

Solucionar problemas de AVP de identificador de red visitado faltante en la solicitud de notificación

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Overview](#)

[Formato de mensaje de NOR-NOA](#)

[Proceso](#)

[¿Cuál es la función del AVP de identificador de red visitado?](#)

[Flujo de llamada](#)

[Flujo de llamada de solicitud/respuesta de notificación](#)

[Troubleshoot](#)

[Situación problemática](#)

Introducción

Este documento describe cómo resolver problemas del VNI faltante en el mensaje 'Notificar solicitud' entre MME y HSS sobre la interfaz S6a.

Prerequisites

Especificaciones técnicas de 3GPP - 29.272, 29.229

Solicitud de comentarios (RFC): 6733

Requirements

Cisco recomienda que conozca la guía de administración de StarOS-Mobility Management Entity (MME).

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Overview

La solicitud y respuesta de notificación (NOR/NOA) es uno de los mensajes más sencillos a través de la interfaz S6a/S6d. La idea básica de este mensaje es informar al Home Subscriber Server (HSS) sobre el cambio en la información de la Red y del Equipo de Usuario.

El procedimiento de notificación se utiliza entre el MME y el HSS, también entre el Nodo de soporte de GPRS en funcionamiento (SGSN) y el HSS para notificar al HSS sobre:

- Asignación, cambio o eliminación de la puerta de enlace (GW) de red de datos de paquetes (PDN) para un nombre de punto de acceso (APN)
- Cuando no se produce una actualización de ubicación entre MME pero el HSS necesita ser notificado sobre la necesidad de enviar una ubicación de cancelación al SGSN actual.
- La entidad de usuario (UE) tiene capacidad de memoria disponible para recibir uno o más mensajes cortos
- La UE se ha vuelto accesible

Formato de mensaje de 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 ]
```

Proceso

1. Inicio: El MME suele iniciar el proceso cuando se produce un evento relevante relacionado con la UE.
2. Mensaje NOR: El MME envía un mensaje NOR al HSS. Este mensaje incluye los identificadores necesarios, como la identidad internacional de abonado móvil (IMSI) y los detalles del evento o cambio.
3. Procesamiento por HSS: El HSS procesa la solicitud, actualiza sus registros y puede realizar otras acciones según sea necesario en función de la información recibida.
4. Notificar respuesta: El HSS envía una respuesta de notificación al MME, confirmando la actualización e incluyendo cualquier dato o instrucción adicional necesaria.

¿Cuál es la función del AVP de identificador de red visitado?

El par de valores de atributos (AVP) del identificador de red visitado (VNI) es de tipo cadena de octetos. Este AVP contiene un identificador que ayuda a la red doméstica a identificar la red visitada (por ejemplo, el nombre de dominio de la red visitada).

VNI AVP sirve para identificar la red en la que se encuentra actualmente el usuario, o "visitante", y se utiliza principalmente en situaciones de itinerancia. Esta información es crucial para:

- Decisiones de routing: Garantizar que las solicitudes y respuestas se enrutan correctamente entre la red doméstica y la red visitada.
- Aplicación de políticas: Aplicación de políticas de red adecuadas y reglas de cobro basadas en la ubicación del usuario y los acuerdos de la red visitada con la red doméstica.

7.3.105 Visited-Network-Identifier

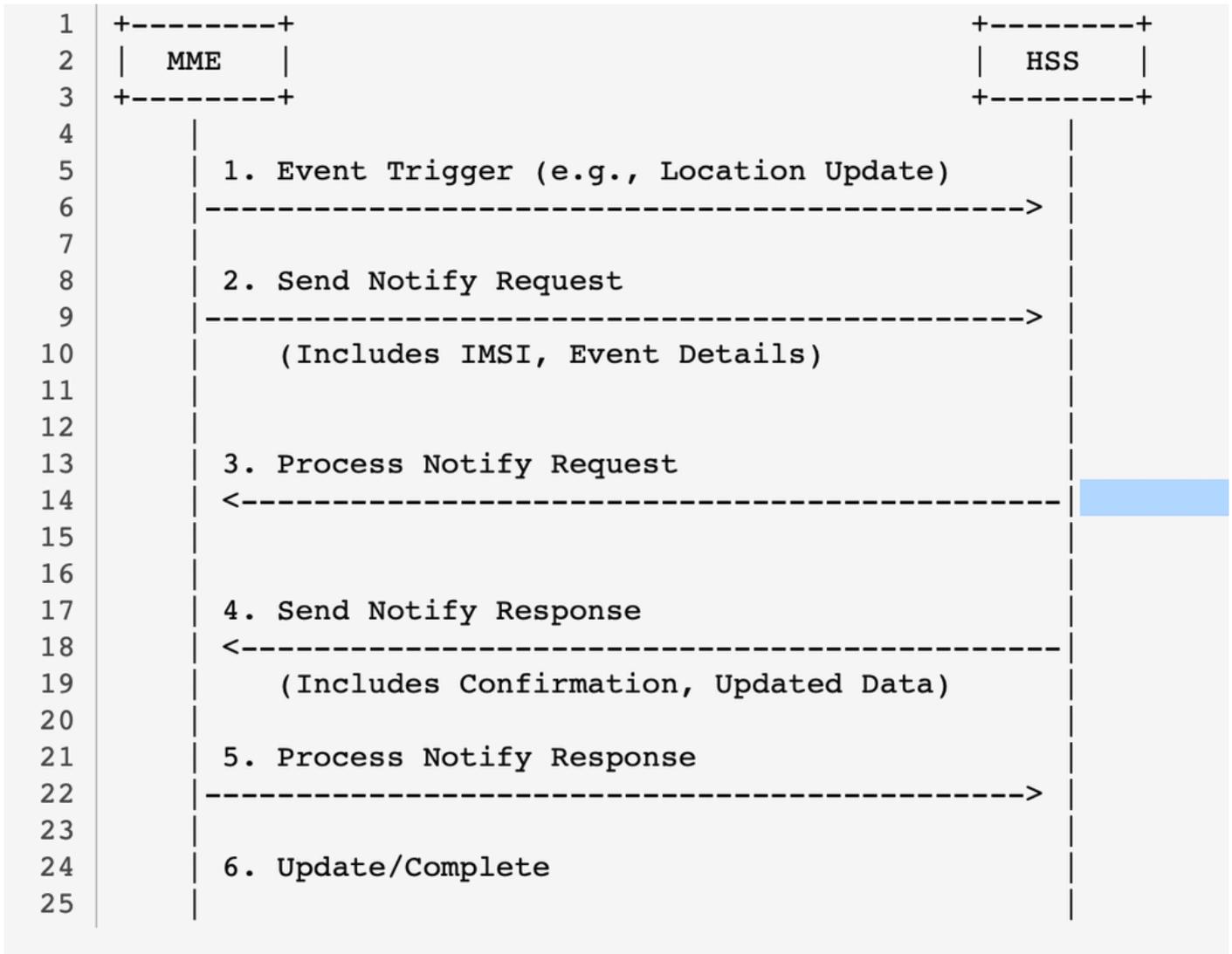
The Visited-Network-Identifier AVP contains the identity of the network where the PDN-GW was allocated, in the case of dynamic PDN-GW assignment.

The AVP shall be encoded as:

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

3gpp reference for Visited-Network-Identifier AVP

Flujo de llamada



NOR call-flow

Flujo de llamada de solicitud/respuesta de notificación

1. Desencadenante de eventos en MME

- Se produce un evento de suscriptor en el MME que requiere la notificación al HSS. Entre los ejemplos, se encuentran los siguientes:
 - Una actualización de ubicación
 - Cambio en la red visitada (por ejemplo, itinerancia)
 - Una actualización de estado de suscripción (por ejemplo, activa o inactiva)
- El MME prepara un mensaje NOR

2. MME envía una solicitud de notificación

- El MME construye el mensaje NOR con estos AVPs clave:
 - Contiene el nombre de dominio de ID de Public Land Mobile Network (PLMN) de la red visitada en la que se encuentra actualmente el suscriptor.
 - ID de sesión: Identificador único de la sesión Diámetro
 - Host de origen y rango de origen: Identifica el MME como el remitente
 - Host de destino y rango de destino: Identifica el HSS como el destinatario

- IMSI (identificador de usuario): El identificador único del suscriptor
- VNI
- Auth-Session-State: Indica si la sesión es stateful o stateless

3. HSS recibe y procesa solicitudes de notificación

- El HSS procesa el NOR y valida sus AVP:
 - Verifique el IMSI para localizar el registro del suscriptor.
 - Valida el VNI para asegurarse de que corresponde a una red conocida y admitida.
 - Actualiza los datos del suscriptor para reflejar la nueva red o estado visitado.
- Si la validación es correcta, HSS prepara una respuesta correcta.
- Si hay problemas (p. ej., falta VNI), el HSS prepara una respuesta de error.

4. HSS envía una respuesta de notificación (NOA)

- El HSS envía un mensaje NOA al MME:
 - DIAMETER_SUCCESS (2001): Indica que el procesamiento se realizó correctamente
 - DIAMETER_INVALID_AVP_VALUE (5004): Si el VNI no es válido
 - DIAMETER_MISSING_AVP (5005): Si falta el VNI pero es obligatorio
 - Contiene el AVP de VNI si causó la falla
- Código de resultado
- AVP fallido (si procede)

5. MME maneja el Notify-Answer

- Al recibir el NOA:
 - Si Result-Code es exitoso, MME continúa con sus operaciones
 - Si se indica un error, el MME analiza el AVP fallido (si existe) para identificar el problema

Troubleshoot

- El aspecto principal es comprobar si la 'solicitud de notificación' está 'habilitada' en todos los 'servicios HSS'. Puede lograr lo mismo ejecutando esta CLI:

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

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

- Una vez que se verifica, puede solicitar estos registros para resolver el problema más a fondo:

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.

Situación problemática

Io.	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]

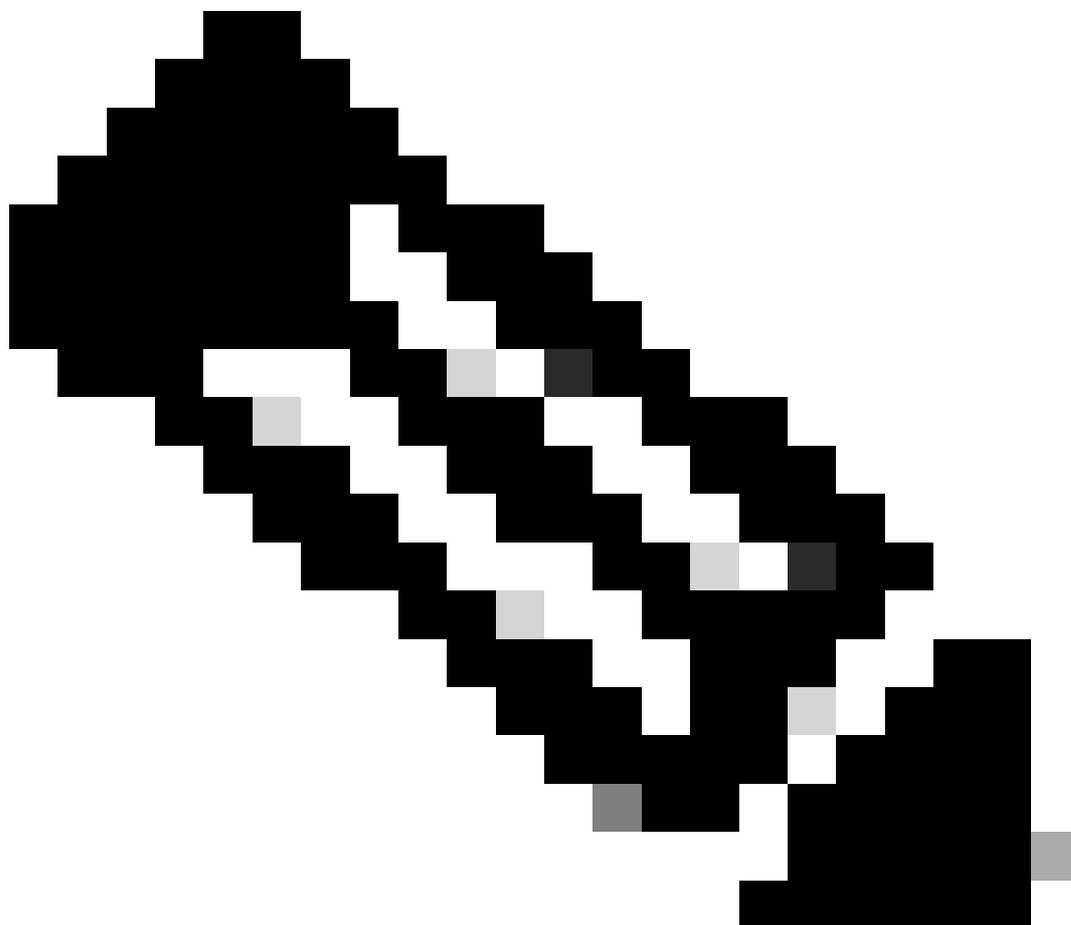
```

PCAP problemático

En esta referencia de Captura de paquetes (PCAP), puede ver el "identificador de red visitado" que falta en "notify-answer".

El paquete 190 es la 'solicitud de notificación' y 191 es la 'respuesta de notificación'.

El código de resultado de diámetro en este escenario es 'Diameter_Missing_AVP', post que también puede ver el 'Failed AVP' que apunta a 'Visited-Network-Identifier' que a su vez muestra 'data empty'.



Nota: El AVP fallido es un AVP agrupado que proporciona información de depuración cuando una solicitud se rechaza o no se procesa por completo debido a un error en un AVP específico.

Algunas razones para un Failed-AVP incluyen:

- Un AVP que no está construido correctamente
 - Un AVP no reconocido o no admitido
 - Un valor AVP no válido
 - Falta un AVP requerido
 - Un AVP que se excluye explícitamente
-

-
- Un AVP restringido a 0, 1 o 0-1 ocurrencias, pero hay dos o más ocurrencias
-

Para solucionar el problema, debe asegurarse de que continúa con todos los registros solicitados.

Como se insistió anteriormente, primero debe verificar la configuración hss-peer-service del nodo problemático.

Configuración de referencia:

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

En esta configuración, puede ver que no había 'no diametro update-dictionary-avps'. El problema era evidente cuando no había un diccionario de actualización asignado a ninguna de las versiones 3gpp. Además, puede encontrarse con algunos escenarios donde la CLI 'diametro update-dictionary-avps 3gpp-r9/10' está presente y el problema sigue siendo evidente.

Por lo tanto, se actualizó a la última versión de acuerdo con la guía de administración de StarOS para rectificar el problema, que es la versión 11.

Esta es la configuración de referencia:

```
<#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.

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).