

Probleemoplossing voor ontbrekende bezochte netwerkidentificatie met AVP onder verzoek melden

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Overzicht](#)

[Berichtformaat van NOR-NOA](#)

[Proces](#)

[Wat is de rol van Visited Network Identifier AVP?](#)

[Call Flow](#)

[Melden-aanvragen/antwoorden gespreksstroom](#)

[Problemen oplossen](#)

[Problematisch scenario](#)

Inleiding

In dit document wordt beschreven hoe de ontbrekende VNI kan worden opgelost onder het bericht 'Melden aanvraag' tussen MME en HSS via de S6a interface.

Voorwaarden

3GPP technische specificaties - 29.272, 29.229

Verzoek om opmerkingen (RFC) - 6733

Vereisten

Cisco raadt u aan te beschikken over kennis van de StarOS-Mobility Management Entity (MME) beheerdershandleiding.

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële

impact van elke opdracht begrijpt.

Overzicht

Notification request and reply (NOR/NOA) is een van de eenvoudigste berichten via de S6a/S6d interface. Het basisidee van dit bericht is om de Home Subscriber Server (HSS) te informeren over de wijziging in de informatie over netwerk- en gebruikersapparatuur.

De kennisgevingsprocedure wordt gebruikt tussen het MME en HSS, ook tussen het Serving GPRS Support Node (SGSN) en HSS om het HSS op de hoogte te stellen van:

- Een toewijzing/wijziging/verwijdering van Packet Data Network (PDN) Gateway (GW) voor een Access Point Name (APN)
- Wanneer een intermme-locatieupdate niet plaatsvindt, moet de HSS op de hoogte worden gebracht van de noodzaak om een Cancel-locatie naar het huidige SGSN te sturen.
- De gebruikersentiteit (UE) heeft geheugencapaciteit beschikbaar om een of meer korte berichten te ontvangen
- De EU is weer bereikbaar geworden

Berichtformaat van 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]

Proces

1. Inleiding: Het proces wordt doorgaans geïnitieerd door het MME wanneer een relevante gebeurtenis met betrekking tot de EU plaatsvindt.
2. NO-bericht: De MME stuurt een NOR-bericht naar de HSS. Dit bericht bevat de nodige identificatoren zoals de International Mobile Subscriber Identity (IMSI) en details van de gebeurtenis of wijziging.
3. Verwerking door HSS: De HSS verwerkt het verzoek, actualiseert zijn gegevens en kan indien nodig verdere acties uitvoeren op basis van de ontvangen informatie.
4. Antwoord melden: De HSS stuurt een Notify Response terug naar de MME, met bevestiging van de update en met inbegrip van eventuele extra benodigde gegevens of instructies.

Wat is de rol van Visited Network Identifier AVP?

Het AVP-paar (Visited-Network-Identifier) Attribute Value Pair (VNI) is van het type Octet-String. Deze AVP bevat een identificatie die het thuisnetwerk helpt bij het identificeren van het bezochte netwerk (bijvoorbeeld de bezochte netwerkdomeinnaam).

De VNI AVP dient om het netwerk te identificeren waar de gebruiker zich momenteel bevindt, of 'bezoek', en wordt voornamelijk gebruikt in roaming-scenario's. Deze informatie is van cruciaal belang voor:

- Routing-beslissingen: Ervoor zorgen dat verzoeken en antwoorden correct tussen het thuisnetwerk en het bezochte netwerk worden verzonden.
- Beleidshandhaving: Toepassen van het juiste netwerkbeleid en heffingsregels op basis van de locatie van de gebruiker en de overeenkomsten van het bezochte netwerk met het thuisnetwerk.

7.3.105 Visited-Network-Identifier

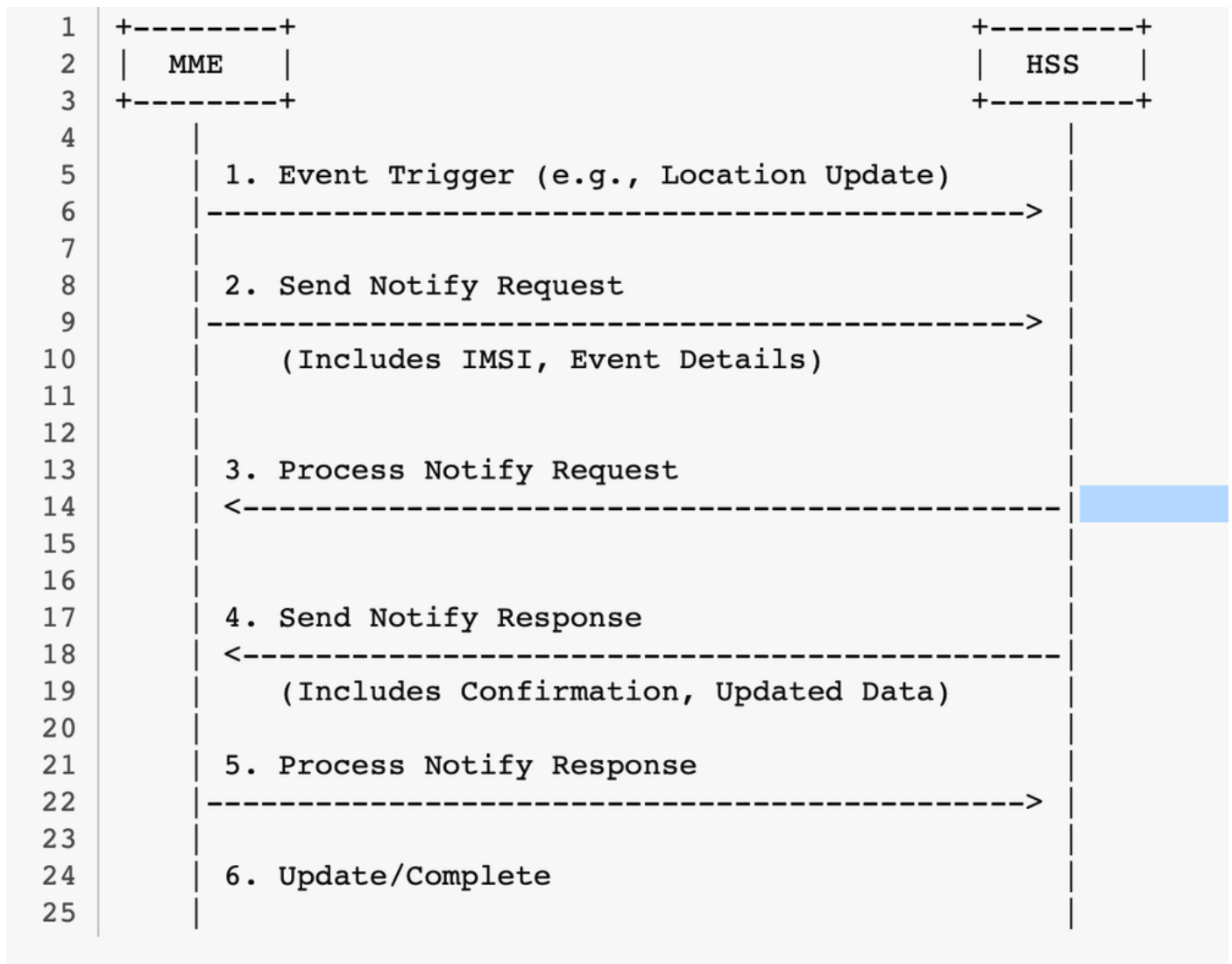
The Visited-Network-Identifier AVP contains the identity of the network where the PDN-GW was allocated, in the case of dynamic PDN-GW assignment.

The AVP shall be encoded as:

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

3gpp-verwijzing voor Visited-Network-Identifier AVP

Call Flow



NOR call-flow

Melden-aanvragen/antwoorden gespreksstroom

1. Event Trigger in de MME

- Een abonneegebeurtenis doet zich voor in de MME die de melding aan de HSS vereist. Voorbeelden zijn:
 - Een locatie-update
 - Een wijziging in het bezochte netwerk (bijvoorbeeld roaming)
 - Een update van de abonnementsstatus (bijvoorbeeld, actief of inactief)
- De MME bereidt een NOR bericht voor

2. MME verzendt melding-aanvraag

- De MME construeert de NOR-boodschap met deze belangrijke AVP's:
 - Bevat de Public Land Mobile Network (PLMN) ID-domeinnaam van het bezochte netwerk waar de abonnee momenteel is gevestigd.
 - Session-ID: Unieke identificatiecode voor de Diameter-sessie
 - Origin-Host en Origin-Real: Identificeert de MME als afzender
 - Bestemming-host en Bestemming-gebied: Identificeert het HSS als de ontvanger

- IMSI (User-Identifier): De unieke identificatiecode van de abonnee
- VNI
- Autorisatiesessie-status: Geeft aan of de sessie stateful of stateless is

3. HSS ontvangt en verwerkt kennisgevingsaanvraag

- HSS verwerkt de NOR en valideert haar AVP's:
 - Controleer IMSI om de record van de abonnee te vinden.
 - Valideert het VNI om ervoor te zorgen dat het overeenkomt met een bekend en ondersteund netwerk.
 - Werkt de gegevens van de abonnee bij om het nieuwe bezochte netwerk of de status weer te geven.
- Als de validatie slaagt, bereidt de HSS een succesvolle respons voor.
- Als er problemen zijn (bijvoorbeeld ontbrekende VNI), bereidt de HSS een foutmelding voor.

4. HSS Verzendt Melden-Antwoord (NOA)

- De HSS stuurt een NOA-bericht naar de MME:
 - DIAMETER_SUCCEES (2001): Geeft aan dat de verwerking is geslaagd
 - DIAMETER_INVALID_AVP_WAARDE (5004) Als het VNI ongeldig is
 - DIAMETER_MISSING_AVP (5005): Indien het VNI ontbreekt, maar vereist is
 - Bevat de VNI AVP als deze de fout heeft veroorzaakt
- Resultaatcode
- Mislukte AVP (indien van toepassing)

5. MME verwerkt het kennisgevingsantwoord

- Na ontvangst van het NOA:
 - Als de Resultaat-Code succesvol is, gaat de MME verder met haar werkzaamheden
 - Als een fout wordt aangegeven, analyseert het MME de mislukte AVP (indien aanwezig) om het probleem te identificeren

Problemen oplossen

- Het belangrijkste aspect is te controleren of het 'kennisgevingsverzoek' is 'ingeschakeld' bij alle 'HSS-diensten'. U kunt hetzelfde doen door deze CLI uit te voeren:

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

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

- Zodra dit is ingeschakeld, kunt u deze logbestanden aanvragen om het probleem verder op

te lossen:

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.

Problematisch scenario

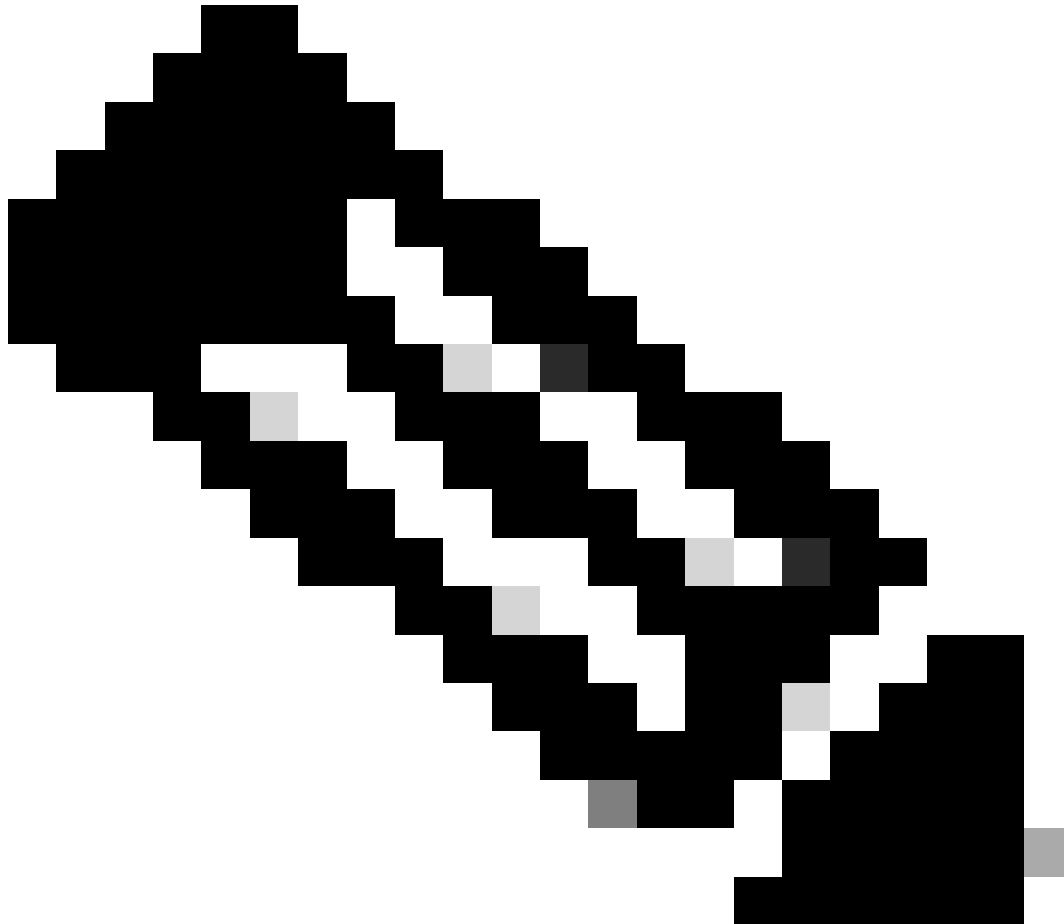
No.	Time	Info
190	2024-11-06 13:02:50.059...	cmd=3GPP-Notify Request(323) flags=RP-- appl=3GPP S...
191	2024-11-06 13:02:50.163...	cmd=3GPP-Notify Answer(323) flags=-P-- appl=3GPP S6...
192	2024-11-06 13:02:50.059...	DATA (TSN=4269) (retransmission)
193	2024-11-06 13:02:50.163...	DATA (TSN=4147) (retransmission)
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... > 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 97 > Internet Protocol Version 4, ... > Stream Control Transmission Protocol, ... > 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- ... > 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- ... > AVP: Origin-Host(264) l=55 f=-M- ... > AVP: Auth-Session-State(277) l=12 f=-M- val=NO_STATE_MAINTAINED (1) > AVP: Failed-AVP(279) l=20 f=-M- AVP Code: 279 Failed-AVP > AVP Flags: 0x40, Mandatory: Set AVP Length: 20 > Failed-AVP: 000002588000000c000028af > 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) > Data is empty > [Expert Info (Warning/Undecoded): Data is empty]		

Problematische dop

In deze referentie Packet Capture (PCAP) kunt u het ontbrekende 'visit-network-Idenfier' zien onder 'notification-reply'.

Het pakket 190 is het 'Notify request', en 191 is het 'Notify reply'.

De diameterresultaatcode in dit scenario is "Diameter_Missing_AVP", post waar je ook de "Mislukte AVP" kunt zien die verwijst naar "Visited-Network-Identfier" die op zijn beurt weer "data leeg" weergeeft.



Opmerking: Mislukte AVP is een gegroepeerde AVP die debugging informatie geeft wanneer een verzoek wordt afgewezen of niet volledig verwerkt vanwege een fout in een specifieke AVP.

Enkele redenen voor een Failure-AVP zijn:

- Een AVP die niet goed is gebouwd
 - Een AVP die niet wordt herkend of niet wordt ondersteund
 - Een AVP-waarde die ongeldig is
 - Een vereiste AVP die ontbreekt
 - Een AVP die expliciet is uitgesloten
-

-
- Een AVP die beperkt is tot 0, 1 of 0-1 voorvallen, maar er zijn twee of meer voorvallen
-

Om het probleem verder op te lossen, moet u ervoor zorgen dat u doorgaat met alle gevraagde logbestanden.

Zoals eerder benadrukt, moet u eerst de hss-peer-service configuratie van de problematische knooppunt controleren.

Referentie configuratie:

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

In deze configuratie, kunt u zien er was "geen diameter update-woordenboek-avps". De kwestie was duidelijk toen er geen update-woordenboek aan om het even welke 3gpp-versie in kaart werd gebracht. Ook, kunt u een paar scenario's ontmoeten waar de CLI 'diameter update-woordenboek-avps 3gpp-r9/10' aanwezig is en de kwestie nog steeds duidelijk is.

Daarom werd het bijgewerkt naar de nieuwste release volgens de StarOS-beheershandleiding om het probleem, dat is release 11, te verhelpen.

Hier is de referentieconfiguratie:

<#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.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.