Troubleshoot Missing Visited-Network-Identifier AVP under Notify Request

Contents

Introduction

This document describes how to troubleshoot the missing VNI under the 'Notify request' message between MME and HSS over the S6a interface.

Prerequisites

3GPP Technical Specifications - 29.272, 29.229

Request for Comments (RFC) - 6733

Requirements

Cisco recommends that you have knowledge of the StarOS-Mobility Management Entity (MME) admin guide.

Components Used

This document is not restricted to specific software and hardware versions.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Overview

Notification Request and Answer (NOR/NOA) is one of the simplest of messages over the S6a/S6d interface. The basic idea of this message is to inform the Home Subscriber Server (HSS) about the change in

Network and User Equipment information.

The Notification Procedure is used between the MME and HSS, also between the Serving GPRS Support Node (SGSN) and HSS in order to notify the HSS about:

- An assignment/change/removal of Packet Data Network (PDN) Gateway (GW) for an Access Point Name (APN)
- When an inter-MME location update does not occur but the HSS needs to be notified about the need to send a Cancel Location to the current SGSN.
- The User Entity (UE) has memory capacity available to receive one or more short message
- The UE has become reachable again

Message Format of 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 ]
```

Process

1. Initiation: The process is typically initiated by the MME when a relevant event related to the UE occurs.

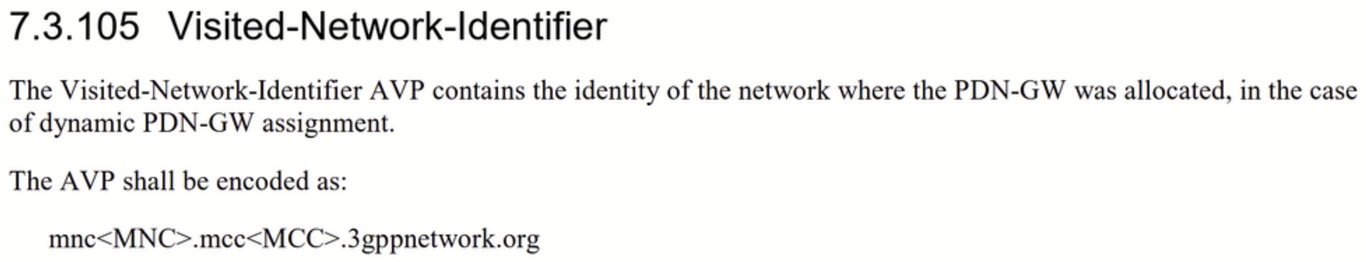
2. NOR Message: The MME sends a NOR message to the HSS. This message includes necessary identifiers like the International Mobile Subscriber Identity (IMSI) and details of the event or change.
3. Processing by HSS: The HSS processes the request, updates its records, and can perform further actions as needed based on the information received.
4. Notify Response: The HSS sends a Notify Response back to the MME, confirming the update and including any additional necessary data or instructions.

What is the Role of Visited Network Identifier AVP?

The Visited-Network-Identifier (VNI) Attribute Value Pair (AVP) is of type Octet-String. This AVP contains an identifier that helps the home network identify the visited network (for example, the visited network domain name).

The VNI AVP serves to identify the network where the user is currently located, or 'visiting', and is primarily used in roaming scenarios. This information is crucial for:

- Routing Decisions: Ensuring that requests and responses are correctly routed between the home network and the visited network.
- Policy Enforcement: Applying appropriate network policies and charging rules based on the location of the user and the agreements of the visited network with the home network.



7.3.105 Visited-Network-Identifier

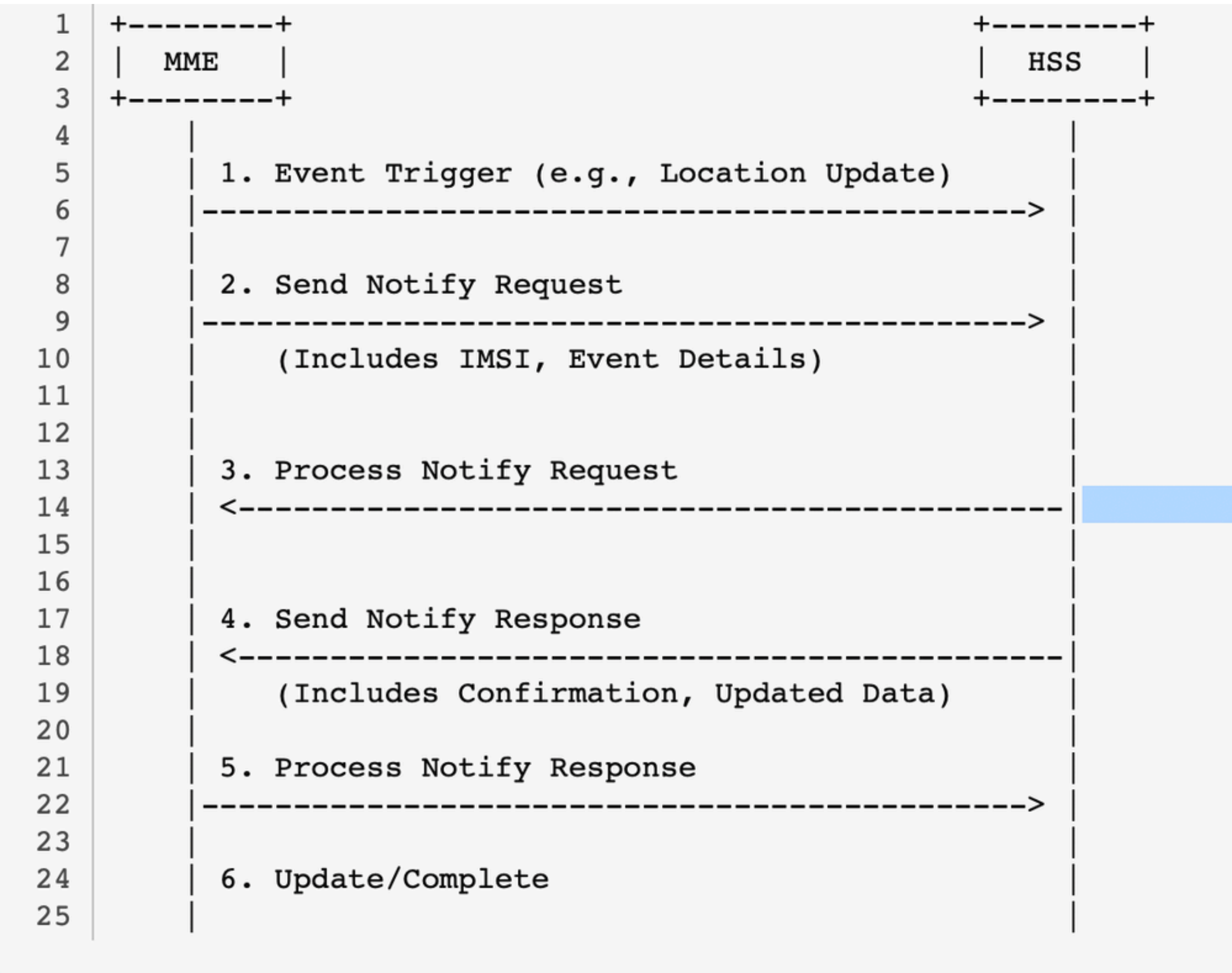
The Visited-Network-Identifier AVP contains the identity of the network where the PDN-GW was allocated, in the case of dynamic PDN-GW assignment.

The AVP shall be encoded as:

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

3gpp reference for Visited-Network-Identifier AVP

Call Flow



```
+--------+                                     +--------+
|  MME   |                                     |  HSS   |
+--------+                                     +--------+
    |                                               |
    | 1. Event Trigger (e.g., Location Update)      |
    |---------------------------------------------> |
    |                                               |
    | 2. Send Notify Request                        |
    |---------------------------------------------> |
    |    (Includes IMSI, Event Details)             |
    |                                               |
    |                                               |
    | 3. Process Notify Request                     |
    | <---------------------------------------------|
    |                                               |
    |                                               |
    | 4. Send Notify Response                       |
    | <---------------------------------------------|
    |    (Includes Confirmation, Updated Data)      |
    |                                               |
    | 5. Process Notify Response                    |
    |---------------------------------------------> |
    |                                               |
    | 6. Update/Complete                            |
    |                                               |
```

NOR call-flow

Notify-Request/Answer Call Flow

1. Event Trigger in the MME

- A subscriber event occurs in the MME that necessitates notifying the HSS. Examples include:
    - A location update
    - A change in the visited network (for example, roaming)
    - A subscription status update (for example, active or inactive)
- The MME prepares a NOR message

2. MME Sends Notify-Request

- The MME constructs the NOR message with these key AVPs:
    - Contains the Public Land Mobile Network (PLMN) ID domain name of the visited network where the subscriber is currently located.
    - Session-ID: Unique identifier for the Diameter session
    - Origin-Host and Origin-Realm: Identifies the MME as the sender
    - Destination-Host and Destination-Realm: Identifies the HSS as the recipient
    - IMSI (User-Identifier): The unique identifier of the subscriber
    - VNI
    - Auth-Session-State: Indicates whether the session is stateful or stateless

3. HSS Receives and Processes Notify-Request

- The HSS processes the NOR and validates its AVPs:
    - Check the IMSI to locate the subscriber’s record.
    - Validates the VNI in order to ensure it corresponds to a known and supported network.
    - Updates the subscriber's data to reflect the new visited network or status.
- If validation succeeds, the HSS prepares a successful response.
- If there are issues (e.g., missing VNI), the HSS prepares an error response.

4. HSS Sends Notify-Answer (NOA)

- The HSS sends a NOA message to the MME:
    - DIAMETER_SUCCESS (2001): Indicates successful processing
    - DIAMETER_INVALID_AVP_VALUE (5004): If the VNI is invalid
    - DIAMETER_MISSING_AVP (5005): If the VNI is missing but required
    - Contains the VNI AVP if it caused the failure
    - Result-Code
    - Failed AVP (if applicable)

5. MME Handles the Notify-Answer

- Upon receiving the NOA:
    - If Result-Code is successful, the MME continues its operations
    - If an error is indicated, the MME analyzes the Failed AVP (if present) in order to identify the issue

Troubleshoot

- The primary aspect is to check if the 'notify request' is 'enabled' across all the 'HSS services'. You can accomplish the same by executing this CLI:

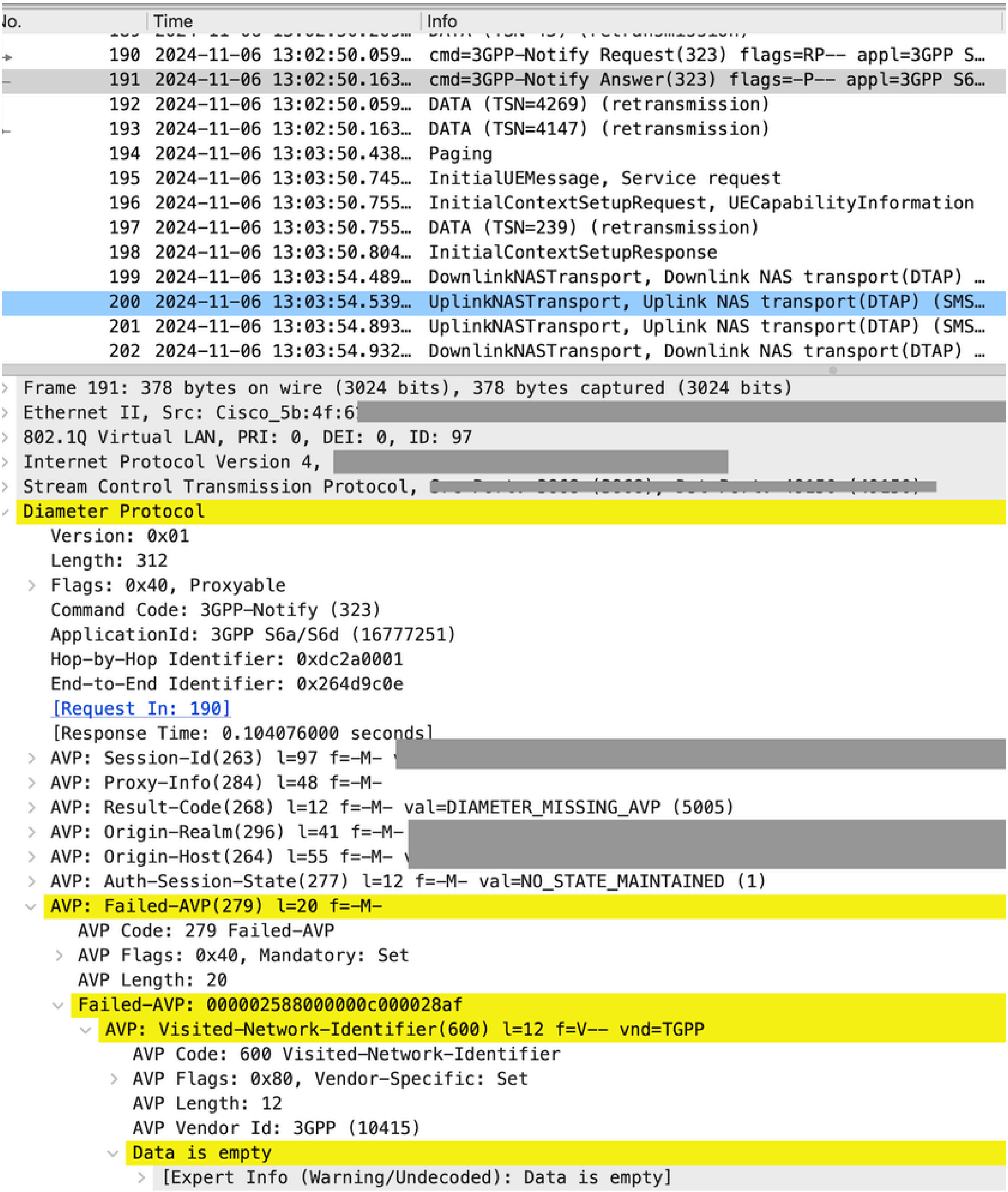
```
******** show hss-peer-service service all *******

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

- Once, this is checked, you can ask for these logs in order to troubleshoot the issue further:

```
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.
```

Problematic Scenario



```
No.     Time                        Info
190 2024-11-06 13:02:50.059…  cmd=3GPP-Notify Request(323) flags=RP-- appl=3GPP S…
191 2024-11-06 13:02:50.163…  cmd=3GPP-Notify Answer(323) flags=-P-- appl=3GPP S6…
192 2024-11-06 13:02:50.059…  DATA (TSN=4269) (retransmission)
193 2024-11-06 13:02:50.163…  DATA (TSN=4147) (retransmission)
194 2024-11-06 13:03:50.438…  Paging
195 2024-11-06 13:03:50.745…  InitialUEMessage, Service request
196 2024-11-06 13:03:50.755…  InitialContextSetupRequest, UECapabilityInformation
197 2024-11-06 13:03:50.755…  DATA (TSN=239) (retransmission)
198 2024-11-06 13:03:50.804…  InitialContextSetupResponse
199 2024-11-06 13:03:54.489…  DownlinkNASTransport, Downlink NAS transport(DTAP) …
200 2024-11-06 13:03:54.539…  UplinkNASTransport, Uplink NAS transport(DTAP) (SMS…
201 2024-11-06 13:03:54.893…  UplinkNASTransport, Uplink NAS transport(DTAP) (SMS…
202 2024-11-06 13:03:54.932…  DownlinkNASTransport, Downlink NAS transport(DTAP) …

> Frame 191: 378 bytes on wire (3024 bits), 378 bytes captured (3024 bits)
> Ethernet II, Src: Cisco_5b:4f:6[redacted]
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 97
> Internet Protocol Version 4, [redacted]
> Stream Control Transmission Protocol, [redacted]
v Diameter Protocol
    Version: 0x01
    Length: 312
  > Flags: 0x40, Proxyable
    Command Code: 3GPP-Notify (323)
    ApplicationId: 3GPP S6a/S6d (16777251)
    Hop-by-Hop Identifier: 0xdc2a0001
    End-to-End Identifier: 0x264d9c0e
    [Request In: 190]
    [Response Time: 0.104076000 seconds]
  > AVP: Session-Id(263) l=97 f=-M- [redacted]
  > AVP: Proxy-Info(284) l=48 f=-M-
  > AVP: Result-Code(268) l=12 f=-M- val=DIAMETER_MISSING_AVP (5005)
  > AVP: Origin-Realm(296) l=41 f=-M- [redacted]
  > AVP: Origin-Host(264) l=55 f=-M-
  > AVP: Auth-Session-State(277) l=12 f=-M- val=NO_STATE_MAINTAINED (1)
  v AVP: Failed-AVP(279) l=20 f=-M-
      AVP Code: 279 Failed-AVP
    > AVP Flags: 0x40, Mandatory: Set
      AVP Length: 20
    v Failed-AVP: 000002588000000c000028af
      v AVP: Visited-Network-Identifier(600) l=12 f=V-- vnd=TGPP
          AVP Code: 600 Visited-Network-Identifier
        > AVP Flags: 0x80, Vendor-Specific: Set
          AVP Length: 12
          AVP Vendor Id: 3GPP (10415)
        v Data is empty
          > [Expert Info (Warning/Undecoded): Data is empty]
```

Problematic pcap

In this reference Packet Capture (PCAP), you can see the missing 'visited-network-Identifier' under 'notify-answer'.

The packet 190 is the 'Notify request', and 191 is the 'Notify Answer'.

The diameter result code in this scenario is 'Diameter_Missing_AVP', post which you can also see the

'Failed AVP' which points to 'Visited-Network-Identifier' which in turn displays 'data empty'.

Note: Failed AVP is a Grouped AVP that provides debugging information when a request is rejected or not fully processed due to an error in a specific AVP.

Some reasons for a Failed-AVP include:

• An AVP that is not constructed properly

• An AVP that is unrecognized or unsupported

• An AVP value that is invalid

• A required AVP that is missing

• An AVP that is explicitly excluded

• An AVP that is restricted to 0, 1, or 0-1 occurrences, but there are two or more occurrences

In order to further troubleshoot the issue, you must ensure that you proceed through all the requested logs.

As insisted earlier, first you have to check the **hss-peer-service** configuration of the problematic node.

Reference configuration:

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

In this configuration, you can see there was 'no diameter update-dictionary-avps'. The issue was evident when there was no update-dictionary mapped to any of the 3gpp-release. Also, you can encounter a few scenarios where the CLI 'diameter update-dictionary-avps 3gpp-r9/10' is present and still the issue is evident.

Hence, it was updated to the latest release as per the StarOS admin guide in order to rectify the issue, which is release 11.

Here is the reference configuration:

<#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 comp

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.