

排除AAAAccSrvUnreachable和AAAAuthSrvUnreachable陷阱故障

目录

[简介](#)

[陷阱触发器](#)

[在AAAMGR流程方法中连续失败](#)

[保持连接方法](#)

[故障排除命令/方法](#)

[Radius配置基础](#)

[show task resources facility aaamgr all](#)

[show radius counters { { all |服务器](#)

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

[ping](#)

[traceroute](#)

[radius测试实例x auth {radius group](#)

[radius测试实例x accounting {radius group](#)

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

[监控用户](#)

[数据包捕获](#)

[补救](#)

[最终示例](#)

[相关的思科支持社区讨论](#)

SNMPAAAAccSrvUnreachableAAAAuthSrvUnreachable(RADIUS)

RADIUS//

LABIP

//RADIUS

AAAMGR

aaamgraaamgrradiusradiusaaamgrsessmgr“show task resources”aaamgraaamgrradiusaaamgr —
“show radius counters”“Access-Request Timeout”

“Access-Request Current Consecutive Failures in a mgr”“show radius counters”“show radius
accountingauthenticationservers detail”RADIUS“Active”“Not Responding”SNMP 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
```

如果此计数器达到配置的值（默认值=4），且从未重置，则按可配置：（请注意，方括号[]用于指示可选限定符，在这些情况下，会捕获故障排除记帐（如果未指定记帐，则默认使用身份验证）

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

然后，在配置的时间段（分钟）内，此服务器被标记为“关闭”：

radius [accounting] deadtime 10

SNMP陷阱和日志也会被触发，例如分别针对身份验证和/或记帐：

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

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

陷阱指示服务器无法访问。记下所有模式。例如，它是发生在一台服务器上还是另一台服务器上，还是发生在所有服务器上？弹跳的频率是多少？

另请注意，触发此陷阱所需的只是一个陷阱失败，因此，此陷阱的棘手之处在于，它不表示问题的程度。它可能非常广泛或非常微小，这取决于操作人员的判断，而本文将讨论如何找到答案。

show snmp trap statistics将报告自启动以来触发的次数，即使较旧的陷阱早已被删除。此示例显示记帐不可达问题：

```
[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 |

请注意，上例中报告的aaamgr是#231。这是驻留在系统管理卡(SMC)上的ASR 5000上的管理aamgr。此输出中具有欺骗性的是，当单个aamgr或aaamgr遇到可达性问题时，日志中报告的实例编号是management aamgr实例，而不是遇到该问题的特定实例。这是因为，如果许多实例遇到可接通性问题，那么如果它们都报告为可接通性问题，日志记录会很快填满，因此设计是一般地报告管理实例，如果不知道，肯定会欺骗用户。在故障排除部分，将提供有关如何确定哪个aamgr发生故障的更多详细信息。从StarOS 17和v18+的某些版本开始，此行为已更改，因此，具有连接问题（如SNMP陷阱中报告的）的对应aamgr实例编号在具有特定ID(Cisco CDETS CSCum84773)的日志中报告，但仍仅报告此情况的第一次发生（跨多个aamgr）。

管理aamgr是最大会话管理器实例编号+ 1，在ASR 5500上，它是385（用于数据处理卡）或1153（用于DPC 2）。

如图所示，管理aamgr负责处理操作员/管理员登录，以及处理从RADIUS服务器本身发起的授权请求的更改。

继续，“show radius accounting（或authentication）servers detail”命令将指示与陷阱/日志对应的状态更改的时间戳Down(提醒：之前定义的Not Responding只是一个aamgr获得超时，而Down是单个aamgr获得每个配置足够的连续超时以触发Down)

```
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
```

如果只配置了一台服务器，则不会将其降级，因为这对成功建立呼叫至关重要。

值得一提的是，在detect-dead-server配置行上可以配置另一个参数，称为“response-timeout”。指定时，服务器仅在同时满足连续故障和响应超时条件时才会被降级。response-timeout指定接收到发送到特定服务器的所有请求的NO响应的时间段。（请注意，当收到响应时，此计时器将不断重置。）当服务器或网络连接完全关闭，而部分受损/降级时，会出现这种情况。

这种情况的使用情形是，流量突发导致连续失败触发，但不需要立即将服务器标记为关闭。相反，只有在特定时间段内没有收到响应时才会将服务器降级，这实际上表示真正的服务器不可达。

刚刚讨论的控制RADIUS状态机更改的方法取决于查看所有aamgr进程和查找触发重试失败情况的进程。这种方法受故障随机性的影响，可能不是理想的故障检测算法。但它特别擅长发现，在其他所有公司都运转良好的情况下，这些公司会破产。

保持连接方法

检测RADIUS服务器可达性的另一种方法是使用虚拟保活测试消息。这包括持续发送假的RADIUS消息，而不是监控实时流量。此方法的另一个优势是它始终处于活动状态，而在aamgr方法中，其中可能存在未发送RADIUS流量的时段，因此无法知道这些时段中是否存在问题，从而在尝试开始时导致延迟检测。此外，当服务器被降级时，这些keepalive会继续发送，以便服务器能够尽快被标记为up。此方法的缺点是，它忽略了与可能遇到问题的特定aaamgr实例相关的问题，因为它使用管理aaamgr实例来测试消息。

以下是与此方法相关的各种可配置设备：

```
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”会打开keep-alive方法，而不是aamgr方法中的连续故障。在上例中，系统每30秒发送一条测试消息，其中用户名为Test-Username，密码为Test-Username，如果未收到响应，则每3秒重试一次，最多重试3次，然后将服务器标记为关闭。一旦得到第一次响应，它就会再次标记。

以下是上述设置的身份验证请求/响应示例：

```
<<<<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
```

与aamgr方法中的连续故障一样，SNMP陷阱用于表示不可达/关闭和可达/上半径状态：

```
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”中还有一个部分用于跟踪身份验证和记帐的keepalive请求 — 以下是身份验证计数器：

```
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

既然已经解释了AAA不可达陷阱的触发因素，下一步就是了解各种故障排除命令以确定影响并尝试找出根本原因。不可达性是一个非常宽泛的术语。它不解释不可达性在网络、服务器或ASR中的位置。例如，是否知道这些请求是否首先被发送？服务器是否收到请求？它是否响应了请求。响应是否将其返回到ASR，如果是，它们是在内部路径（即流）上处理或丢弃的。本节尝试说明如何回答这些问题。

Radius配置基础

首先，您需要熟悉一些有关RADIUS配置的基础知识。RADIUS的大多数配置都在一个专门命名的组中，并且所有情景都有一个默认组，可以按如下方式进行配置。很多情况下，配置只有一个组，即默认组。

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

如果使用特定命名的aaa组，则用户配置文件或应用点名称(APN)中配置的以下语句（取决于呼叫控制技术）会指向它们，例如：

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

注意：系统首先检查分配给用户的特定aaa组，然后检查AAA组默认值，以查找未在特定组中定义的其他可配置。

以下是一些有用的命令，用于汇总分配给各种aaa组配置中所有可配置设备的所有值。这允许快速查看包括默认值在内的所有可配置设备，而无需手动检查配置，并且可能有助于避免在假设某些设置时出错。以下命令报告所有情景：

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

最重要的可配置是RADIUS访问和记帐服务器本身。示例如下：

```
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
```

请注意限制每秒每个aamgr发送到服务器的请求数的最大速率功能

此外，还需要定义NAS IP地址，该地址是接口上发送RADIUS请求和接收响应的环境中的IP地址。如果未定义，则不发送请求，并且监控用户跟踪可能不会发出明显错误（未发送RADIUS请求，也未指示原因）。

```
radius attribute nas-ip-address address 10.211.41.129
```

请注意，由于身份验证和记帐通常由同一服务器处理，因此RADIUS服务器上使用不同的端口号来区分身份验证和记帐流量。对于ASR5K端，未指定UDP源端口号，由机箱按照相应的顺序选择（稍后将进一步介绍）。

通常，为冗余目的指定多个访问和记帐服务器。可以配置轮询或优先顺序：

```
radius [accounting]算法{first-server |轮询}
```

第一个服务器选项会导致所有请求都发送到具有最低优先级的服务器。只有在重试失败或更糟糕的情况下，服务器被降级时，才尝试使用下一个优先级的服务器。下面详细介绍。

当发送RADIUS（记帐或访问）请求时，会收到回复。在超时期间（秒）内未收到应答时：

radius [accounting] timeout 3

重新发送请求的次数最多为指定次数：

radius [accounting] max-retries 5

这意味着，请求可以发送总最大重试次数+ 1次，直到在尝试的特定RADIUS服务器上放弃。此时，它会按顺序尝试同一序列到下一个RADIUS服务器。如果每台服务器都尝试了最大重试次数+ 1次而没有响应，则呼叫会被拒绝，假设到此为止没有其他故障原因。

如图所示，即使身份验证和记帐由于所有服务器超时而失败，用户仍可通过可配置设备进行访问，但商业部署不太可能实施以下操作：

radius allow [accounting] authentication-down

此外，还有一些可配置设备可以限制特定请求在所有已配置服务器之间的绝对传输总数，并且默认情况下禁用这些配置：

radius [accounting] max-transmissions 256

例如，如果此设置为= 1，则即使有辅助服务器，也从不尝试它，因为只尝试一次特定用户设置尝试。

show task resources facility aaamgr all

每个aamgr进程与关联的会话管理器进程配对并“工作”（负责整体呼叫处理），并位于不同的数据包服务卡(PSC)或数据处理卡(DPC)上，但使用相同的实例ID。此外，在本示例输出中，请注意在ASR 5000的系统管理卡(SMC)(或ASR 5500的管理输入输出卡(MIO))上运行的特殊aamgr实例231，它不处理用户请求，但会用于radius测试命令（有关该的更多详细信息，请参阅后面的章节）AND操作员CLI登录处理。

在此代码段中，位于PSC 13上的aaamgr 107负责处理位于PSC 1上的成对sessmgr 107的所有RADIUS处理。aaamgr 107的可达性问题影响sessmgr 107上的呼叫。

| cpu | facility | task | cputime | | memory | | files | | sessions | | S | status |
|------|----------|------|---------|------|--------|--------|-------|------|----------|------|---|--------|
| | | | inst | used | allc | used | alloc | used | allc | used | | |
| 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，请注意，与会话计数相关的其他会话相比，aaamgr 92的问题正在影响成对的会话管理器，这很容易看到：

| cpu | facility | task | cputime | | memory | | files | | sessions | | S | status |
|------|----------|------|---------|------|--------|--------|-------|------|----------|-------|---|--------|
| | | | inst | used | allc | used | alloc | used | allc | used | | |
| 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 <aaamgr #>] |摘要}

首先要熟悉的命令是“show radius counters”的变体

此命令会返回许多用于排除RADIUS故障的有用计数器。“show radius counters all”命令对于在服务器上跟踪成功和失败非常有价值，而且必须了解组成此命令的各种计数器的含义，因为它可能并不明显。该命令对上下文敏感，因此必须在定义AAA组的同一上下文中运行。

重要说明：在未监控的时间段内，很难从计数器值或计数器之间的关系中得出任何结论。要得出准确的结论，最佳方法是重置计数器并在发生故障时的一段时间内监控它们。

在以下输出中，请注意“已发送访问请求”= 1，而“重试访问请求”= 3。因此，对特定RADIUS服务器的任何给定新请求只计一次，并且所有重试次数单独计算。在本例中，这总共是3 + 1 =发送的4个访问请求。请注意计数器“Access-Request Timeouts”= 1。仅当所有重试失败时，才会出现单次超时，因此，在这种情况下，3次重试而无响应将导致1次超时（而非4次）。在成功或所有尝试都失败之前，所有已配置的服务器都会发生这种情况。因此，请注意为每台服务器单独跟踪的计数器。以下是一个示例，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
```

另请注意，超时不计为故障，结果是，如果有超时，接收的Access-Accept和Access-Reject的数量将不会加到Access-Request Sent。

对这些计数器的分析可能并不完全简单。例如，对于移动IP(MIP)协议，由于身份验证失败，因此

不发送MIP注册应答(RRP)，并且由于未收到MIP RRP，移动设备可以继续发起新的MIP注册请求(RRQ)。每个新MIP RRQ使PDSN发送新的身份验证请求，该请求本身可以有其自己的一系列重试。这在数据包跟踪顶部的Id字段中可见 — 每组重试都是唯一的。结果是“已发送”、“重试”和“超时”的计数器可能比收到的呼叫数的预期值高很多。可以启用一个选项来最小化这些额外重试次数，并且可以在外部代理(FA)(但不能在家庭代理(HA))服务中设置：“authentication mn-aaa <此处选择> optimize-retries”

其他一些有用计数器：

“Access-Request Response Dropped” — 如果呼叫在等待对身份验证请求的响应时未能设置，则会发生。

“Access-Request Response Last Round Trip Time” (访问请求响应上次往返时间) — 表示终端之间的任何延迟，但显然不表示延迟可能在何处。

“Access-Request Current Consecutive Failures in a mgr”与在AAA Unreachable陷阱触发器的第一部分讨论的内容有关。它表示连续超时计数最高的aaamgr。

“当前访问/记帐请求已排队”表示未响应且仍保留在队列中的请求 (记帐允许在身份验证不响应的情况下无限期地建立队列)

报告AAA不可达时，最常见的情况是访问超时和/或响应丢弃也在发生，而访问响应跟不上请求。

如果可以访问专用技术支持模式，则可以在aaamgr实例级别进行进一步调查，以确定一个或多个特定aagr是否是导致总体“不良”计数增加的原因。例如，查找位于特定PSC/DPC上的aaamgr，查找计数高或单个aaamgr或随机aaamgr出现问题的情况 — 查找模式。如果所有或大多数组件都出现问题，则根本原因可能性增加，即机箱外部或机箱上出现大规模问题。在这种情况下，应执行常规运行状况检查。

以下输出示例显示了特定aamgr的记帐问题。(此问题被证明是ASR5K和RADIUS服务器之间防火墙中的一个Bug，该防火墙阻止来自特定aamgr实例(114)端口的流量。)在三周内，仅收到48个响应，但超过100,000个超时 (不包括重新传输)。

```
[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

```

总之，请确定哪些计数器在递增，哪些服务器在递增，以什么速度递增。

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

虽然检查此命令的所有多余输出已超出本文的范围，但有几个示例值得查看。与任何其他故障排除一样，比较认为是好的实例与错误的实例之间的输出通常会显示报告值存在明显差异。这可能反映在请求总数、失败/成功率、身份验证取消等。提醒您，请务必清除会话子系统（一个实例无法清除，必须全部清除），以消除可能提供当前状态模糊画面的任何历史记录。

继续前面提到的有关单个aamgr记帐失败的相同问题，此处显示来自同一问题的不同节点的输出，但不同的会话实例36除外。请注意故障aamgr的所有相关字段，以及这些值如何随着命令的两次捕获而逐渐增加。同时，实例37的输出显示为工作aamgr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 gtpb charg          0 Current gtpb charg
0 Total gtpb charg success  0 Total gtpb charg failure
0 Total gtpb charg cancelled 0 Total gtpb charg purged
0 Total gtpb sec charg      0 Total gtpb 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 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
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
...

```

还应运行show task resources，检查所有会话中是否存在任何不均衡的会话计数（使用的列）。如果找到任何，请使用此命令检查这些会话的配对aaamgr，以查看是否有任何字段超出行——如果问题是由RADIUS引起的，则很有可能找到某些内容。

在上一节的show task resources示例中，sessmgr 92上的会话计数显著降低，该会话计数与aaamgr 92配对。show session子系统的输出显示最大未处理计数和aaa auth清除计数器总数的显著增加，以及当前最大未处理计数的提高。您可以在机箱和/或Notepad++或其他强大的搜索编辑器上使用grep功能来快速分析数据。多次运行命令，查看哪些值在增加或保持提升：

```

[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会测试基本连接，以查看AAA服务器是否可以访问。ping可能需要使用src关键字来源，具体取决于网络，并且需要从AAA环境中完成，才能获得值。如果对服务器执行ping操作失败，则尝试ping中间元素，包括情景中的下一跳地址，确认如果ping操作失败，则存在指向下一跳地址的ARP条目。Traceroute还有助于解决路由问题。

```
[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 test instance x auth {radius group <group> |全部 | server <IP> port <port>}
<username> <password>
```

```
radius test instance x accounting {radius group <group name> |全部 | server <IP>
port <port>}
```


通过访问技术支持测试命令，您可以进一步测试特定aamgr是否能够访问任何RADIUS服务器。对于基本RADIUS连接测试，请使用此命令的通用版本，该版本不指定任何特定实例#，但默认使用管理实例。如果失败，则可能指向独立于特定实例的更广泛问题。

此命令发送基本身份验证请求或记帐启动和停止请求，并等待响应。对于身份验证，请使用任何用户名和密码，在这种情况下，将需要拒绝响应，确认RADIUS正在按设计工作，或者可以使用已知工作用户名/密码，在这种情况下，应接收接受响应

以下是监控协议的输出示例，并在实验机箱上运行命令的身份验证版本：

```
[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
```

以下是来自实时机箱的示例：

```
<<<<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
```

以下是运行命令的记帐版本的输出示例。不需要密码。

```
[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
```

以下输出适用于刚才提到的与特定RADIUS记帐服务器的连接中断的相同aamgr实例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 |

此命令报告已配置的NAS IP地址用于连接RADIUS服务器的网络处理器单元(NPU)流ID和UDP端口。这在输出的aaa group default部分中报告。当然，如果需要将数据包捕获中的RADIUS数据包与特定的aaamgr实例#匹配，端口号将非常有用。（请注意，NPU流非常复杂，不是本文讨论的内容，而是支持工程师能够进一步调查的实体。）它还跟踪对服务器的未处理请求。在本文中使用的同一示例问题中，只有特定RADIUS服务器<==> NAS IP / UDP端口对发生故障，如突出显示所示。

```
[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>

监控用户

监控用户可用于确定是否至少尝试了身份验证以及是否正在为受监控的呼叫处理应答。打开代表 Sessmgr发件人信息的选项“S” — 有效报告正在处理相关消息的sessmgr或aamgr实例编号。以下是 HA上MIP调用的示例 连接到sessmgr / aamgr实例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

本文最后还给出了一个故障示例。

数据包捕获

有时，ASR上的信息不足，无法确定为什么会出现连通性问题，在这种情况下，需要捕获数据包。排除单个用户问题时，在跟踪中识别各个数据包应该很容易。否则，如果问题与特定端口/aamgr实例相关联，则了解UDP端口在特定aamgr实例# <==> RADIUS服务器对的任一端使用可能很有帮助。可能需要尝试在网络的多个位置捕获数据包，以确定数据包被丢弃的位置。在本文所分析的问题中，数据包捕获是ASR和RADIUS服务器之间传输路径中恰当位置的数据包捕获，是解决问题的突破口。

补救

最后一部分提供一些修复RADIUS连接问题的想法。这些列表不按任何特定顺序显示，而只是在故障排除过程中要考虑的列表。

如果RADIUS服务器过载，则可以通过为“radius(accounting)max-outstanding”配置的值（默认值256）降低负载，该值对任何给定aamgr进程的未处理（未应答）请求数设置限制。如果达到限制，日志可能会指示：“无法为RADIUS身份验证服务器x.x.x.x:1812分配消息ID”。

对特定服务器进行速率限制的RADIUS消息也可以通过相应服务器配置行的rate-limit关键字帮助减少负载。

有时，这不是连接问题，而是会计流量增加问题，这不是RADIUS持久性的问题，而是指向另一个区域，如增加的ppp重新协商，这会导致更多计费开始和停止。因此，您可能需要排除RADIUS之外的故障，以查找所观察到的症状的原因或触发器。

如果在故障排除过程中决定出于任何原因从实时服务器列表中删除RADIUS身份验证或记帐服务器，则会有（非配置）命令，该命令将使服务器无限期停止服务，直到需要将其恢复服务。这比必须手动从配置中删除它更简洁：

```
{ | enable} radius [accounting] server 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迁移或线卡切换通常可以清除问题，因为迁移会导致卡上的进程重新启动，包括 npumgr，npumgr是NPU流不时出现问题的原因。

但是，与上述aaamgr 92示例的有趣转折是，AAA无法到达故障实际上是在完成PSC迁移时启动的。这是由于PSC迁移完成时NPU流丢失而触发的，使PSC 11处于备用状态。一小时后，当它激活时，aamgr 92丢失流的实际影响就开始了。如果没有技术支持的帮助，此类问题将很难排除。

```
[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

```

该问题通过端口切换暂时解决，导致PSC卡（对于aamgr 92缺少NPU流）不再连接到活动线卡。

```

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

```

最后一个故障陷阱：

```
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

```

同样，重新启动“卡住”的特定映像也可能解决问题，但是，由于技术支持涉及受限的技术支持命令，因此应执行此活动。在前面的show task resources部分介绍的aaamgr 92示例中，这是尝试的，但没有帮助，因为根本原因不是aaamgr 92，而是aaamgr 92所需的缺失NPU流（它是NPU问题

,而不是aaamgr问题)。以下是尝试的相关输出。运行“show task table”以显示进程id和任务实例#92的关联。

```
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      0    2887
```

最终示例

这是实际网络中发生实际故障的最后一个示例，它汇集了本文讨论的许多故障排除命令和方法。请注意，此节点处理3G MIP和4G长期演进(LTE)以及演进的高速分组数据(eHRPD)呼叫类型。

show snmp trap history

仅通过陷阱，可以确认起始点与客户报告的19:25 UTC匹配。另外，请注意主服务器209.165.201.3的**AAAAuthSvrUnreachable**陷阱在数小时后才开始发生(不清楚原因，但请注意；但是记帐无法访问该服务器立即开始)

```
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
209.165.201.3
```

显示任务资源

输出显示DPC 8/1上的呼叫数要少得多。仅根据此，如果不进行任何进一步分析，就可以建议DPC 8上存在问题，并提出迁移到备用DPC的选项。但是，必须确认实际用户影响是什么 — 在这些情况下，用户通常会在后续尝试中成功连接，因此对用户影响不太大，并且他们可能不会向提供商报告任何情况，假设也没有发生用户平面故障（这取决于故障情况）。

| | | | | | | | | | | | | |
|-----|-----------|-----|------|------|--------|--------|-----|------|------|-------|---|------|
| 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

```

监控用户

在DPC 9/1上，DPC 9/1上的sessmgr 242的主209.165.201.3的身份验证请求未响应时，捕获到呼叫设置，该呼叫设置碰巧驻留在DPC 8/1上，确认了由于8/1上的AAA无法访问而导致3G故障。它还确认，即使没有209.165.201.3的aaaauthSrvUnreachable陷阱，但这并不意味着处理该服务器的响应时没有问题（如上所示，陷阱确实会启动，但几小时后）。

```

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的会话计数与其他工作会话类似。进一步调查显示，4G呼叫（也托管于此机箱上）能够连接，因此它们弥补了3G移动IP呼叫无法连接的问题。可以确定，在停机开始后8小时内，此sessmgr 242没有MIP呼叫，而在停机开始前9小时，有连接的呼叫：

```
[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
```

MIPLTEeHRPDMIP

```
[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测试实例X身份验证服务器

8/1上的所有aamgrs均已失效 — 没有radius测试实例命令适用于任何aaamgrs，但8/0卡和其他卡上的aaamgrs确实有效：

| | | | | | | | | | | | |
|-------------|-----|------|------|--------|--------|----|-----|------|-------|----|------|
| 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

排除RADIUS故障的旗舰命令显示大量超时，并且会迅速增加：

```
[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
```

补救

在维护时段，DPC从8迁移到10解决了问题，AAAAuthSvrUnreachable陷阱停止，DPC 8是RMA'd，根本原因被确定为DPC 8上的硬件故障（出于本文的目的，该故障的详细信息并不重要）。

```
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 |