# Fehlerbehebung: AAAccSrvUnreachable und AAAuthSrvUnreachable Traps

## Inhalt



## Einführung

In diesem Artikel wird beschrieben, wie SNMP-Traps für AAAccSrvUnreachable und AAAuthSrvUnreachable behoben werden, die aufgrund von Erreichbarkeitsproblemen mit einem RADIUS-Server (Remote Authentication Dial-In User Service) ausgelöst werden, der zum Authentifizieren von Teilnehmern (oder Operatoren, die sich beim Knoten anmelden, verwendet wird, aber nicht behandelt. Es gibt zwei Ansätze, mit denen bestimmt werden kann, wann eine dieser Traps ausgelöst wird. In diesem Artikel wird erläutert, welche Bedingungen diese Traps auslösen und welche Ansätze zur Fehlerbehebung und Datenerfassung verwendet werden können, um die Ursache zu ermitteln und diese zu beheben. Darüber hinaus werden einige mögliche Abhilfemaßnahmen erörtert, die in Betracht gezogen werden können.

Beachten Sie, dass das Ergebnis der Unerreichbarkeit Anrufausfälle oder Abrechnungsfehler ist, genauso wie wenn Radius-Antworten Absagen anstatt Akzeptanzen sind. Die Erfolgs-/Fehlerquote (Authentifizierung) wird unabhängig von der Timeout-/Erreichbarkeit gemessen (dafür gibt es Traps und Alarme) und kann sicherlich selbst analysiert werden. Der Schwerpunkt dieses Artikels liegt jedoch auf dem Erreichbarkeitsproblem und nicht auf dem Ablehnungsproblem.

Beispielausgabe aus der LAB und tatsächliche Tickets werden durchgängig verwendet, um die Diskussionen zu beleben. In diesem Artikel werden öffentliche IP-Adressen als **gefälschte** Adressen angezeigt.

## Trap-Trigger

Es stehen zwei verschiedene Modelle/Algorithmen/Ansätze zur Auswahl, um den Status eines Radius-Servers zu bestimmen und einen anderen Server zu testen, wenn Fehler auftreten:

## Folgeausfälle in einem einheitlichen Prozessansatz

Der ursprüngliche Ansatz und der häufiger von den Betreibern verwendete Ansatz besteht darin, die Anzahl der Fehler in einer Reihe für einen bestimmten Prozess nachzuverfolgen. Ein Aaamgr-Prozess ist für die Verarbeitung und den Austausch von RADIUS-Nachrichten mit einem RADIUS-Server verantwortlich. In einem Chassis werden viele Aaamgr-Prozesse vorhanden sein, die jeweils mit Sessmgr-Prozessen (den Hauptprozessen für die Anrufsteuerung) gekoppelt sind. (Alle aamgr-Prozesse mit dem Befehl "show task resources" (Taskressourcen anzeigen)) Daher verarbeitet ein bestimmter aamgr-Prozess RADIUS-Meldungen für viele Anrufe, nicht nur einen einzelnen Anruf. Dieser Algorithmus beinhaltet die Nachverfolgung der Anzahl von Anrufen, die ein bestimmter AMAG-Prozess nicht in der Lage war, auf dieselbe Anforderung zu reagieren, die er erneut senden musste - ein "Access-Request-Timeout", wie in "show radius-Zähler" angegeben.

Der entsprechende Zähler "Access-Request Current Consecutive Failures in a mgr", auch aus "show radius zählers", wird erhöht, wenn dies auftritt, und der Befehl "show radius accounting (or authentication) servers detail" gibt die Zeitstempel für die Änderung des Radius-Status von Active zu Not Responding an (aber kein SNMP-Trap oder -Protokolle werden für nur einen Ausfall generiert). Hier ein Beispiel für die Radius-Accounting:

```
[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
```

Wenn dieser Zähler den konfigurierten Wert (Standard = 4) erreicht, ohne jemals zurückgesetzt zu werden, kann Folgendes konfiguriert werden: (Beachten Sie, dass die Klammern [ ] verwendet werden, um den optionalen Qualifizierer anzugeben, und in diesen Fällen die Fehlerbehebungsabrechnung erfasst (Authentifizierung ist der Standardwert, wenn Accounting nicht angegeben ist).

radius [Accounting] zur Erkennung von ununterbrochenen Serverausfällen 4

Anschließend wird dieser Server für den konfigurierten Zeitraum (Minuten) mit "Down" markiert:

radius [Accounting] - Zeitraum 10

Ein SNMP-Trap und Protokolle werden ebenfalls ausgelöst, z. B. für die Authentifizierung bzw. die Abrechnung:

```
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
```

Die Traps zeigen an, dass der Server nicht erreichbar ist. Notieren Sie sich alle Muster. Zum Beispiel, geschieht es mit einem Server oder einem anderen oder mit allen Servern, und wie oft wird das Bounce-System gestartet - geschieht es kontinuierlich oder gelegentlich?

Beachten Sie auch, dass es für die Auslösung dieser Falle nur nötig ist, dass ein Spieler ausfällt. Der schwierige Teil an dieser Falle ist, dass er nicht das Ausmaß des Problems angibt. Es könnte sehr umfangreich oder sehr klein sein - das ist Sache des Operators zu bestimmen, und Ansätze zur Feststellung, dass es in diesem Artikel diskutiert werden.

show snmp trap statistics gibt die Anzahl der Auslöser seit dem Hochfahren an, selbst wenn die älteren Traps seit langem gelöscht wurden. Dieses Beispiel zeigt ein Problem, das nicht erreichbar ist:

```
[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
```

Beachten Sie, dass der im obigen Beispiel gemeldete AMGR #231 ist. Dies ist der Management-Manager des ASR 5000, der sich auf der Systemverwaltungskarte (SMC) befindet. Täuschend an dieser Ausgabe ist, dass die in den Protokollen gemeldete Instanzennummer die Verwaltungsinstanz ist und nicht die Instanz(n), bei der das Problem auftritt, wenn ein einzelner Administrator oder mehrere Administratoren Probleme mit der Erreichbarkeit feststellen. Dies ist darauf zurückzuführen, dass bei vielen Fällen Probleme mit der Erreichbarkeit auftreten, die Protokollierung schnell aufgefüllt würde, wenn sie alle als solche gemeldet würden. Daher wurde das Design verwendet, allgemein über die Management-Instanz zu berichten, die, wenn man das nicht weiß, dies sicherlich täuschen würde. Im Abschnitt "Fehlerbehebung" finden Sie weitere Details dazu, wie Sie bestimmen können, welche Adapter fehlerhaft sind/sind.  Ab einigen Versionen von StarOS 17 und v18+ wurde dieses Verhalten so geändert, dass die entsprechende Anzahl an Instanzen mit Verbindungsproblemen (wie in SNMP-Traps berichtet) in den Protokollen mit der jeweiligen ID (Cisco CDETS CSCum84773) gemeldet wird, obwohl immer noch nur das erste Auftreten (über mehrere Entfernungen hinweg) dieser Ereignisse gemeldet wird.

Der Management-Manager ist die maximale Sessmgr-Instanznummer + 1, bei einem ASR 5500 ist er 385 für Data Processing Card (DPC) oder 1153 (bei DPC 2).

Als Vorsitzender ist der Management Manager für die Verarbeitung von Operator-/Administrator-Anmeldungen sowie die Bearbeitung von Autorisierungsanfragen verantwortlich, die von RADIUS-Servern selbst initiiert wurden.

Im weiteren Verlauf gibt der Befehl show radius accounting (or authentication) servers detail die Zeitstempel der Statusänderungen zu Down an, die den Traps/Protokollen entsprechen (Erinnerung: Bei der zuvor definierten Nichtantwort erhält nur ein einziger Administrator eine Zeitüberschreitung, während bei "Down" ein einziger Administrator genügend aufeinander folgende Timeouts pro Konfiguration erhält, um den Ausfall auszulösen.)

```
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
```

Wenn nur ein Server konfiguriert ist, wird er nicht markiert, da dies für eine erfolgreiche Anrufeinrichtung entscheidend wäre.

Erwähnenswert ist, dass es einen weiteren Parameter gibt, der in der Konfigurationszeile "detect-disabled-server" konfiguriert werden kann, die als "response-timeout" bezeichnet wird. Wenn angegeben, wird ein Server nur dann als ausgefallen gekennzeichnet, wenn die aufeinander folgenden Ausfälle und die Bedingungen für die Reaktion-Timeout erfüllt sind. Das Response-

Timeout gibt einen Zeitraum an, in dem KEINE Antworten auf ALLE an einen bestimmten Server gesendeten Anfragen empfangen werden. (Beachten Sie, dass dieser Timer bei Erhalt der Antworten fortlaufend zurückgesetzt wird.) Diese Bedingung ist zu erwarten, wenn entweder ein Server oder die Netzwerkverbindung komplett ausfällt, im Vergleich zu teilweise kompromittierten/beschädigten Verbindungen.

Der Anwendungsfall hierfür wäre ein Szenario, in dem ein Datenverkehrsspitz die aufeinander folgenden Ausfälle auslöst, ein unmittelbar daraus resultierendes Markieren eines Servers jedoch nicht erwünscht ist. Stattdessen wird der Server erst nach Ablauf einer bestimmten Zeitspanne gekennzeichnet, wenn keine Antworten empfangen werden. Dies bedeutet, dass der Server nicht erreichbar ist.

Diese Methode, die gerade besprochen wurde, um Änderungen des Radius-State-Rechners zu steuern, hängt davon ab, ob alle aamgr-Prozesse untersucht und eine ermittelt werden muss, die die Bedingung fehlerhafter Neuversuche auslöst. Diese Methode unterliegt bis zu einem gewissen Grad einer Zufälligkeit von Ausfällen und ist daher möglicherweise nicht der ideale Algorithmus zur Erkennung von Ausfällen. Aber es ist besonders gut, wenn man einen oder mehrere Agenten findet, die kaputt sind, während alle anderen gut arbeiten.

## Keepalive-Ansatz

Eine andere Methode zur Erkennung der Verfügbarkeit von Radius-Servern ist die Verwendung von Dummy-Keepalive-Testnachrichten. Dies beinhaltet das permanente Senden gefälschter Radius-Meldungen, anstatt Live-Datenverkehr zu überwachen. Ein weiterer Vorteil dieser Methode besteht darin, dass sie immer aktiv ist, im Vergleich zu den aufeinander folgenden Fehlern in einem aamgr-Ansatz, in dem es Zeiträume geben kann, in denen kein Radius-Datenverkehr gesendet wird, und daher ist es nicht möglich zu wissen, ob in diesen Zeiten ein Problem besteht, was zu einer verzögerten Erkennung führt, wenn die Versuche beginnen. Auch wenn ein Server ausgefallen ist, werden diese Keepalives weiterhin gesendet, sodass der Server so schnell wie möglich markiert werden kann. Der Nachteil dieses Ansatzes besteht darin, dass Probleme, die an bestimmte Instanzen von Administratoren gebunden sind, bei denen Probleme auftreten können, nicht erkannt werden, da die Instanz des Management-Administrators für die Testnachrichten verwendet wird.

Nachfolgend sind die verschiedenen für diesen Ansatz relevanten Konfigurationen aufgeführt:

```
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 000000000000000
radius keepalive valid-response access-accept
```

Der Befehl "radius (accounting) detect-tot-server keepalive" aktiviert den Keepalive-Ansatz anstelle der aufeinander folgenden Ausfälle in einem aamgr-Ansatz. Im obigen Beispiel sendet das System alle 30 Sekunden eine Testmeldung mit dem Benutzernamen Test-Benutzername und dem Passwort Test-Username. Wenn keine Antwort eingeht, versucht es alle 3 Sekunden erneut, und es wiederholt sich bis zu dreimal, danach wird der Server heruntergefahren. Sobald er die erste Antwort erhält, wird er wieder freigegeben.

Hier ein Beispiel für eine Authentifizierungsanfrage/-antwort für die oben genannten Einstellungen:

```
<<<<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-vsa1
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 = 000000000000000
     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-vsa1
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
```

Dieselben SNMP-Traps werden verwendet, um den Zustand "nicht erreichbar/nicht erreichbar/erreichbar/aktiv" anzugeben, wie dies bei aufeinander folgenden Ausfällen in einem normalen Ansatz der Fall ist:

```
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
```

Die "show radius counter all" haben einen Bereich für die Nachverfolgung der Keepalive-Anforderungen für Authentifizierung und Abrechnung - hier sind die Authentifizierungszähler:

```
   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
```

# Problemlösungsbefehle/Ansätze

Nun, da der Auslöser für AAA Unreachable-Traps erklärt wurde, besteht der nächste Schritt darin, die verschiedenen Fehlerbehebungsbefehle zu verstehen, mit denen die Auswirkungen ermittelt und die Ursache ermittelt werden kann. Unerreichbarkeit ist ein sehr weit gefasster Begriff. Es erklärt nicht, wo die Unerreichbarkeit liegt - im Netzwerk, auf dem Server oder auf dem ASR. Ist es zum Beispiel bekannt, ob die Anfragen überhaupt erst gesendet wurden? Hat der Server die Anfragen erhalten? Hat er auf die Anfragen reagiert? Haben die Antworten den Fall an den ASR zurückgesendet, und wenn ja, wurden sie verarbeitet oder auf den internen Pfad zurückgesetzt (d. h. Datenflüsse). In diesem Abschnitt werden die Antworten auf diese Fragen erläutert.

## RADIUS-Konfigurationsgrundlagen

Zunächst müssen Sie sich mit einigen grundlegenden Aspekten der RADIUS-Konfiguration vertraut machen. Die Konfiguration für RADIUS erfolgt größtenteils in einer speziell benannten Gruppe, und alle Kontexte verfügen über eine Standardgruppe, die wie folgt konfiguriert werden kann. Häufig wird in Konfigurationen nur eine Gruppe, die Standardgruppe, verwendet.

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

Wenn bestimmte benannte AAA-Gruppen verwendet werden, wird auf sie die folgende Anweisung verwiesen, die in einem Subscriber-Profil oder Application Point Name (APN) konfiguriert ist (je nach Anrufsteuerungstechnologie), z. B.:

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

Hinweis: Das System überprüft zunächst die bestimmte Gruppe, die dem Teilnehmer zugewiesen ist, und überprüft dann die Gruppenstandardeinstellung auf zusätzliche, nicht in der bestimmten Gruppe definierte Konfigurationseinstellungen.

Nachfolgend finden Sie nützliche Befehle, die alle Werte zusammenfassen, die allen Konfigurationseinstellungen in den verschiedenen AAA-Gruppenkonfigurationen zugewiesen wurden. Dies ermöglicht die schnelle Anzeige aller konfigurierbaren Dateien, einschließlich der Standardwerte, ohne die Konfiguration manuell überprüfen zu müssen, und hilft möglicherweise, Fehler zu vermeiden, wenn bestimmte Einstellungen übernommen werden. Diese Befehle werden in allen Kontexten gemeldet:

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

Die wichtigste konfigurierbare ist natürlich der Radius-Access und Accounting-Server selbst. Hier ein Beispiel:

```
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
```

Beachten Sie die Funktion für maximale Übertragungsrate, die die Anzahl der an den Server gesendeten Anfragen pro Benutzer pro Sekunde beschränkt.

Darüber hinaus muss auch die NAS-IP-Adresse definiert werden, d. h. die IP-Adresse einer Schnittstelle im Kontext, aus dem RADIUS-Anfragen gesendet und Antworten empfangen werden. Wenn nicht definiert, werden Anfragen nicht gesendet, und die Überwachung der Subscriber-Traces darf keinen offensichtlichen Fehler (keine Radius-Anfragen gesendet und keine Angabe warum).

radius-attribute nas-ip-address address 10.211.41.129

Da Authentifizierung und Accounting häufig vom selben Server verwaltet werden, wird eine andere Portnummer verwendet, um den Authentifizierungs- und den Accounting-Datenverkehr auf dem RADIUS-Server zu unterscheiden. Auf der Seite des ASR5K wird die UDP-Quell-Port-Nummer NICHT angegeben und vom Chassis auf aamgr-Basis ausgewählt (weitere Informationen zu diesem späteren Zeitpunkt).
In der Regel werden aus Redundanzgründen mehrere Zugangs- und Abrechnungsserver angegeben. Sie können entweder einen Round-Robin oder eine priorisierte Bestellung konfigurieren:

radius [accounting]-Algorithmus {first-server | Round-Robin}

Bei der ersten Serveroption werden ALLE Anfragen mit der niedrigsten Priorität an den Server gesendet. Nur wenn Wiederholungsfehler auftreten oder, schlimmer noch, ein Server ausgefallen ist, wird der Server mit der nächsten Priorität versucht. Weitere Informationen hierzu finden Sie weiter unten.

Wenn ein Radius (Accounting oder Access) gesendet wird, wird eine Antwort erwartet. Wenn innerhalb des Timeout (Sekunden) keine Antwort eingeht, gilt Folgendes:

radius [Accounting] Timeout 3

Die Anforderung wird bis zu der angegebenen Anzahl gesendet:

radius [Accounting] max. retries 5

Dies bedeutet, dass eine Anfrage maximal einmal + einmal gesendet werden kann, bis sie auf dem gewünschten Radius-Server aufgegeben wird. An diesem Punkt versucht sie die gleiche Sequenz in der Reihenfolge an den nächsten Radius-Server. Wenn für jeden Server die Einstellung "max-retries + 1 mal ohne Antwort" versucht wurde, wird der Anruf abgelehnt, vorausgesetzt, es gibt bis zu diesem Zeitpunkt keinen anderen Grund für einen Ausfall.

Als Präsidentschaftskandidat gibt es Konfigurationen, die Benutzern den Zugriff ermöglichen, selbst wenn die Authentifizierung und die Abrechnung aufgrund von Zeitüberschreitungen zu allen Servern fehlschlagen, obwohl eine kommerzielle Bereitstellung dies wahrscheinlich nicht implementieren würde:

radius allow [accounting] authentication-down

Darüber hinaus gibt es Konfigurationen, die die absolute Gesamtzahl der Übertragungen einer bestimmten Anforderung auf alle konfigurierten Server begrenzen können. Diese sind standardmäßig deaktiviert:

radius [Accounting] max. Übertragungen 256

Wenn dieser beispielsweise auf "= 1" gesetzt ist, wird der Versuch, selbst wenn ein sekundärer Server vorhanden ist, nie unternommen, da nur ein Versuch für eine bestimmte Teilnehmereinrichtung versucht wird.

## Anzeige der Aufgabenressourcen für alle

Jeder aamgr-Prozess wird mit einem verknüpften Sessmgr-Prozess (der für die allgemeine Anrufbearbeitung verantwortlich ist) gepaart und "arbeitet für". Dieser Prozess befindet sich auf einer anderen Packet Services Card (PSC) oder Data Processing Card (DPC), jedoch mit derselben Instanz-ID. In diesem Beispiel wird auch die spezielle AMGR-Instanz 231 auf der Systemverwaltungskarte (SMC) für ASR 5000 (oder Management Input Output Card für ASR 5500 (MIO)) ausgegeben, die keine Teilnehmeranfragen verarbeitet, aber für RADIUS-Testbefehle verwendet wird (weitere Informationen hierzu finden Sie im späteren Abschnitt) UND für die CLI-Anmeldeverarbeitung des Betreibers.

In diesem Ausschnitt ist aamgr 107 im PSC 13 für die gesamte RADIUS-Verarbeitung für den paarweise verbundenen Sessmgr 107 auf PSC 1 verantwortlich. Die Erreichbarkeitsprobleme für AMAM 107 wirken sich auf Anrufe auf Sessmgr 107 aus.

```
                  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
```

Im folgenden Beispiel ist zu beachten, dass Probleme mit AMAGR 92 die paarweise gepaarte SESMGR im Vergleich zu anderen Sessions in Bezug auf Sitzungszählungen so leicht beeinträchtigen:

```
                   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 counter { {all} | server <server IP>} [instance <aamgr #> | Zusammenfassung}

Der wichtigste Befehl, mit dem Sie vertraut sind, sind die verschiedenen Typen von "show radius counters".

Dieser Befehl gibt viele nützliche Zähler zurück, um Radius-Probleme zu beheben. Der Befehl "show radius counters all" ist sehr hilfreich, um den Erfolg und die Fehler auf Serverbasis zu verfolgen. Es ist wichtig, die Bedeutung der verschiedenen Zähler zu verstehen, aus denen dieser Befehl besteht, da er nicht offensichtlich ist. Der Befehl ist kontextsensitiv und muss daher in demselben Kontext ausgeführt werden, in dem die AAA-Gruppe(n) definiert ist.

Wichtiger Hinweis: In einem nicht überwachten Zeitraum ist es schwierig, Schlussfolgerungen aus den Gegenwerten oder den Beziehungen zwischen Zählern zu ziehen. Um genaue Schlussfolgerungen zu ziehen, empfiehlt es sich, die Zähler zurückzusetzen und über einen bestimmten Zeitraum zu überwachen, wenn das Problem behoben wird.

In der folgenden Ausgabe beachten Sie "Access-Request Sent" = 1, während "Access-Request Retried" = 3. So wird jede neue Anforderung an einen bestimmten Radius-Server nur einmal gezählt, und alle Wiederholungen werden separat gezählt. In diesem Fall werden insgesamt 3 + 1 = 4 Zugriffsanfragen gesendet. Beachten Sie den Zähler "Access-Request Timeouts" = 1. Ein einmaliges Timeout tritt nur auf, wenn ALL die Wiederholungsversuche fehlschlagen. In diesem Fall werden 3 Wiederholungen ohne Antwort zu 1 Timeout (nicht 4) geführt. Dies geschieht auf allen konfigurierten Servern, bis ein Fehler auftritt oder alle Versuche fehlgeschlagen sind. Achten Sie also auf die Zähler, die für jeden Server separat nachverfolgt werden. Hier ein Beispiel dafür:

```
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
```

Beachten Sie auch, dass Zeitüberschreitungen NICHT als Fehler gezählt werden. Das Ergebnis ist, dass die Anzahl der empfangenen Access-Accept- und empfangenen Access-Reject-Nachrichten nicht zu Access-Request-Sent addiert wird, wenn es Zeitüberschreitungen gibt.

Die Analyse dieser Zähler ist möglicherweise nicht ganz einfach.  Beim Mobile IP (MIP)-Protokoll beispielsweise wird, da die Authentifizierungen fehlschlagen, keine MIP Registration Reply (RRP) gesendet, und das Mobiltelefon kann weiterhin neue MIP Registration Requests (RRQ) initiieren, da es keinen MIP RRP erhalten hat. Jeder neue MIP-RRQ veranlasst den PDSN, eine neue

Authentifizierungsanfrage zu senden, die selbst eine eigene Reihe von Wiederholungen haben kann. Dies wird im Feld "ID" am oberen Rand einer Paketverfolgung angezeigt. Es ist für jede Gruppe von Wiederholungen eindeutig. Das Ergebnis ist, dass die Zähler für Gesendet, Wiederholt und Timeout bei der Anzahl der empfangenen Anrufe viel höher sein können als erwartet. Es gibt eine Option, die aktiviert werden kann, um diese zusätzlichen Wiederholungsversuche zu minimieren, und die im Foreign Agent (FA)-Dienst (jedoch nicht im Home Agent (HA)) festgelegt werden kann: "authentication mn-aaa <6 optionen here> optimierte-retries"

Weitere nützliche Zähler:

"Access-Request Response Drop" (Zugriffsanfrage-Antwort abgebrochen): tritt auf, wenn der Anruf beim Warten auf Antworten auf Authentifizierungsanforderungen nicht eingerichtet werden kann.

"Access-Request Response Last Round Trip Time" (Letzte Reiseroute für Zugriffsanfrage) - Zeigt alle Verzögerungen zwischen den Endpunkten an, auch wenn dies offensichtlich nicht die Ursache der Verzögerung ist.

"Access-Request Current Consecutive Failures in a mgr" bezieht sich auf das, was im ersten Abschnitt über Trigger für nicht erreichbare AAA-Traps erörtert wurde. Er stellt die Aammer(s) mit der höchsten Anzahl aufeinander folgender Timeouts dar.

"Current Access/Accounting-Request Queued" gibt Anfragen an, auf die nicht reagiert wird und die nicht in der Warteschlange verbleiben (Accounting ermöglicht die permanente Erstellung der Warteschlange, die Authentifizierung dagegen nicht)

Das häufigste Szenario, in dem AAA Unreachable gemeldet wird, ist, dass auch Zugriffszeitüberschreitungen und/oder Antwortverluste auftreten, während die Zugriffsantworten nicht mit Anforderungen Schritt halten.

Wenn Zugriff auf den privilegierten Modus für den technischen Support besteht, können weitere Untersuchungen auf Instanzebene durchgeführt werden, um festzustellen, ob ein oder mehrere spezifische Parameter die Ursache für die Erhöhung der Gesamtzahl der "schlechten" Benutzer sind. Suchen Sie beispielsweise nach Agenten, die sich auf einem bestimmten PSC/DPC mit einer hohen Anzahl befinden, oder vielleicht nach einzelnen Agenten oder zufälligen Administratoren mit Problemen - suchen Sie nach Mustern. Wenn alle oder die meisten Administratoren Probleme haben, besteht eine erhöhte Wahrscheinlichkeit, dass die Ursache entweder außerhalb des Chassis liegt ODER sich im Chassis in großem Umfang manifestiert. In diesem Fall sollten allgemeine Gesundheitskontrollen durchgeführt werden.

Die folgende Beispielausgabe zeigt ein Problem mit einem bestimmten Namen für die Rechnungslegung. (Das Problem erwies sich als Fehler in einer Firewall zwischen dem ASR5K und dem RADIUS-Server, der den Datenverkehr von einem bestimmten Administrator-Instanzport (114) blockierte.) Innerhalb von drei Wochen wurden nur 48 Antworten empfangen, doch es sind über 100.000 Timeouts aufgetreten (und das beinhaltet keine Neuübertragungen).

```
[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
```

Stellen Sie abschließend fest, welche Zähler inkrementieren, für welche Server und mit welcher Geschwindigkeit.

## Untersystem Show Session {aaamgr | sessmgr {all} | instance <Instanz #>}

Obwohl es außerhalb des Anwendungsbereichs dieses Artikels ist, alle überflüssigen Ergebnisse aus diesem Befehl zu untersuchen, sind einige Beispiele zu betrachten. Wie bei jeder anderen Fehlerbehebung zeigt der Vergleich der Ausgabe zwischen den als gut und schlechten Instanzen des Angreifers häufig offensichtliche Unterschiede bei den angegebenen Werten. Dies kann sich in der Gesamtanzahl der Anfragen, der Fehler-/Erfolgsrate, der abgebrochenen Authentifizierung usw. widerspiegeln. Achten Sie darauf, das Session-Subsystem zu löschen (eine Instanz kann nicht gelöscht werden, alle müssen gelöscht werden), um jeglichen Verlauf zu löschen, der möglicherweise ein getrüchtes Bild des aktuellen Status liefern könnte.

Wenn Sie mit dem gleichen Problem fortfahren, das bereits zuvor bezüglich eines einzelnen fehlenden Agenten für die Buchhaltung erwähnt wurde, wird hier die Ausgabe eines anderen Knotens mit demselben Problem angezeigt, mit Ausnahme einer anderen Sessmr-Instanz 36. Notieren Sie sich alle interessanten Felder für den fehlerhaften AMAM und wie diese Werte im Laufe der Zeit mit den beiden Captures des Befehls steigen. In der Zwischenzeit wird die Ausgabe von Instanz 37 als Beispiel für einen funktionierenden Monitor angezeigt.

```
[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 gtpp charg                    0 Current gtpp charg
       0 Total gtpp charg success            0 Total gtpp charg failure
       0 Total gtpp charg cancelled          0 Total gtpp charg purged
       0 Total gtpp sec charg                0 Total gtpp 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 gtpp charg                    0 Current gtpp charg
       0 Total gtpp charg success            0 Total gtpp charg failure
       0 Total gtpp charg cancelled          0 Total gtpp charg purged
       0 Total gtpp sec charg                0 Total gtpp 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
...
```

Außerdem sollten Show Task-Ressourcen ausgeführt werden, um in allen Sitzungen auf ungleiche Sitzungszahlen (verwendete Spalte) zu überprüfen. Wenn irgendwelche gefunden werden, überprüfen Sie die paarweise aamgrs für diese Sessmrs mit diesem Befehl, ob es Felder

gibt, die nicht in der Zeile sind - wenn das Problem auf RADIUS zurückzuführen ist, dann gibt es eine gute Chance, etwas zu finden.

Im Beispiel für die Anzeige von Aufgabenressourcen in einem vorherigen Abschnitt gab es eine deutlich geringere Sitzungsanzahl für Sessmgr 92, die mit aamgr 92 gepaart wurde. Die Ausgabe des Teilsystems "Show Session" zeigt eine deutliche Steigerung der Gesamtzahl ausstehender und durch Autos gelöschter Zähler sowie der oberen Leistungsindikatoren mit max. ausstehenden Zählern. Sie können die grep-Funktion live im Chassis und/oder Editor++ oder einem anderen leistungsstarken Sucheditor verwenden, um Daten schnell zu analysieren. Führen Sie den Befehl mehrmals aus, um festzustellen, welche Werte erhöht oder erhöht bleiben:

```
[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

Ein ICMP Ping testet die grundlegende Konnektivität, um festzustellen, ob der AAA-Server erreicht werden kann. Der Ping-Befehl muss je nach Netzwerk mit dem src-Schlüsselwort bereitgestellt werden und muss aus dem AAA-Kontext heraus ausgeführt werden, um einen Mehrwert zu bieten. Wenn der Ping an den Server fehlschlägt, versuchen Sie, zwischengeschaltete Elemente zu pingen, einschließlich der nächsten Hop-Adresse im Kontext. Dies bestätigt, dass ein ARP-Eintrag zur Next-Hop-Adresse vorhanden ist, wenn der Ping-Befehl fehlschlägt. Traceroute kann auch bei Routing-Problemen helfen.

```
[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-Testinstanz x auth {radius group <group> | Alle | server <IP> port <port>} <Benutzername> <Kennwort>

## Radius-Testinstanz x Accounting {Radius-Gruppe <Gruppenname> | Alle | server <IP> port <port>}

Mit dem Zugriff auf die Testbefehle des technischen Supports kann noch einmal geprüft werden, ob ein bestimmter Administrator einen RADIUS-Server erreichen kann. Bei einem grundlegenden RADIUS-Verbindungstest, der unabhängig von einer bestimmten Instanz des Benutzers ausgeführt wird, verwenden Sie die generische Version dieses Befehls, der keine bestimmte Instanz # angibt, aber die Verwaltungsinstanz standardmäßig verwendet. Wenn dies fehlschlägt, kann es auf ein umfassenderes, von bestimmten Instanzen unabhängiges Problem hinweisen.
Dieser Befehl sendet eine grundlegende Authentifizierungsanfrage oder Accounting-**Start**- und **Stopp-**Anfragen und wartet auf eine Antwort. Verwenden Sie zur Authentifizierung einen beliebigen Benutzernamen und ein beliebiges Kennwort. In diesem Fall ist eine Ablehnungsantwort zu erwarten, um zu bestätigen, dass RADIUS wie vorgesehen funktioniert, oder es kann ein bekannter funktionierender Benutzername/Kennwort verwendet werden. In diesem Fall sollte eine Accept-Antwort empfangen werden.

Im Folgenden finden Sie ein Beispiel für die Ausgabe des Überwachungsprotokolls und die Ausführung der Authentifizierungsversion des Befehls in einem Übungs-Chassis:

```
[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-vsa1
```

```
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-vsa1
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
```

Ein Beispiel aus einem Live-Chassis:

```
<<<<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
```

Im Folgenden finden Sie ein Beispiel für die Ausführung der Accounting-Version des Befehls. Ein Kennwort ist nicht erforderlich.

```
[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-vsa1
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-vsa1 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-vsa1 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-vsa1 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
```

Die folgende Ausgabe gilt für dieselbe Instanz 36, die gerade erwähnt wurde, wenn die Verbindung zu einem bestimmten RADIUS-Accounting-Server unterbrochen ist:

```
[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 | Alle}

Dieser Befehl meldet die Flow-ID der Netzwerkprozessoreinheit (NPU) und den UDP-Port, die von der konfigurierten NAS-IP-Adresse für die Verbindung mit RADIUS-Servern verwendet werden. Dies wird im Standardabschnitt der AAA-Gruppe der Ausgabe gemeldet. Sicherlich kann die Portnummer nützlich sein, wenn RADIUS-Pakete in einer Paketerfassung mit einer bestimmten Instanz # übereinstimmen müssen. (Beachten Sie, dass NPU-Datenflüsse kompliziert sind und nicht in diesem Artikel behandelt werden, sondern eine Einheit, die ein Support-Techniker genauer untersuchen kann.) Es verfolgt auch ausstehende Anfragen an den Server. Im gleichen Beispielproblem, das in diesem Artikel verwendet wird, war nur ein bestimmter RADIUS-Server **<=>** NAS-IP/UDP-Portpaar fehlerhaft, wie hervorgehoben.

```
[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>
```

## Monitorteilnehmer

Mit einem Monitor-Subscriber kann ermittelt werden, ob zumindest versucht wird, eine Authentifizierung durchzuführen, und ob eine Antwort für die zu überwachenden Anrufe verarbeitet wird. Aktivieren Sie die Option 'S', die für Sessmgr Sender Info steht. Diese Funktion berichtet effektiv über die Instanz # der sessmgr oder aamgr, die das betreffende Messaging verarbeitet. Hier ein Beispiel für einen MIP-Anruf auf einem HA. Anfügen an Instanzen von sessmgr / aamgr 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
```

Am Ende dieses Artikels gibt es auch ein Fehlerbeispiel.

### Paketerfassung

Manchmal gibt es nicht genügend Informationen über den ASR, um festzustellen, warum Probleme mit der Erreichbarkeit auftreten. In diesem Fall ist eine Paketerfassung erforderlich. Bei der Fehlerbehebung einzelner Teilnehmerprobleme sollte die Identifizierung der entsprechenden Pakete in einer Spur einfach sein. Andernfalls kann es hilfreich sein, den UDP-Port zu kennen, der an einem der beiden Enden einer bestimmten Instanz # <=> RADIUS-Serverpaar verwendet wird, wenn das Problem mit bestimmten Ports/AMGR-Instanzen verknüpft ist.  Um festzustellen, wo Pakete verworfen werden, kann es erforderlich sein, eine Erfassung an mehreren Stellen im Netzwerk durchzuführen. Bei dem in diesem Artikel behandelten Problem handelte es sich um eine Paketerfassung genau an der richtigen Stelle im Transportpfad zwischen dem ASR und dem RADIUS-Server, die die Lösung des Problems ermöglichte.

## Problembehebung

Dieser letzte Abschnitt enthält einige Vorschläge zur Behebung von Problemen mit RADIUS-Verbindungen. Diese werden nicht in einer bestimmten Reihenfolge angezeigt, sondern nur in einer Liste, die bei der Fehlerbehebung berücksichtigt werden sollte.

Wenn der RADIUS-Server überlastet wird, kann die Last über den für "radius (accounting) max-ausstehenden Wert (default 256) konfigurierten Wert verringert werden, der eine Beschränkung für die Anzahl der ausstehenden (unbeantworteten) Anfragen für einen bestimmten aamgr-Prozess festlegt. Wenn der Grenzwert erreicht ist, können Protokolle Folgendes anzeigen: "Message ID konnte nicht für den RADIUS-Authentifizierungsserver x.x.x.x:1812 zugewiesen werden."

Durchsatzbegrenzende RADIUS-Nachrichten für bestimmte Server können ebenfalls dazu beitragen, die Last über das Schlüsselwort "rate-limit" für die entsprechenden Serverkonfigurationslinien zu reduzieren.

Manchmal ist es kein Problem der Konnektivität, sondern des erhöhten Buchhaltungs-Datenverkehrs, was kein Problem mit RADIUS ist, sondern verweist auf einen anderen Bereich, wie z. B. verstärkte Pppp-Neuverhandlungen, die mehr Buchführungsstarts und -stopps verursachen. Es kann also erforderlich sein, außerhalb von RADIUS eine Fehlerbehebung durchzuführen, um eine Ursache oder einen Auslöser für die beobachteten Symptome zu finden.

Wenn während des Fehlerbehebungsprozesses entschieden wurde, einen RADIUS-Authentifizierungs- oder Accounting-Server aus der Liste der Live-Server aus welchem Grund auch immer zu entfernen, gibt es einen (nicht konfigurierten) Befehl, der einen Server unbegrenzt außer Betrieb setzt, bis er wieder in Betrieb genommen werden soll. Dieser Ansatz ist übersichtlicher, als ihn manuell aus der Konfiguration entfernen zu müssen:

```
{Deaktivieren} | 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
```

Eine PSC- oder DPC-Migration oder ein Line Card-Switchover können häufig Probleme beheben, da die Migration zu einem Neustart der Vorgänge auf der Karte führt, einschließlich des NPumps, der von Zeit zu Zeit Probleme bei NPU-Strömen verursacht hat.

Aber in einer interessanten Wendung mit dem oben erwähnten Beispiel von AMAG 92 begannen die Fehler der AAA Unreachable, als eine PSC-Migration durchgeführt wurde. Dies wurde ausgelöst, weil ein NPU-Fluss fehlte, wenn eine PSC-Migration durchgeführt wurde, die PSC 11 zum Standby-Modus machte. Als sie eine Stunde später aktiv wurde, begann der eigentliche Einfluss des fehlenden Datenflusses für ca. 92. Probleme wie diese lassen sich nur mit Unterstützung des technischen Supports beheben.

```
[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
```

Das Problem wurde durch einen Port-Switchover vorübergehend behoben, wodurch die PSC-Karte, deren NPU-Fluss für AMAG 92 fehlte, nicht mehr an eine aktive Linecard angeschlossen war.

```
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
```

Die letzte Fehlerfalle:

```
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
```

Ebenso kann das Neustarten bestimmter Agenten, die "festgefahren" werden, auch Probleme lösen, obwohl dies eine Aktivität ist, die der technische Support tun sollte, da es eingeschränkte Befehle des technischen Supports beinhaltet. Im Beispiel "aamgr 92", das zuvor im Abschnitt "show task resources" vorgestellt wurde, wurde dies versucht, jedoch nicht, da die Ursache nicht "aamgr 92" war, sondern der fehlende NPU-Fluss, der von Aamgr 92 benötigt wurde (es handelte sich um ein NPU-Problem, nicht um ein aamgr-Problem). Hier ist die relevante Ausgabe des Versuchs. "show task table" wird ausgeführt, um die Zuordnung von Prozess-ID und Task-Instanz Nr. 92 anzuzeigen.

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

# Letztes Beispiel

Hier ein letztes Beispiel für einen echten Ausfall in einem Live-Netzwerk, das viele der in diesem Artikel besprochenen Befehle und Ansätze zur Fehlerbehebung zusammenfasst. Beachten Sie, dass dieser Knoten 3G MIP und 4G Long Term Evolution (LTE) sowie weiterentwickelte High Rate Packet Data (eHRPD)-Anruftypen verarbeitet.

### SNMP-Trap-Verlauf anzeigen

Allein durch Traps kann bestätigt werden, dass der Ausgangspunkt mit dem übereinstimmt, was der Kunde als 19:25 UTC angegeben hat. Beachten Sie, dass AAAuthSvrUnreachable-Traps für den Primärserver 209.165.201.3 erst Stunden später beginnen (nicht klar, warum, aber gut zu beachten; aber **Buchhaltung nicht erreichbar** für diesen Server startete sofort)

```
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
```

### Taskressourcen anzeigen

Die Ausgabe zeigt eine deutlich geringere Anzahl von Anrufen auf DPC 8/1 an. Auf der Grundlage dieser Überlegungen KÖNNTE ohne weitere Analyse auf DPC 8 ein Problem vermuten und die Option zur Migration auf das Standby-DPC vorschlagen. Es ist jedoch wichtig anzuerkennen, was die tatsächlichen Auswirkungen auf den Abonnenten sind. In diesen Szenarien werden die Teilnehmer in der Regel bei einem späteren Versuch erfolgreich eine Verbindung herstellen. Daher sind die Auswirkungen für den Abonnenten nicht zu signifikant, und sie melden dem Anbieter wahrscheinlich nichts, vorausgesetzt, dass auch auf der Benutzerebene kein Ausfall stattfindet (was je nach dem, was kaputt ist, möglich ist).

```
 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
```

## Monitorteilnehmer

Es wurde eine Anrufeinrichtung abgefangen, bei der die Authentifizierungsanfrage für den primären 209.165.201.3 für Sessmgr 242 auf DPC 9/1 nicht beantwortet wurde, bei dem der paarweise Adapter auf DPC 8/1 gespeichert ist. Dies bestätigte 3G-Fehler, die aufgrund von AAA am 8/1 nicht erreichbar sind. Es bestätigt auch, dass es bis zu diesem Zeitpunkt keine AAAuthSrvUnreachable-Traps für 209.165.201.3 gegeben hat, es aber nicht bedeutet, dass es kein Problem bei der Bearbeitung von Antworten für diesen Server gibt (wie oben gezeigt, fangen Traps an, aber Stunden später).

```
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 [Zusammenfassung] smgr-instance X

Interessant ist, dass die Anzahl der Sitzungen für Sessmgr 242 mit anderen Arbeitssitzungen vergleichbar ist. Weitere Untersuchungen ergaben, dass 4G-Anrufe, die auch auf diesem Chassis gehostet werden, eine Verbindung herstellen konnten. Sie konnten somit das Fehlen von 3G Mobile IP-Anrufen ausgleichen.  Es kann festgestellt werden, dass bis zu 8 Stunden, die nach Beginn des Ausfalls vergangen sind, keine MIP-Anrufe für diesen Sessmgr 242 vorhanden sind. Wenn Sie 9 Stunden vor Beginn des Ausfalls zurückgehen, werden Anrufe verbunden:

```
[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
```

LTE- und eHRPD-Anrufe weisen beim Vergleich von Sitzungen, die mit funktionierenden und defekten Räumen verbunden sind, ein höheres Verhältnis zu MIP-Anrufen auf:

```
[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-Testinstanz X Authentifizierungsserver

Alle Parameter in 8/1 sind leer - keine Befehle für Radius-Test-Instanzen funktionieren für diese Adapter, aber für Ammergs auf 8/0 und anderen Karten:

```
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
```

### Anzeigeradius aller Zähler

Der Hauptbefehl zur Fehlerbehebung bei RADIUS zeigt eine Menge Zeitüberschreitungen, die schnell zunehmen:

```
[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
```

Problembehebung

In den Wartungsfenstern wurde das Problem durch eine DPC-Migration von 8 auf 10 behoben, die AAAuthSrvUnreachable-Traps wurden angehalten, und DPC 8 wurde als RMAd und die Ursache für einen Hardwarefehler auf DPC 8 ermittelt (Einzelheiten dieses Fehlers sind für die Zwecke dieses Artikels nicht wichtig).

```
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
```