

Risoluzione dei problemi relativi all'AVP Visited-Network-Identifier mancante in Notify Request

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Panoramica](#)

[Formato messaggio di NOR-NOA](#)

[Processo](#)

[Qual è il ruolo di AVP \(Visited Network Identifier\)?](#)

[Flusso di chiamata](#)

[Flusso di chiamata Notify-Request/Answer](#)

[Risoluzione dei problemi](#)

[Scenario problematico](#)

Introduzione

In questo documento viene descritto come risolvere i problemi relativi al VNI mancante nel messaggio "Notifica richiesta" tra MME e HSS sull'interfaccia S6a.

Prerequisiti

Specifiche tecniche 3GPP - 29.272, 29.229

RFC (Request for Comments) - 6733

Requisiti

Cisco raccomanda la conoscenza della guida per l'amministratore di StarOS-Mobility Management Entity (MME).

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Panoramica

Richiesta e risposta di notifica (NOR/NOA) è uno dei messaggi più semplici con l'interfaccia S6a/S6d. L'idea di base di questo messaggio è informare il Home Subscriber Server (HSS) della modifica nelle informazioni relative alla rete e all'apparecchiatura utente.

La procedura di notifica viene utilizzata tra l'MME e l'HSS, anche tra il GPRS Support Node (SGSN) e l'HSS al fine di notificare all'HSS quanto segue:

- Assegnazione, modifica o rimozione di Packet Data Network (PDN) Gateway (GW) per un Access Point Name (APN)
- Quando non viene eseguito un aggiornamento della posizione tra MME, ma è necessario che l'HSS venga informato della necessità di inviare una posizione di annullamento all'SGSN corrente.
- L'entità utente (UE) dispone di capacità di memoria per ricevere uno o più messaggi brevi
- L'UE è di nuovo raggiungibile

Formato messaggio di 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]

Processo

1. Avvio: Il processo viene in genere avviato dall'MME quando si verifica un evento rilevante correlato all'UE.
2. Messaggio NOR: Il ME invia un messaggio NOR all'HSS. Questo messaggio include gli identificatori necessari, ad esempio IMSI (International Mobile Subscriber Identity), e i dettagli dell'evento o della modifica.
3. Elaborazione tramite HSS: L'HSS elabora la richiesta, aggiorna i propri record e può eseguire ulteriori azioni in base alle informazioni ricevute.
4. Notifica risposta: L'HSS invia una risposta di notifica all'MME, confermando l'aggiornamento e includendo eventuali dati o istruzioni supplementari necessari.

Qual è il ruolo di AVP (Visited Network Identifier)?

La coppia di valori dell'attributo VNI (Visited-Network-Identifier) è di tipo Octet-String. Questo AVP contiene un identificatore che consente alla rete domestica di identificare la rete visitata (ad esempio, il nome di dominio della rete visitata).

Il VNI AVP serve a identificare la rete in cui si trova attualmente l'utente, o "in visita", ed è utilizzato principalmente in scenari di roaming. Queste informazioni sono fondamentali per:

- Decisioni di routing: Garantire che le richieste e le risposte siano instradate correttamente tra la rete domestica e la rete visitata.
- Applicazione delle policy: Applicare policy di rete e regole di tariffazione appropriate in base alla posizione dell'utente e agli accordi della rete visitata con la rete domestica.

7.3.105 Visited-Network-Identifier

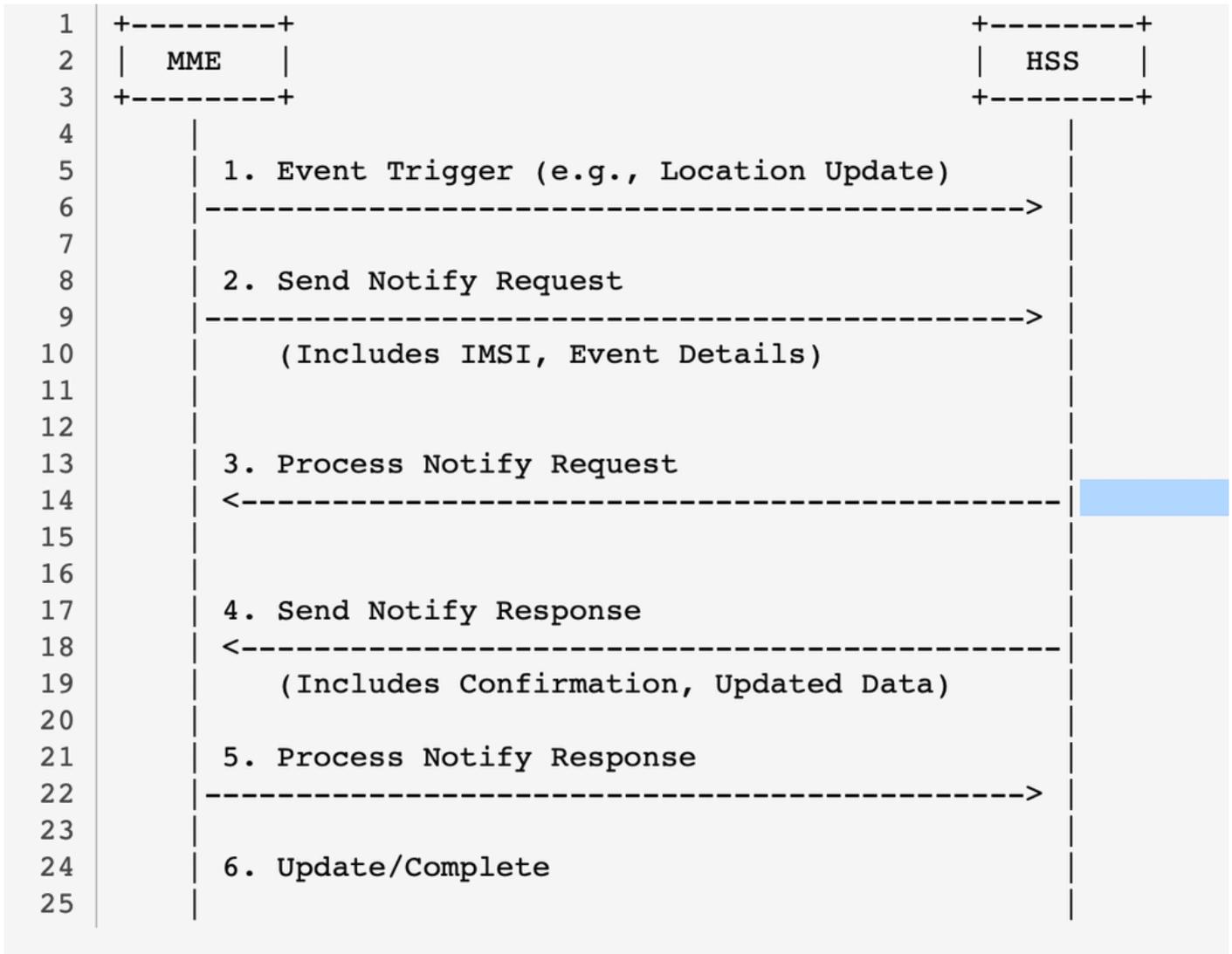
The Visited-Network-Identifier AVP contains the identity of the network where the PDN-GW was allocated, in the case of dynamic PDN-GW assignment.

The AVP shall be encoded as:

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

Riferimento 3gpp per AVP Visited-Network-Identifier

Flusso di chiamata



flusso di chiamata NOR

Flusso di chiamata Notify-Request/Answer

1. Trigger di evento in MME

- Si verifica un evento sottoscrittore nell'MME che richiede una notifica all'HSS. Alcuni esempi:
 - Aggiornamento percorso
 - Una modifica nella rete visitata (ad esempio, roaming)
 - Aggiornamento dello stato di una sottoscrizione (ad esempio, attiva o inattiva)
- L'MME prepara un messaggio NOR

2. MME invia Notify-Request

- L'MME costruisce il messaggio NOR con questi AVP chiave:
 - Contiene il nome di dominio dell'ID Public Land Mobile Network (PLMN) della rete visitata in cui si trova attualmente il sottoscrittore.
 - ID sessione: Identificatore univoco per la sessione Diameter
 - Origin-Host e Origin-Realm: Identifica l'MME come mittente
 - Destinazione-Host e Destinazione-Realm: Identifica HSS come destinatario
 - IMSI (identificatore utente): Identificatore univoco del sottoscrittore

- VNI
- Auth-Session-State: Indica se la sessione è con o senza stato

3. HSS riceve e elabora la richiesta di notifica

- L'HSS elabora il NOR e convalida i relativi AVP:
 - Controllare l'IMSI per individuare il record del destinatario.
 - Convalida il VNI per verificare che corrisponda a una rete nota e supportata.
 - Aggiorna i dati del sottoscrittore in base al nuovo stato o alla nuova rete visitata.
- Se la convalida ha esito positivo, HSS prepara una risposta.
- In caso di problemi (ad esempio, assenza di VNI), HSS prepara una risposta di errore.

4. HSS invia una notifica-risposta (NOA)

- L'HSS invia un messaggio NOA all'MME:
 - DIAMETER_SUCCESS (2001): Indica la riuscita dell'elaborazione
 - DIAMETER_INVALID_AVP_VALUE (5004): Se il VNI non è valido
 - DIAMETER_MISSING_AVP (5005): Se il VNI è mancante ma richiesto
 - Contiene l'AVP VNI se ha causato il problema
- Codice risultato
- AVP non riuscito (se applicabile)

5. MME gestisce la Notify-Answer

- Al ricevimento del NOA:
 - Se il codice risultato ha esito positivo, MME continua le operazioni
 - Se viene indicato un errore, l'MME analizza l'AVP non riuscito (se presente) per identificare il problema

Risoluzione dei problemi

- L'aspetto principale consiste nel verificare se la richiesta di notifica è abilitata in tutti i servizi HSS. A tal fine, è possibile eseguire questa CLI:

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

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

- Una volta selezionata questa opzione, è possibile richiedere questi registri per risolvere ulteriormente il problema:

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.

Scenario problematico

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) ...


```

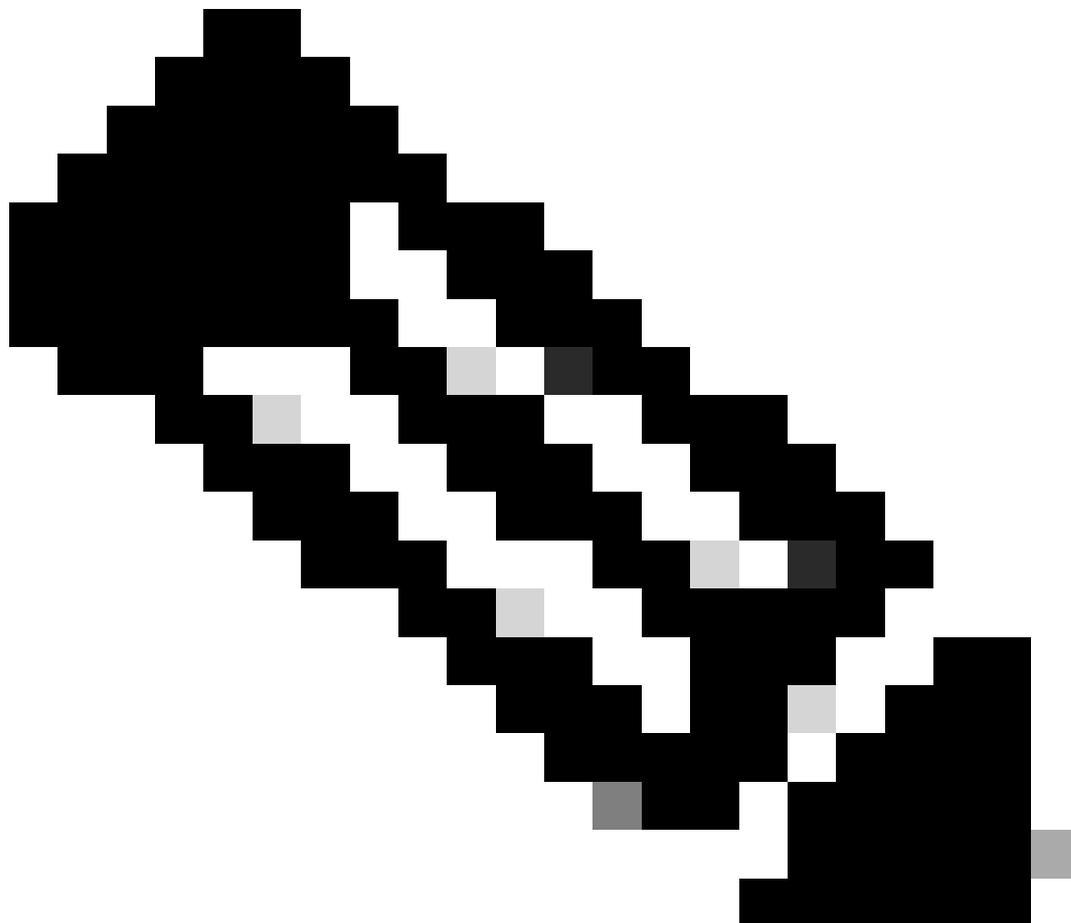
> Frame 191: 378 bytes on wire (3024 bits), 378 bytes captured (3024 bits)
> Ethernet II, Src: Cisco_5b:4f:6...
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 97
> Internet Protocol Version 4, ...
> Stream Control Transmission Protocol, ...
< Diameter Protocol
  Version: 0x01
  Length: 312
  > Flags: 0x40, 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]
  
```

Problematic pcap

In questo documento di riferimento relativo all'acquisizione dei pacchetti (PCAP), è possibile visualizzare l'identificatore di rete visitato mancante in notifica-risposta.

Il pacchetto 190 è la 'richiesta di notifica' e 191 è la 'risposta di notifica'.

In questo scenario, il codice del risultato del diametro è 'Diameter_Missing_AVP', che consente di visualizzare anche 'Errore AVP' che punta a 'Visited-Network-Identifer', che a sua volta visualizza 'data empty'.



Nota: La funzione AVP non riuscita è una funzione AVP raggruppata che fornisce informazioni di debug quando una richiesta viene rifiutata o non completamente elaborata a causa di un errore in una funzione AVP specifica.

Alcuni dei motivi che giustificano un errore nell'AVP sono:

- Avp non costruito correttamente
 - Avp non riconosciuto o non supportato
 - Valore AVP non valido
 - Avp richiesto mancante
 - Avp esplicitamente escluso
-

· Avp limitato a 0, 1 o 0-1 occorrenze, ma con due o più occorrenze

Per risolvere ulteriormente il problema, accertarsi di esaminare tutti i registri richiesti.

Come richiesto in precedenza, è innanzitutto necessario controllare la configurazione hss-peer-service del nodo problematico.

Configurazione di riferimento:

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

In questa configurazione, è possibile verificare la presenza di 'no diameter update-dictionary-avps'. Il problema era evidente quando non c'era un update-dictionary mappato a nessuna delle release 3gpp. Inoltre, è possibile incontrare alcuni scenari in cui è presente il problema CLI 'diametralmente update-dictionary-avps 3gpp-r9/10' e ancora il problema è evidente.

Pertanto, è stato aggiornato all'ultima release come da StarOS admin guide per correggere il problema, che è la release 11.

La configurazione di riferimento è la seguente:

```
<#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.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).