛才提到的連線到特定RADIUS記帳伺服器的同一個aamgr例項36:

```
[source]PDSN> radius test instance 36 accounting all test
Wednesday September 10 10:06:29 UTC 2014

RADIUS Start to accounting server 209.165.201.1, port 1646
Accounting Success: response received
Round-trip time for response was 51.2 ms

RADIUS Stop to accounting server 209.165.201.1, port 1646
Accounting Success: response received
Round-trip time for response was 46.2 ms

RADIUS Start to accounting server 209.165.201.2, port 1646
Accounting Success: response received
Round-trip time for response was 89.3 ms

RADIUS Stop to accounting server 209.165.201.2, port 1646
Accounting Success: response received
Round-trip time for response was 87.8 ms
```

RADIUS Start to accounting server 209.165.201.3, port 1646

**Communication Failure: no response received**

RADIUS Stop to accounting server 209.165.201.3, port 1646

**Communication Failure: no response received**

RADIUS Start to accounting server 209.165.201.4, port 1646

Accounting Success: response received

Round-trip time for response was 81.6 ms

RADIUS Stop to accounting server 209.165.201.4, port 1646

Accounting Success: response received

Round-trip time for response was 77.1 ms

RADIUS Start to accounting server 209.165.201.5, port 1646

Accounting Success: response received

Round-trip time for response was 46.7 ms

RADIUS Stop to accounting server 209.165.201.5, port 1646

Accounting Success: response received

Round-trip time for response was 46.7 ms

RADIUS Start to accounting server 209.165.201.6, port 1646

Accounting Success: response received

Round-trip time for response was 79.6 ms

RADIUS Stop to accounting server 209.165.201.6, port 1646

Accounting Success: response received

Round-trip time for response was 10113.0 ms

## **show radius info [radius group <group name>] instance { X }**

此命令報告網路處理器單元(NPU)流ID和UDP埠，由配置的NAS IP地址用於連線到RADIUS伺服器。輸出的aaa group default部分中報告了此問題。如果資料包捕獲中的RADIUS資料包需要與特定的aamgr例項#匹配，則埠號無疑會很有用。（請注意，NPU流非常複雜，並非本文所討論的內容，而是支援工程師能夠進一步調查的實體。）它還跟蹤對伺服器的未處理請求。在本文中使用的同一示例問題中，只有特定的RADIUS伺服器<==> NAS IP/UDP埠對出現故障，如突出顯示。

```
[source]PDSN> show radius info radius group all instance 114
```

```
Wednesday October 01 11:39:15 UTC 2014
```

```
Context source:
```

```
-----
```

```
AAAMGR instance 114:  cb-list-en: 1 AAA Group: aaa-roamingprovider.com
```

```
-----
```

```
Authentication servers:
```

```
-----
```

```
Primary authentication server address 209.165.201.1, port 1645
```

```
state Active
```

```
priority 1
```

```
requests outstanding 0
```

```
max requests outstanding 3
```

```
consecutive failures 0
```

```
Secondary authentication server address 209.165.201.2, port 1645
```

```
state Active
```

```
priority 2
```

```
requests outstanding 0
```

```
max requests outstanding 3
```

```
consecutive failures 0
```

Accounting servers:

-----  
Primary accounting server address 209.165.201.1, port 1646  
state Active  
priority 1  
requests outstanding 0  
max requests outstanding 3  
consecutive failures 0

Secondary accounting server address 209.165.201.2, port 1646  
state Active  
priority 2  
requests outstanding 0  
max requests outstanding 3  
consecutive failures 0

AAAMGR instance 114: cb-list-en: 1 AAA Group: aaa-maingroup.com

-----  
Authentication servers:

-----  
Primary authentication server address 209.165.201.3, port 1645  
state Active  
priority 1  
requests outstanding 0  
max requests outstanding 3  
consecutive failures 0

Secondary authentication server address 209.165.201.4, port 1645  
state Active  
priority 2  
requests outstanding 0  
max requests outstanding 3  
consecutive failures 0

Accounting servers:

-----  
Primary accounting server address 209.165.201.3, port 1646  
state Down  
priority 1  
requests outstanding 3  
max requests outstanding 3  
consecutive failures 7  
dead time expires in 146 seconds

Secondary accounting server address 209.165.201.4, port 1646  
state Active  
priority 2  
requests outstanding 0  
max requests outstanding 3  
consecutive failures 0

AAAMGR instance 114: cb-list-en: 1 AAA Group: default

-----  
socket number: 388550648  
socket state: ready  
local ip address: 10.210.21.234  
local udp port: 25808  
flow id: 20425379  
use med interface: yes  
VRF context ID: 2

Authentication servers:

-----  
Primary authentication server address 209.165.201.5, port 1645  
state Active  
priority 1  
requests outstanding 0

```
max requests outstanding 3
consecutive failures 0
Secondary authentication server address 209.165.201.6, port 1645
state Not Responding
priority 2
requests outstanding 0
max requests outstanding 3
consecutive failures 0
```

Accounting servers:

```
-----
Primary accounting server address 209.165.201.5, port 1646
state Active
priority 1
requests outstanding 0
max requests outstanding 3
consecutive failures 0
Secondary accounting server address 209.165.201.6, port 1646
state Active
priority 2
requests outstanding 0
max requests outstanding 3
consecutive failures 0
```

[source]PDSN>

## 監控使用者

監控使用者可用於確定是否至少嘗試了身份驗證，以及是否正在針對受監控呼叫處理應答。啟用代表Sessmgr發件人資訊的選項「S」—有效報告處理相關郵件的sessmgr或aamgr例項#。以下是在HA上執行MIP呼叫的示例 連線到sessmgr/aaamgr例項132。

Incoming Call:

```
-----
MSID/IMSI      :                               Callid       : 2719afb2
IMEI           : n/a                          MSISDN        : n/a
Username       : 6667067222@cisco.com        SessionType   : ha-mobile-ip
Status         : Active                       Service Name  : HAService
Src Context    : source
-----
```

\*\*\* Sender Info (ON ) \*\*\*

Thursday June 11 2015

INBOUND>>>> From sessmgr:132 sessmgr\_ha.c:861 (Callid 2719afb2) 15:42:35:742 Eventid:26000(3)

MIP Rx PDU, from 203.0.113.11:434 to 203.0.113.1:434 (190)

Message Type: 0x01 (Registration Request)

Flags: 0x02

Lifetime: 0x1C20

Home Address: 0.0.0.0

Home Agent Address: 255.255.255.255

Thursday June 11 2015

<<<<OUTBOUND From aaamgr:132 aaamgr\_radius.c:367 (Callid 2719afb2) 15:42:35:743

Eventid:23901(6)

RADIUS AUTHENTICATION Tx PDU, from 203.0.113.1:59933 to 209.165.201.3:1645 (301) PDU-dict=custom9

Code: 1 (Access-Request)

Id: 12

Length: 301

Thursday June 11 2015

INBOUND>>>> From aaamgr:132 aaamgr\_radius.c:1999 (Callid 2719afb2) 15:42:35:915

Eventid:23900(6)

```
RADIUS AUTHENTICATION Rx PDU, from 209.165.201.3:1645 to 203.0.113.1:59933 (156) PDU-
dict=custom9
Code: 2 (Access-Accept)
Id: 12
```

Thursday June 11 2015

```
<<<<OUTBOUND From sessmgr:132 mipha_fsm.c:6617 (Callid 2719afb2) 15:42:36:265 Eventid:26001(3)
MIP Tx PDU, from 203.0.113.1:434 to 203.0.113.11:434 (112)
Message Type: 0x03 (Registration Reply)
Code: 0x00 (Accepted)
Lifetime: 0x1C20
Home Address: 10.229.6.167
```

在本文的最後也有一個失敗示例。

## 封包擷取

有時，沒有足夠的ASR資訊來確定出現可達性問題的原因，在這種情況下，需要捕獲資料包。在排查個別使用者問題時，在跟蹤中識別各自的資料包應該很容易。否則，如果問題與特定埠/aaamgr例項相關，瞭解特定aaamgr例項# <==> RADIUS伺服器對任一端使用的UDP埠可能會有所幫助。在網路中的多個位置嘗試捕獲可能是確定資料包被丟棄的位置所必需的。在本文所分析的問題中，ASR和RADIUS伺服器之間的傳輸路徑中恰當位置的資料包捕獲是解決問題的突破口。

## 補救

最後一部分提供一些修正RADIUS連線問題的想法。這些不以任何特定的順序顯示，而只是故障排除過程中要考慮的清單。

如果RADIUS伺服器超載，則可能會透過設定為「radius(accounting)max-outstanding」的值（預設為256）來降低負載，此值對任何給定的aaamgr程式設定未處理（未應答）要求數量的限制。如果達到此限制，日誌可能會指示此情況：「無法為radius身份驗證伺服器x.x.x.x:1812分配消息ID」。對特定伺服器的速率限制RADIUS訊息也可能會透過針對各伺服器組態行的速率限制關鍵字協助減少負載。

有時，這不是連線的問題，而是記帳流量增加的問題，這不是RADIUS傳輸的問題，而是指向另一個領域，例如增加的ppp重新協商會導致更多記帳的開始和停止。因此，可能需要在RADIUS之外進行故障排除，以找出所觀察到症狀的原因或觸發器。

如果在故障排除過程中，由於某種原因決定將radius身份驗證或記帳伺服器從活動伺服器清單中刪除，則會使用(non-config)命令無限期地使伺服器停止服務，直到希望恢復服務。與必須手動將其從配置中移除相比，這是一種更乾淨的方法：

```
{disable | enable} radius [accounting]x.x.x.x
```

```
[source]CSE2# show radius authentication servers detail
```

```
+-----Type:          (A) - Authentication      (a) - Accounting
|                   (C) - Charging          (c) - Charging Accounting
|                   (M) - Mediation        (m) - Mediation Accounting
|
|+-----Preference: (P) - Primary          (S) - Secondary
||
||+----State:        (A) - Active          (N) - Not Responding
|||                 (D) - Down            (W) - Waiting Accounting-On
|||                 (I) - Initializing    (w) - Waiting Accounting-Off
|||                 (a) - Active Pending  (U) - Unknown
|||
||+---Admin          (E) - Enabled          (D) - Disabled
||| Status:
```

```

||||
||||+-Admin
|||| status      (O) - Overridden      (.) - Not Overridden
|||| Overridden:
||||
vvvvv IP          PORT GROUP
-----
APNDO 192.168.50.200 1812 default

```

PSC或DPC遷移或線卡切換通常可以清除問題，因為遷移會導致卡上的進程重新啟動，包括npumgr，它一直是NPU流方面不時出現問題的原因。

但是，與前面提到的aaamgr 92的示例相比，一個有趣的轉折是，AAA不可達故障實際上是在PSC遷移完成時開始的。這是因為PSC遷移完成使PSC 11成為備用時，NPU流丟失。一小時後，丟失流量對aamgr 92的實際影響開始生效。如果沒有技術支援的幫助，將很難解決此類問題。

```
[Ingressc]PGW# show rct stat
```

```
RCT stats Details (Last 6 Actions)
```

Action	Type	From	To	Start Time	Duration
Migration	Planned	11	16	2012-Jan-09+16:27:38.135	36.048 sec
Migration	Planned	3	11	2012-Jan-09+17:28:57.413	48.739 sec

```
Mon Jan 09 17:31:11 2012 Internal trap notification 39 (AAAAuthSvrUnreachable) server 2 ip address 209.165.201.3
```

```
Mon Jan 09 17:31:16 2012 Internal trap notification 40 (AAAAuthSvrReachable) server 2 ip address 209.165.201.3
```

此問題通過埠切換臨時解決，導致缺少aamgr 92的NPU流的PSC卡不再連線到活動線卡。

```
Tue Jan 10 06:52:17 2012 Internal trap notification 93 (CardStandby) card 27
```

```
Tue Jan 10 06:52:17 2012 Internal trap notification 1024 (PortDown) card 27 port 1 ifindex 453050375port type 10G Ethernet
```

```
Tue Jan 10 06:52:17 2012 Internal trap notification 55 (CardActive) card 28
```

```
Tue Jan 10 06:52:17 2012 Internal trap notification 1025 (PortUp) card 28 port 1 ifindex 469827588port type 10G Ethernet
```

最後一個故障陷阱：

```
Tue Jan 10 06:53:11 2012 Internal trap notification 43 (AAAAccSvrReachable) server 5 ip address 209.165.201.3
```

```
[Ingress]PGW# radius test instance 93 authen server 209.165.201.3 port 1645 test test
Tuesday January 10 07:18:22 UTC 2012
```

```
Authentication from authentication server 209.165.201.3, port 1645
```

```
Authentication Failure: Access-Reject received
```

```
Round-trip time for response was 38.0 ms
```

```
[Ingress]PGW# show session subsystem facility aaamgr instance 92
```

```
Tuesday January 10 07:39:47 UTC 2012
```

```
12294 Total aaa auth purged
```

```
14209 Total radius auth requests          0 Current radius auth requests
```

```
9494 Total radius requests pend server max-outstanding
```

```
0 Current radius requests pend server max-outstanding
```

同樣，重新啟動會出現「停滯」的特定任務也可能解決問題，儘管由於涉及到受限的技術支援命令

，這是技術支援應執行的活動。在前面的show task resources一節中介紹的aaamgr 92示例中，嘗試了此操作，但沒有幫助，因為根本原因不是aamgr 92，而是aaamgr 92需要的缺失NPU流（這是NPU問題，而不是aamgr問題）。以下是嘗試的相關輸出。運行「show task table」以顯示進程id和任務例項# 92的關聯。

```
5 2012-Jan-10+06:20:53 aaamgr 16/0/04722 12.0(40466) PLB27085474/PLB38098237
```

```
[Ingress]PGW# show crash number 5
***** CRASH #05 *****
Build: 12.0(40466)
Fatal Signal 6: Aborted
PC: [b7eb6b90/X] __poll()
Note: User-initiated state dump w/core.
```

```
***** show task table *****
      task
cpu facility      inst  pid pri  parent
-----
16/0 aaamgr        92   4722  0  sessctrl
      inst  pid
      0    2887
```

## 最終示例

這是即時網路實際中斷的最後一個示例，它將本文討論的許多故障排除命令和方法彙集到一起。請注意，此節點處理3G MIP、4G Long Term Evolution(LTE)和演化高速分組資料(eHRPD)呼叫型別。

### show snmp trap history

僅通過陷阱，可以確認起點與客戶報告的19:25 UTC匹配。另外請注意，主伺服器209.165.201.3的**AAAAuthSvrUnreachable**陷阱在數小時後才會開始發生(原因不清楚，但請注意；但記帳無法到達該伺服器立即開始)

```
Sun Dec 29 19:28:13 2013 Internal trap notification 42 (AAAAccSvrUnreachable) server 5 ip
address 209.165.201.3
Sun Dec 29 19:32:13 2013 Internal trap notification 39 (AAAAuthSvrUnreachable) server 2 ip
address 209.165.201.3
Sun Dec 29 19:33:05 2013 Internal trap notification 40 (AAAAuthSvrReachable) server 2 ip address
209.165.201.3
Sun Dec 29 19:34:13 2013 Internal trap notification 43 (AAAAccSvrReachable) server 5 ip address
209.165.201.3
Sun Dec 29 19:34:13 2013 Internal trap notification 39 (AAAAuthSvrUnreachable) server 2 ip
address 209.165.201.3
Sun Dec 29 19:35:05 2013 Internal trap notification 40 (AAAAuthSvrReachable) server 2 ip address
209.165.201.3
Sun Dec 29 19:38:13 2013 Internal trap notification 42 (AAAAccSvrUnreachable) server 6 ip
address 209.165.201.8
...
Sun Dec 29 23:12:13 2013 Internal trap notification 39 (AAAAuthSvrUnreachable) server 4 ip
address 209.165.201.3
Sun Dec 29 23:13:03 2013 Internal trap notification 40 (AAAAuthSvrReachable) server 4 ip address
209.165.201.3
Sun Dec 29 23:54:13 2013 Internal trap notification 39 (AAAAuthSvrUnreachable) server 4 ip
address 209.165.201.3
Sun Dec 29 23:54:14 2013 Internal trap notification 40 (AAAAuthSvrReachable) server 4 ip address
209.165.201.3
Sun Dec 29 23:58:13 2013 Internal trap notification 39 (AAAAuthSvrUnreachable) server 4 ip
address 209.165.201.3
Sun Dec 29 23:58:14 2013 Internal trap notification 40 (AAAAuthSvrReachable) server 4 ip address
```



### 顯示任務資源

輸出顯示DPC 8/1上的呼叫計數低得多。僅基於此，無需進一步分析，即可建議DPC 8上存在問題並建議遷移到備用DPC的選項。但必須確認實際對使用者的影響 — 在這些情況下，使用者通常會在隨後的嘗試中成功連線，因此對使用者的影響不是太顯著，並且他們可能不會向提供商報告任何資訊，假定使用者平面也沒有中斷（這取決於中斷的內容）。

7/1	sessmgr	230	27%	100%	586.2M	2.49G	43	500	4123	35200	I	good
7/1	aaamgr	237	0.9%	95%	143.9M	640.0M	22	500	--	--	-	good
7/1	sessmgr	243	22%	100%	588.1M	2.49G	42	500	4118	35200	I	good
7/1	sessmgr	258	19%	100%	592.8M	2.49G	43	500	4122	35200	I	good
7/1	aaamgr	268	0.9%	95%	143.5M	640.0M	22	500	--	--	-	good
7/1	sessmgr	269	23%	100%	586.7M	2.49G	43	500	4115	35200	I	good
7/1	aaamgr	274	0.4%	95%	144.9M	640.0M	22	500	--	--	-	good
7/1	sessmgr	276	30%	100%	587.9M	2.49G	43	500	4123	35200	I	good
7/1	aaamgr	285	1.0%	95%	142.7M	640.0M	22	500	--	--	-	good
7/1	aaamgr	286	0.8%	95%	143.8M	640.0M	22	500	--	--	-	good
7/1	sessmgr	290	28%	100%	588.2M	2.49G	41	500	4115	35200	I	good
8/0	sessmgr	177	23%	100%	588.7M	2.49G	48	500	4179	35200	I	good
8/0	sessmgr	193	24%	100%	591.3M	2.49G	44	500	4173	35200	I	good
8/0	aaamgr	208	0.9%	95%	143.8M	640.0M	22	500	--	--	-	good
8/0	sessmgr	211	23%	100%	592.1M	2.49G	45	500	4173	35200	I	good
8/0	sessmgr	221	27%	100%	589.2M	2.49G	44	500	4178	35200	I	good
8/0	aaamgr	222	0.9%	95%	142.0M	640.0M	22	500	--	--	-	good
8/0	sessmgr	225	25%	100%	592.0M	2.49G	43	500	4177	35200	I	good
8/0	aaamgr	238	0.9%	95%	140.0M	640.0M	22	500	--	--	-	good
8/0	aaamgr	243	1.0%	95%	144.9M	640.0M	22	500	--	--	-	good
8/0	sessmgr	244	31%	100%	593.3M	2.49G	43	500	4177	35200	I	good
8/0	aaamgr	246	0.9%	95%	138.5M	640.0M	22	500	--	--	-	good
8/0	aaamgr	248	0.9%	95%	141.4M	640.0M	22	500	--	--	-	good
8/0	aaamgr	258	0.9%	95%	138.3M	640.0M	22	500	--	--	-	good
8/0	aaamgr	259	0.8%	95%	139.2M	640.0M	22	500	--	--	-	good
8/0	aaamgr	260	0.8%	95%	142.9M	640.0M	22	500	--	--	-	good
8/0	aaamgr	262	0.9%	95%	145.0M	640.0M	22	500	--	--	-	good
8/0	aaamgr	264	0.9%	95%	143.4M	640.0M	22	500	--	--	-	good
8/0	sessmgr	270	24%	100%	592.2M	2.49G	44	500	4171	35200	I	good
8/0	sessmgr	277	20%	100%	593.7M	2.49G	43	500	4176	35200	I	good
8/0	sessmgr	288	23%	100%	591.9M	2.49G	43	500	4177	35200	I	good
8/0	sessmgr	296	24%	100%	593.0M	2.49G	42	500	4170	35200	I	good
8/1	sessmgr	186	2.0%	100%	568.3M	2.49G	48	500	1701	35200	I	good
8/1	sessmgr	192	2.0%	100%	571.1M	2.49G	46	500	1700	35200	I	good
8/1	aaamgr	200	1.0%	95%	147.3M	640.0M	22	500	--	--	-	good
8/1	sessmgr	210	2.1%	100%	567.1M	2.49G	46	500	1707	35200	I	good
8/1	aaamgr	216	0.9%	95%	144.6M	640.0M	22	500	--	--	-	good
8/1	sessmgr	217	2.0%	100%	567.7M	2.49G	45	500	1697	35200	I	good
8/1	sessmgr	231	2.2%	100%	565.7M	2.49G	45	500	1705	35200	I	good
8/1	sessmgr	240	2.0%	100%	569.8M	2.49G	45	500	1702	35200	I	good
8/1	aaamgr	242	0.9%	95%	148.5M	640.0M	22	500	--	--	-	good
8/1	sessmgr	252	1.8%	100%	566.5M	2.49G	44	500	1704	35200	I	good
8/1	aaamgr	261	0.9%	95%	142.0M	640.0M	22	500	--	--	-	good
8/1	aaamgr	263	1.0%	95%	144.1M	640.0M	22	500	--	--	-	good
8/1	aaamgr	265	1.0%	95%	146.4M	640.0M	22	500	--	--	-	good
8/1	aaamgr	267	1.0%	95%	144.4M	640.0M	22	500	--	--	-	good
8/1	aaamgr	269	1.0%	95%	143.8M	640.0M	22	500	--	--	-	good
8/1	sessmgr	274	1.9%	100%	570.5M	2.49G	44	500	1704	35200	I	good
8/1	sessmgr	283	2.0%	100%	570.0M	2.49G	44	500	1708	35200	I	good
8/1	sessmgr	292	2.1%	100%	567.6M	2.49G	44	500	1703	35200	I	good

```

9/0 sessmgr      1 30% 100% 587.2M 2.49G 48 500 4161 35200 I good
9/0 diamproxy   1 5.2% 90% 37.74M 250.0M 420 1000 -- -- - good
9/0 sessmgr     14 25% 100% 587.4M 2.49G 48 500 4156 35200 I good
9/0 sessmgr     21 20% 100% 591.5M 2.49G 47 500 4156 35200 I good
9/0 sessmgr     34 23% 100% 586.5M 2.49G 48 500 4155 35200 I good
9/0 aaamgr      44 0.9% 95% 145.1M 640.0M 21 500 -- -- - good
9/0 sessmgr     46 29% 100% 592.1M 2.49G 48 500 4157 35200 I good

```

## 監控使用者

在DPC 9/1上未響應對sessmgr 242的主要209.165.201.3的身份驗證請求時，捕獲到呼叫設定，該主要209.165.201.3的身份驗證請求恰好其配對aamgr駐留在DPC 8/1上，因此確認3G失敗，因為8/1上無法到達AAA。它還確認，即使在此時間點之前209.165.201.3沒有任何AAASrv陷阱可到達，這並不意味著處理響應沒有問題該伺服器（如上所示，陷阱確實會啟動，但會在數小時後啟動）。

```

8/1 aaamgr      242 0.9% 95% 148.5M 640.0M 22 500 -- -- - good
9/1 sessmgr     242 20% 100% 589.7M 2.49G 43 500 4167 35200 I good

```

-----  
Incoming Call:  
-----

```

MSID/IMSI      :                               Callid       : 4537287a
IMEI           : n/a                          MSISDN       : n/a
Username       : 6664600074@cisco.com         SessionType  : ha-mobile-ip
Status         : Active                       Service Name : HAService
Src Context    : Ingress

```

-----  
INBOUND>>>> From sessmgr:242 sessmgr\_ha.c:880 (Callid 4537287a) 23:18:19:099 Eventid:26000(3)  
MIP Rx PDU, from 203.0.113.1:434 to 203.0.113.3:434 (190)  
Message Type: 0x01 (Registration Request)

<<<<OUTBOUND From aaamgr:242 aaamgr\_radius.c:370 (Callid 4537287a) 23:18:19:100  
Eventid:23901(6)  
RADIUS AUTHENTICATION Tx PDU, from 203.0.113.3:27856 to 209.165.201.3:1645 (301) PDU-  
dict=custom9  
Code: 1 (Access-Request)  
Id: 195  
Length: 301  
Authenticator: CD 59 0C 6D 37 2C 5D 19 FB 60 F3 35 23 BB 61 6B  
User-Name = 6664600074@cisco.com

INBOUND>>>> From sessmgr:242 mipha\_fsm.c:8438 (Callid 4537287a) 23:18:21:049 Eventid:26000(3)  
MIP Rx PDU, from 203.0.113.1:434 to 203.0.113.3:434 (140)  
Message Type: 0x01 (Registration Request)  
Flags: 0x02  
Lifetime: 0x1C20

<<<<OUTBOUND From sessmgr:242 mipha\_fsm.c:6594 (Callid 4537287a) 23:18:22:117 Eventid:26001(3)  
MIP Tx PDU, from 203.0.113.3:434 to 203.0.113.1:434 (104)  
Message Type: 0x03 (Registration Reply)  
Code: 0x83 (Mobile Node Failed Authentication)

\*\*\*CONTROL\*\*\* From sessmgr:242 sessmgr\_func.c:6746 (Callid 4537287a) 23:18:22:144 Eventid:10285  
CALL STATS: <6664600074@cisco.com>, msid <>, Call-Duration(sec): 0  
Disconnect Reason: MIP-auth-failure  
Last Progress State: Authenticating

**show sub [summary] smgr-instance X**

有趣的是，sessmgr 242的會話計數與其他正在工作的sessmgr類似。進一步調查發現，同樣在該機

箱上託管的4G呼叫能夠連線，因此它們彌補了3G移動IP呼叫無法連線的缺陷。可以確定，回退到中斷開始後的8小時，沒有此sessmgr 242的MIP呼叫，而回退到中斷開始前9小時，存在已連線的呼叫：

```
[local]PGW# show sub sum smgr-instance 242 connected-time less-than 28800 (8 hours)
Monday December 30 03:38:23 UTC 2013
```

```
Total Subscribers:          1504
Active:                      1504      Dormant:          0
hsgw-ipv4-ipv6:              0        pgw-pmip-ipv6:    98
pgw-pmip-ipv4:               0        pgw-pmip-ipv4-ipv6: 75
pgw-gtp-ipv6:                700      pgw-gtp-ipv4:     3
pgw-gtp-ipv4-ipv6:          628      sgw-gtp-ipv6:     0
..
ha-mobile-ip:                0        ggsn-pdp-type-ppp: 0
```

```
[local]PGW# show sub sum smgr-instance 242 connected-time less-than 32400 (9 hours)
Monday December 30 03:38:54 UTC 2013 ...
ha-mobile-ip: 63 ggsn-pdp-type-ppp: 0
```

## LTEeHRPDMIP

```
[local]PGW# show sub sum smgr-instance 272
Monday December 30 03:57:51 UTC 2013
hsgw-ipv4-ipv6: 0 pgw-pmip-ipv6: 125 pgw-pmip-ipv4: 0 pgw-pmip-ipv4-ipv6: 85 pgw-gtp-ipv6: 1530
pgw-gtp-ipv4-ipv6: 1126
ha-mobile-ip: 1103
```

```
[local]PGW# show sub sum smgr-instance 242
Monday December 30 03:52:35 UTC 2013
hsgw-ipv4-ipv6: 0 pgw-pmip-ipv6: 172 pgw-pmip-ipv4: 0 pgw-pmip-ipv4-ipv6: 115
pgw-gtp-ipv6: 1899
pgw-gtp-ipv4-ipv6: 1348
```

```
ha-mobile-ip: 447
```

## radius測試例項X驗證伺服器

8/1上的所有aamgrs都停用 — 無radius測試例項命令適用於其中任何aamgrs，但適用於8/0和其他卡上的aamgrs:

9/1 sessmgr	242	22%	100%	600.6M	2.49G	41	500	3989	35200	I	good
4/1 sessmgr	20	27%	100%	605.1M	2.49G	47	500	3965	35200	I	good
4/0 sessmgr	27	25%	100%	592.8M	2.49G	46	500	3901	35200	I	good
8/1 aaamgr	242	0.9%	95%	150.6M	640.0M	22	500	--	--	-	good
8/1 aaamgr	20	1.0%	95%	151.9M	640.0M	21	500	--	--	-	good
8/0 aaamgr	27	1.0%	95%	146.4M	640.0M	21	500	--	--	-	good

```
[Ingress]PGW# radius test instance 242 auth server 209.165.201.3 port 1645 test test
Monday December 30 01:03:08 UTC 2013
```

```
Authentication from authentication server 209.165.201.3, port 1645
Communication Failure: No response received
```

```
[Ingress]PGW# radius test instance 20 auth server 209.165.201.3 port 1645 test test
Monday December 30 01:08:45 UTC 2013
```

```
Authentication from authentication server 209.165.201.3, port 1645
Communication Failure: No response received
```

```
[Ingress]PGW# radius test instance 27 auth server 209.165.201.3 port 1645 test test
Monday December 30 01:11:40 UTC 2013
```

```
Authentication from authentication server 209.165.201.3, port 1645
Authentication Failure: Access-Reject received
Round-trip time for response was 16.8 ms
```

## show radius counters all

用於排除RADIUS故障的旗艦命令顯示大量超時正在快速增加：

```
[Ingress]PGW> show radius counters all | grep -E "Authentication server address|Access-Request
Timeouts"
```

```
Monday December 30 00:42:24 UTC 2013
```

```
Authentication server address 209.165.201.3, port 1645, group default
Access-Request Timeouts: 400058
Authentication server address 209.165.201.5, port 1645, group default
Access-Request Timeouts: 26479
```

```
[Ingress]PGW> show radius counters all | grep -E "Authentication server address|Access-Request
Timeouts"
```

```
Monday December 30 00:45:23 UTC 2013
```

```
Authentication server address 209.165.201.3, port 1645, group default
Access-Request Timeouts: 400614
Authentication server address 209.165.201.5, port 1645, group default
Access-Request Timeouts: 26679
```

```
[Ingress]PGW> show radius counters all
```

```
Monday December 30 00:39:15 UTC 2013
```

```
...
```

```
Authentication server address 209.165.201.3, port 1645, group default
Access-Request Sent: 233262801
Access-Request with DMU Attributes Sent: 0
Access-Request Pending: 22
Access-Request Retried: 0
Access-Request with DMU Attributes Retried: 0
Access-Challenge Received: 0
Access-Accept Received: 213448486
Access-Reject Received: 19414836
Access-Reject Received with DMU Attributes: 0
Access-Request Timeouts: 399438
Access-Request Current Consecutive Failures in a mgr: 3
Access-Request Response Bad Authenticator Received: 16187
Access-Request Response Malformed Received: 1
Access-Request Response Malformed Attribute Received: 0
Access-Request Response Unknown Type Received: 0
Access-Request Response Dropped: 9039
Access-Request Response Last Round Trip Time: 267.6 ms
Access-Request Response Average Round Trip Time: 201.9 ms
Current Access-Request Queued: 2
```

```
Authentication server address 209.165.201.5, port 1645, group default
```

```
Access-Request Sent: 27731
Access-Request with DMU Attributes Sent: 0
Access-Request Pending: 0
Access-Request Retried: 0
Access-Request with DMU Attributes Retried: 0
Access-Challenge Received: 0
Access-Accept Received: 1390
Access-Reject Received: 101
Access-Reject Received with DMU Attributes: 0
```

```
Access-Request Timeouts: 26240
Access-Request Current Consecutive Failures in a mgr: 13
Access-Request Response Bad Authenticator Received: 0
Access-Request Response Malformed Received: 0
Access-Request Response Malformed Attribute Received: 0
Access-Request Response Unknown Type Received: 0
Access-Request Response Dropped: 0
Access-Request Response Last Round Trip Time: 227.5 ms
Access-Request Response Average Round Trip Time: 32.3 ms
Current Access-Request Queued: 0
```

## 補救

在維護時段內，DPC從8遷移到10解決了問題，AAAAuthSvrUnreachable陷阱已停止，並且DPC 8為RMA'd，並且根本原因確定為DPC 8上的硬體故障（對於本文而言，該故障的詳細情況不重要）。

```
Mon Dec 30 05:58:14 2013 Internal trap notification 39 (AAAAuthSvrUnreachable) server 4 ip
address 209.165.201.3
Mon Dec 30 05:58:14 2013 Internal trap notification 39 (AAAAuthSvrUnreachable) server 2 ip
address 209.165.201.5
Mon Dec 30 05:58:27 2013 Internal trap notification 40 (AAAAuthSvrReachable) server 2 ip address
209.165.201.5
Mon Dec 30 05:58:27 2013 Internal trap notification 40 (AAAAuthSvrReachable) server 4 ip address
209.165.201.3
Mon Dec 30 05:59:14 2013 Internal trap notification 43 (AAAAccSvrReachable) server 5 ip address
209.165.201.5
Mon Dec 30 06:01:14 2013 Internal trap notification 39 (AAAAuthSvrUnreachable) server 4 ip
address 209.165.201.3
Mon Dec 30 06:01:27 2013 Internal trap notification 40 (AAAAuthSvrReachable) server 4 ip address
209.165.201.3

Mon Dec 30 06:01:28 2013 Internal trap notification 16 (PACMigrateStart) from card 8 to card 10

Mon Dec 30 06:01:49 2013 Internal trap notification 60 (CardDown) card 8 type Data Processing
Card
Mon Dec 30 06:01:50 2013 Internal trap notification 1504 (CiscoFruCardStatusChanged) FRU entity
Card : 10 operational status changed to Active
Mon Dec 30 06:01:50 2013 Internal trap notification 55 (CardActive) card 10 type Data Processing
Card
Mon Dec 30 06:01:50 2013 Internal trap notification 17 (PACMigrateComplete) from card 8 to card
10

Mon Dec 30 06:02:08 2013 Internal trap notification 5 (CardUp) card 8 type Data Processing Card
Mon Dec 30 06:02:08 2013 Internal trap notification 1502 (EntStateOperEnabled) Card(8) Severity:
Warning
Mon Dec 30 06:02:08 2013 Internal trap notification 93 (CardStandby) card 8 type Data Processing
Card

Mon Dec 30 06:08:41 2013 Internal trap notification 1504 (CiscoFruCardStatusChanged) FRU entity
Card : 08 operational status changed to Offline
Mon Dec 30 06:08:41 2013 Internal trap notification 60 (CardDown) card 8 type Data Processing
Card
Mon Dec 30 06:08:41 2013 Internal trap notification 1503 (EntStateOperDisabled) Card(8)
Severity: Critical

Mon Dec 30 06:09:24 2013 Internal trap notification 1505 (CiscoFruPowerStatusChanged) FRU entity
Card : 08 Power OFF
Mon Dec 30 06:09:24 2013 Internal trap notification 1504 (CiscoFruCardStatusChanged) FRU entity
Card : 08 operational status changed to Empty
Mon Dec 30 06:09:24 2013 Internal trap notification 7 (CardRemoved) card 8 type Data Processing
Card
```

Mon Dec 30 06:09:24 2013 Internal trap notification 1507 (CiscoFruRemoved) FRU entity Card : 08 removed  
 Mon Dec 30 06:09:24 2013 Internal trap notification 1505 (CiscoFruPowerStatusChanged) FRU entity Card : 08 Power OFF  
 Mon Dec 30 06:09:50 2013 Internal trap notification 1505 (CiscoFruPowerStatusChanged) FRU entity Card : 08 Power ON  
 Mon Dec 30 06:09:53 2013 Internal trap notification 1504 (CiscoFruCardStatusChanged) FRU entity Card : 08 operational status changed to Offline  
 Mon Dec 30 06:09:53 2013 Internal trap notification 8 (CardInserted) card 8 type Data Processing Card  
 Mon Dec 30 06:09:53 2013 Internal trap notification 1506 (CiscoFruInserted) FRU entity Card : 08 inserted  
 Mon Dec 30 06:10:00 2013 Internal trap notification 1504 (CiscoFruCardStatusChanged) FRU entity Card : 08 operational status changed to Booting  
 Mon Dec 30 06:11:59 2013 Internal trap notification 1504 (CiscoFruCardStatusChanged) FRU entity Card : 08 operational status changed to Standby  
 Mon Dec 30 06:11:59 2013 Internal trap notification 5 (CardUp) card 8 type Data Processing Card  
 Mon Dec 30 06:11:59 2013 Internal trap notification 93 (CardStandby) card 8 type Data Processing Card

[local]PGW# show rct stat  
 Wednesday January 01 16:47:21 UTC 2014

RCT stats Details (Last 2 Actions)

Action	Type	From	To	Start Time	Duration
Migration	Planned	8	10	2013-Dec-30+06:01:28.323	21.092 sec
Shutdown	N/A	8	0	2013-Dec-30+06:08:41.483	0.048 sec