Fehlerbehebung bei fehlendem Visited-Network-Identifier AVP unter Benachrichtigungsanfrage

Inhalt

Einleitung

In diesem Dokument wird die Fehlerbehebung für den fehlenden VNI in der Meldung "Notify request" (Anforderung benachrichtigen) zwischen MME und HSS über die S6a-Schnittstelle beschrieben.

Voraussetzungen

3GPP Technische Daten - 29.272, 29.229

Request For Comments (RFC) - 6733

Anforderungen

Cisco empfiehlt, dass Sie mit dem StarOS Mobility Management Entity (MME)-Administrationsleitfaden vertraut sind.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Überblick

Notification Request and Answer (NOR/NOA) ist eine der einfachsten Meldungen über die S6a/S6d-Schnittstelle. Der Grundgedanke dieser Nachricht besteht darin, den Home Subscriber Server (HSS) über die Änderung der Informationen zu Netzwerk und Benutzergeräten zu informieren.

Das Benachrichtigungsverfahren wird zwischen MME und HSS verwendet, auch zwischen dem Serving GPRS Support Node (SGSN) und HSS, um den HSS über Folgendes zu benachrichtigen:

- Zuweisung/Änderung/Entfernung eines PDN-Gateways (Packet Data Network) für einen Access Point-Namen (APN)
- Wenn keine Aktualisierung des Standorts innerhalb von MME erfolgt, der HSS jedoch darüber informiert werden muss, dass ein Abbruchspeicherort an den aktuellen SGSN gesendet werden muss.
- Die Benutzereinheit (UE) verfügt über eine Speicherkapazität zum Empfangen einer oder mehrerer Kurznachrichten.
- Die EU ist wieder erreichbar

Nachrichtenformat von NOR-NOA

```
< Notify-Request> ::= < Diameter Header: 323, REQ, PXY, 16777251 >
                      < Session-Id >
                      [ Vendor-Specific-Application-Id ]
                      { Auth-Session-State }
                      { Origin-Host }
                      { Origin-Realm }
                       [ Destination-Host ]
                                              { Destination-Realm }

                      { User-Name }
                     * [ Supported-Features ]
                      [ Terminal-Information ]
                      [ MIP6-Agent-Info ]
                      [ Visited-Network-Identifier ]
                      [ Context-Identifier ]
                      [Service-Selection]
                      [ Alert-Reason ]
                      [ UE-SRVCC-Capability ]
                      [ NOR-Flags ]
                    [Homogeneous-Support-of-IMS-Voice-Over-PS-Sessions ]
                     *[ AVP ]


< Notify-Answer> ::= < Diameter Header: 323, PXY, 16777251 >
                      < Session-Id >
                      [ Vendor-Specific-Application-Id ]
                      [ Result-Code ]
                      [ Experimental-Result ]
                      { Auth-Session-State }
                      { Origin-Host }
                      { Origin-Realm }
                      [ OC-Supported-Features ]
```

```
 [ OC-OLR ]
*[ Supported-Features ]
*[ AVP ]
*[ Failed-AVP ]
```

Prozess

1. Einleitung: Der Prozess wird in der Regel vom MME initiiert, wenn ein relevantes Ereignis im Zusammenhang mit der EU auftritt.
2. NOR-Meldung: Die MME sendet eine NOR-Nachricht an den HSS. Diese Nachricht enthält die erforderlichen Identifikatoren, z. B. die IMSI (International Mobile Subscriber Identity), sowie Details zum Ereignis oder zur Änderung.
3. Verarbeitung durch HSS: Der HSS verarbeitet die Anforderung, aktualisiert seine Datensätze und kann je nach Bedarf weitere Aktionen auf Basis der erhaltenen Informationen durchführen.
4. Benachrichtigungsantwort: Der HSS sendet eine Benachrichtigungsantwort zurück an die MME, bestätigt die Aktualisierung und fügt alle zusätzlichen erforderlichen Daten oder Anweisungen hinzu.

Welche Rolle spielt der Visited Network Identifier AVP?

Das Visited-Network-Identifier (VNI)-Attributwertpaar (AVP) ist vom Typ "Octet-String". Dieser AVP enthält eine Kennung, die dem Heimnetzwerk hilft, das besuchte Netzwerk zu identifizieren (z. B. den Namen der besuchten Netzwerkdomäne).

Der VNI AVP dient dazu, das Netzwerk zu identifizieren, in dem sich der Benutzer derzeit befindet, oder "zu Besuch" ist, und wird hauptsächlich in Roaming-Szenarien verwendet. Diese Informationen sind von entscheidender Bedeutung für:

- Routing-Entscheidungen: Sicherstellen, dass Anfragen und Antworten korrekt zwischen dem Heimnetzwerk und dem besuchten Netzwerk weitergeleitet werden
- Richtliniendurchsetzung: Anwendung geeigneter Netzwerkrichtlinien und Abrechnungsregeln, basierend auf dem Standort des Benutzers und den Vereinbarungen des besuchten Netzwerks mit dem Heimnetzwerk.

7.3.105 Visited-Network-Identifier

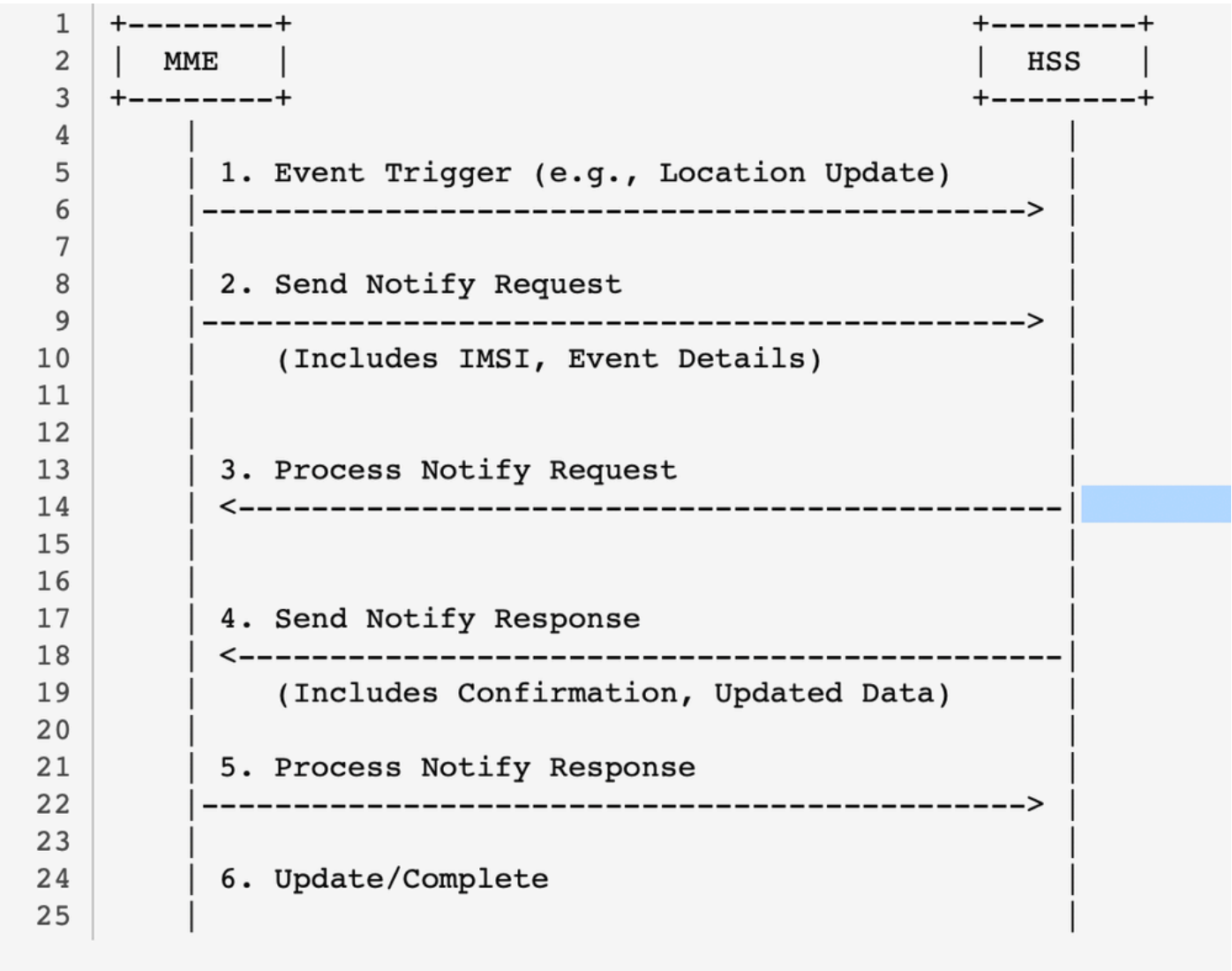
The Visited-Network-Identifier AVP contains the identity of the network where the PDN-GW was allocated, in the case of dynamic PDN-GW assignment.

The AVP shall be encoded as:

mnc<MNC>.mcc<MCC>.3gppnetwork.org

3gpp-Referenz für Visited-Network-Identifier AVP

Anrufablauf



NOR Call-Flow

Anruffluss bei Anforderung/Antwort benachrichtigen

1. Ereignisauslöser im MME

- Ein Teilnehmerereignis tritt in der MME auf, das eine Benachrichtigung des HSS erfordert. Beispiele:
  - Eine Standortaktualisierung
  - Änderung des besuchten Netzwerks (z. B. Roaming)
  - Aktualisierung des Abonnementstatus (z. B. aktiv oder inaktiv)
- Die MME bereitet eine NOR-Nachricht vor

2. MME sendet Benachrichtigungsanfrage

- Die MME erstellt die NOR-Nachricht mit den folgenden Schlüssel-AVPs:
  - Enthält den PLMN-ID-Domänennamen (Public Land Mobile Network) des besuchten Netzwerks, in dem sich der Teilnehmer derzeit befindet.
  - Sitzungs-ID: Eindeutiger Bezeichner für die Diameter-Sitzung
  - Origin-Host und Origin-Realm: Identifiziert MME als Absender
  - Ziel-Host und Ziel-Bereich: Identifiziert den HSS als Empfänger

- IMSI (Benutzer-ID): Die eindeutige Kennung des Teilnehmers.
- VNI
- Auth-Sitzungsstatus: Gibt an, ob die Sitzung zustandsbehaftet oder zustandslos ist

3. HSS empfängt und verarbeitet Benachrichtigungsanforderung

- Der HSS verarbeitet den NOR und validiert seine AVPs:
  - Überprüfen Sie IMSI, um den Datensatz des Teilnehmers zu finden.
  - Validiert den VNI, um sicherzustellen, dass er einem bekannten und unterstützten Netzwerk entspricht.
  - Aktualisiert die Daten des Abonnenten, um das neu besuchte Netzwerk oder den Status wiederzugeben.
- Wenn die Validierung erfolgreich ist, bereitet der HSS eine erfolgreiche Antwort vor.
- Bei Problemen (z. B. fehlendem VNI) bereitet der HSS eine Fehlerantwort vor.

4. HSS sendet NOA (Notify-Answer)

- Der HSS sendet eine NOA-Nachricht an die MME:
  - DURCHMESSER_ERFOLG (2001): Weist auf eine erfolgreiche Verarbeitung hin
  - DURCHMESSER_UNGÜLTIG_AVP_WERT (5004): Ist der VNI ungültig
  - DURCHMESSER_MISSING_AVP (5005): Wenn der VNI fehlt, aber erforderlich ist
  - Beinhaltet den VNI AVP, der den Ausfall verursacht hat
  - Ergebniscode
  - AVP fehlgeschlagen (falls zutreffend)

5. MME verarbeitet die Benachrichtigungs-Antwort

- Nach Erhalt der NOA:
  - Wenn der Ergebniscode erfolgreich ist, setzt das MME seine Vorgänge fort.
  - Wenn ein Fehler angezeigt wird, analysiert die MME den ausgefallenen AVP (falls vorhanden), um das Problem zu identifizieren.

Fehlerbehebung

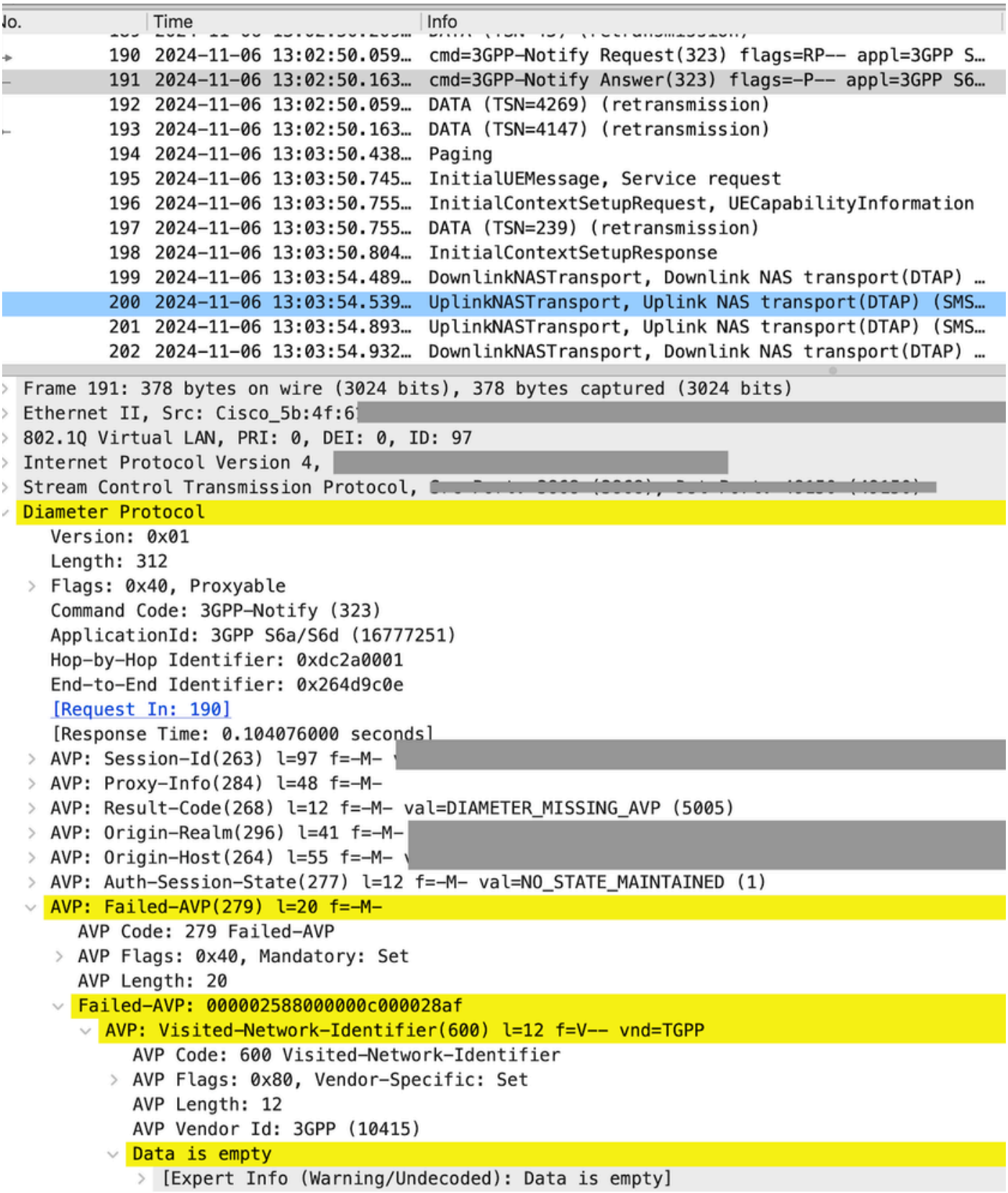
- Der primäre Aspekt besteht darin, zu überprüfen, ob die 'Benachrichtigungsanforderung' für alle 'HSS-Dienste' aktiviert ist. Sie können dasselbe erreichen, indem Sie diese CLI ausführen:

```
******** show hss-peer-service service all *******

Service name                    : hss<>
Notify Request Message          : Enable
Service name                    : hss<>
Notify Request Message          : Enable
```

- Wenn diese Option aktiviert ist, können Sie diese Protokolle anfordern, um das Problem weiter zu beheben:

```
1. Request “config verbose”

2. Monitor Subscriber with all the required options:
       monitor subscriber <imsi>, along with 19,33,34,35,A,S,X,Y,+++

3. Debug logs:

       logging filter active facility diameter level debug
       logging filter active facility sessmgr level debug
       logging filter active facility mme-app level debug
       logging active
        no logging active // to deactivate


4. Logging monitor:

       configure
        logging monitor msid <imsi>
       exit

5. Request  syslogs which captures the issue.
```

Problemszenario

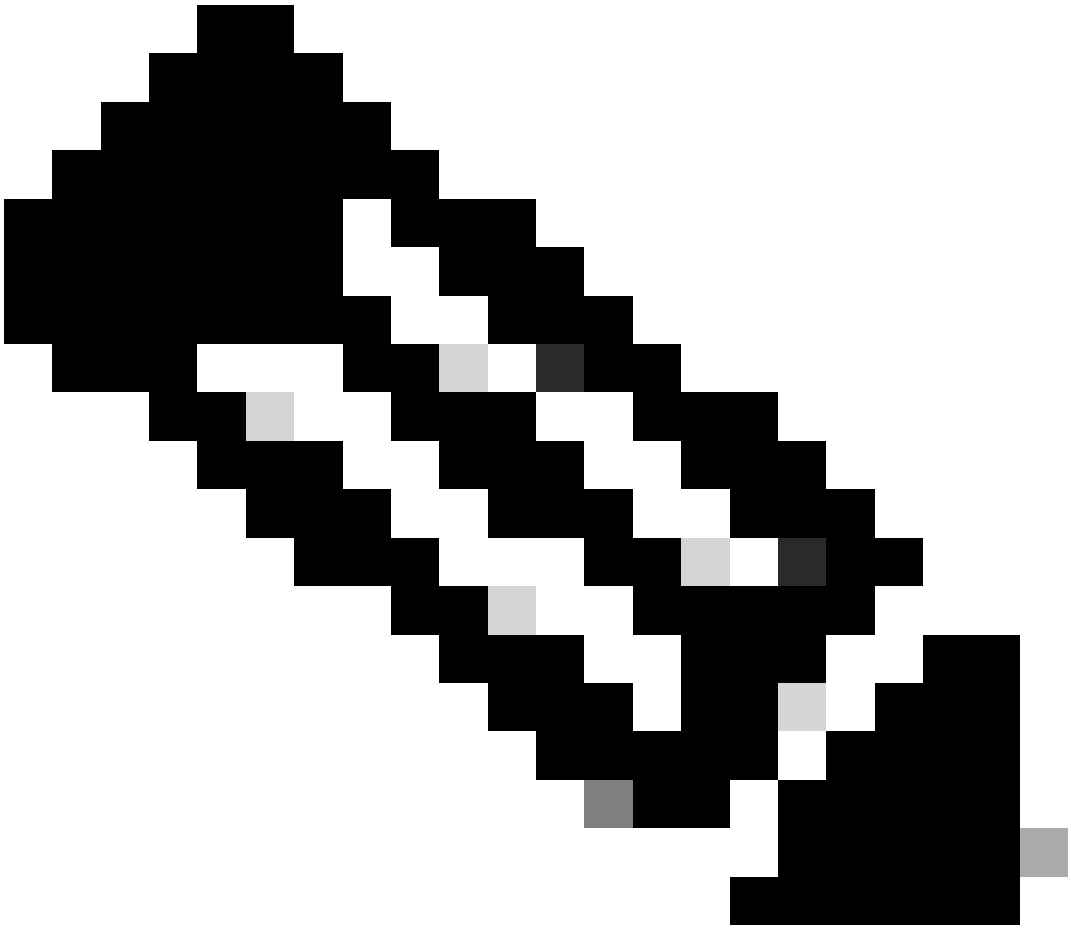


Problematische pcap

In dieser Referenz Packet Capture (PCAP) sehen Sie unter "notify-answer" den fehlenden "visited-network-identifier".

Das Paket 190 ist die 'Notify request', und 191 ist die 'Notify Answer'.

Der Ergebniscode für den Durchmesser in diesem Szenario ist 'Diameter_Missing_AVP', ein Beitrag, den Sie auch sehen können, die 'Failed AVP', die auf 'Visited-Network-Identifier' zeigt, die wiederum zeigt 'data empty'.



Anmerkung: Fehlgeschlagenes AVP ist ein gruppiertes AVP, das Debuginformationen bereitstellt, wenn eine Anforderung abgelehnt oder aufgrund eines Fehlers in einem bestimmten AVP nicht vollständig verarbeitet wird.

Einige Gründe für ein Failed-AVP:

- Eine AVP, die nicht richtig konstruiert ist
- Eine AVP, die nicht erkannt oder nicht unterstützt wird
- Ein ungültiger AVP-Wert
- Eine erforderliche AVP, die fehlt
- Ein AVP, der ausdrücklich ausgeschlossen ist

- Ein AVP, der auf 0, 1 oder 0-1 Ereignisse beschränkt ist, es gibt jedoch zwei oder mehr Ereignisse

---

Um das Problem weiter zu beheben, müssen Sie sicherstellen, dass Sie alle angeforderten Protokolle durchlaufen.

Wie bereits erwähnt, müssen Sie zunächst die hss-peer-service-Konfiguration des problematischen Knotens überprüfen.

Referenzkonfiguration:

```
hss-peer-service <>
      diameter hss-endpoint <>
      no diameter update-dictionary-avps
      --- more lines ---
    exit
```

In dieser Konfiguration können Sie sehen, dass es "no ameter update-dictionary-avps" gab. Das Problem war offensichtlich, als keinem der 3gpp-Releases ein Update-Dictionary zugeordnet war. Außerdem kann es einige Szenarien geben, in denen CLI 'durchmesser update-dictionary-avps 3gpp-r9/10' vorhanden ist und das Problem weiterhin offensichtlich ist.

Daher wurde es gemäß dem StarOS Admin-Leitfaden auf die neueste Version aktualisiert, um das Problem zu beheben, nämlich Release 11.

Die Referenzkonfiguration lautet wie folgt:

<#root>

Mode

```
Exec > Global Configuration > Context Configuration > HSS Peer Service Configuration
```

configure > context

context_name

> hss-peer-service

service_name

```
Entering the above command sequence results in the following prompt:
```

[*context_name*]*host_name*(config-hss-peer-service)#

Syntax

diameter update-dictionary-avps { 3gpp-r10 | 3gpp-r11 | 3gpp-r9 }

no diameter update-dictionary-avps

no

Sets the command to the default value where Release 8 ('standard') dictionary is used for backward compa

3gpp-r10

Configures the MME /SGSN to signal additional AVPs to HSS in support of Release 10 of 3GPP 29.272.

3gpp-r11

Configures the MME /SGSN to signal additional AVPs to HSS in support of Release 11 of 3GPP 29.272.

Using this keyword is necessary to enable the MME to fully support inclusion of the Additional Mobile S

a-msisdn

command in the Call-Control Profile configuration mode.

3gpp-r9

Configures the MME/SGSN to signal Release 9 AVPs to HSS.

Usage Guidelines

Use this command to configure the 3GPP release that should be supported for this HSS peer service.

This command is only applicable for the 'standard' diameter dictionary as defined in the

diameter hss-dictionary

command.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.