

Notify要求下にVisited-Network-Identifier AVPが存在しない場合のトラブルシューティング

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[概要](#)

[NOR-NOAのメッセージ形式](#)

[プロセス](#)

[訪問済みネットワーク識別子\(AVP\)の役割は何ですか。](#)

[コールフロー](#)

[Notify-Request/Answerコールフロー](#)

[トラブルシュート](#)

[問題のあるシナリオ](#)

はじめに

このドキュメントでは、S6aインターフェイスを介したMMEとHSS間の「Notify request」メッセージの下にVNIが表示されない場合のトラブルシューティング方法について説明します。

前提条件

3GPP技術仕様 – 29.272、29.229

コメント要求(RFC) - 6733

要件

StarOS-Mobility Management Entity(MME)管理ガイドに関する知識があることが推奨されます。

使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

概要

Notification Request and Answer(NOR/NOA)は、S6a/S6dインターフェイスを介した最も単純なメッセージの1つです。このメッセージの基本的な概念は、ネットワークおよびユーザ機器情報の変更についてホームサブスクライバサーバ(HSS)に通知することです。

通知手順は、MMEとHSSの間、およびサービングGPRSサポートノード(SGSN)とHSSの間で使
用され、HSSに次の情報を通知します。

- アクセスポイント名(APN)のパケットデータネットワーク(PDN)ゲートウェイ(GW)の割り当て/変更/削除
- MME間のロケーション更新が発生しないが、現在のSGSNにキャンセルロケーションを送信する必要があることをHSSに通知する必要がある場合。
- ユーザーエンティティ(UE)には、1つ以上のショートメッセージを受信できるメモリ容量があります
- UEが再び到達可能になった

NOR-NOAのメッセージ形式

```
< 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 ]
```

プロセス

1. 開始：このプロセスは通常、UEに関連するイベントが発生したときにMMEによって開始されます。
2. NORメッセージ：MMEはHSSにNORメッセージを送信します。このメッセージには、International Mobile Subscriber Identity(IMSI)などの必要なIDと、イベントまたは変更の詳細が含まれます。
3. HSSによる処理：HSSは要求を処理し、そのレコードを更新し、受信した情報に基づいて必要に応じてアクションを実行できます。
4. Notify Response:HSSはNotify ResponseをMMEに返し、更新を確認し、追加の必要なデータまたは指示を含めます。

訪問済みネットワーク識別子(AVP)の役割は何ですか。

Visited-Network-Identifier(VNI)属性値ペア(AVP)のタイプはオクテット文字列です。このAVPには、訪問先のネットワークをホームネットワークが識別するのに役立つ識別子（訪問先のネットワークドメイン名など）が含まれています。

VNI AVPは、ユーザが現在配置されているネットワーク、つまり「訪問先」を特定する役割を果たし、主にローミングシナリオで使用されます。この情報は、次の目的のために不可欠です。

- ・ ルーティングの決定：要求と応答がホームネットワークと訪問先ネットワークの間で正しくルーティングされることを確認します。
- ・ ポリシーの適用：ユーザの場所と、訪問先のネットワークとホームネットワークの契約に基づいて、適切なネットワークポリシーと課金ルールを適用します。

7.3.105 Visited-Network-Identifier

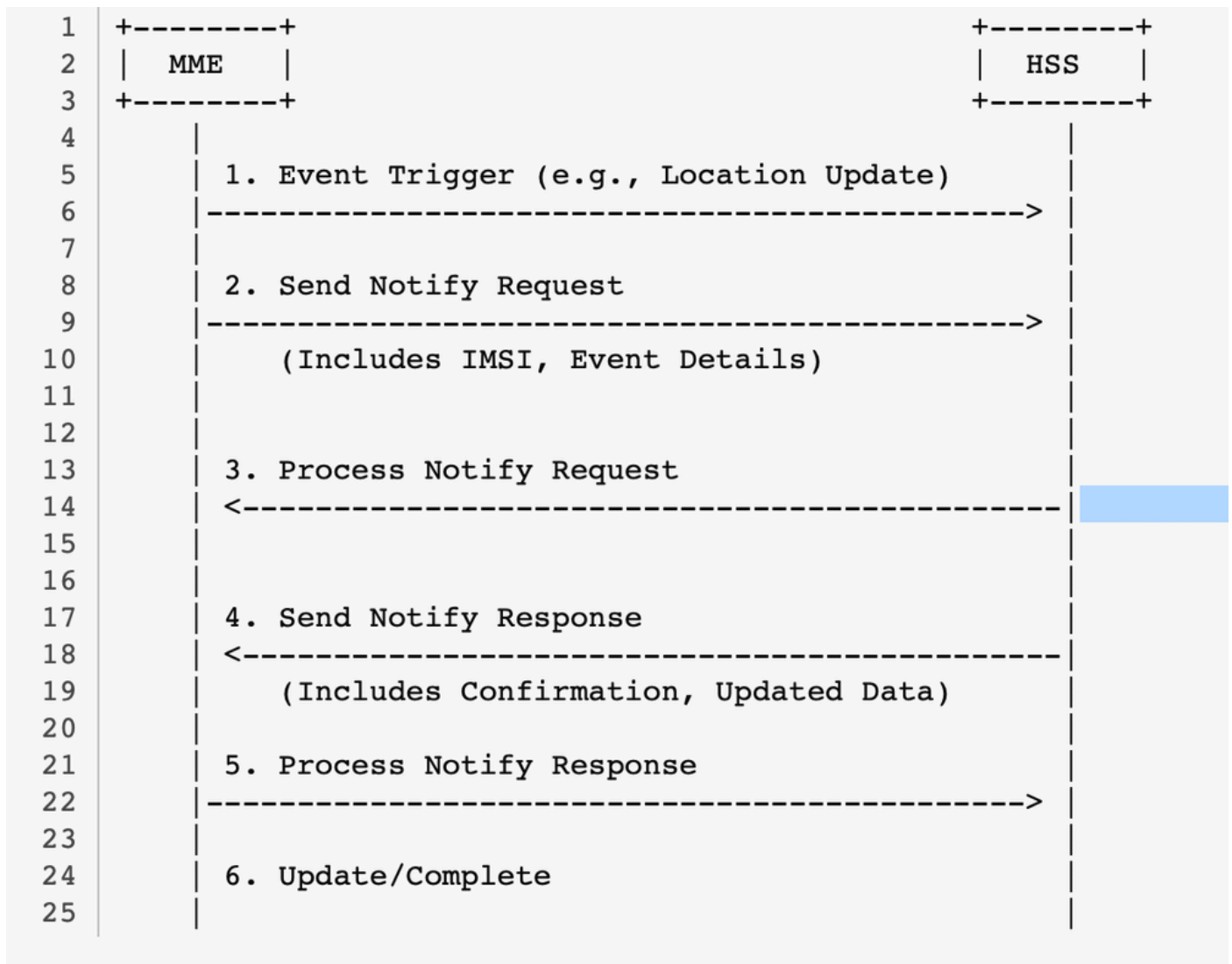
The Visited-Network-Identifier AVP contains the identity of the network where the PDN-GW was allocated, in the case of dynamic PDN-GW assignment.

The AVP shall be encoded as:

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

Visited-Network-Identifier AVPの3gppリファレンス

コールフロー



NORコールフロー

Notify-Request/Answerコールフロー

1. MMEのイベントトリガー

- 加入者イベントは、HSSへの通知を必要とするMMEで発生します。次に例を示します。
 - 場所の更新
 - アクセスしたネットワークの変更（ローミングなど）
 - サブスクリプションステータスの更新（アクティブまたは非アクティブなど）
- MMEはNORメッセージを準備します

2. MMEが通知要求を送信

- MMEは、次のキーAVPを使用してNORメッセージを作成します。
 - サブスクライバが現在配置されている訪問先ネットワークのPublic Land Mobile Network(PLMN)IDドメイン名が含まれます。
 - Session-ID:Diameterセッションの一意の識別子
 - Origin-HostおよびOrigin-Realm:MMEを送信元として識別します。
 - Destination-HostおよびDestination-Realm：受信者としてHSSを識別します。
 - IMSI(User-Identifier)：サブスクライバの一意の識別子

- VNI
- Auth-Session-State : セッションがステートフルかステートレスかを示します。

3. HSSがNotify-Requestを受信して処理する

- HSSはNORを処理し、そのAVPを検証します。
 - IMSIをチェックして、サブスクライバのレコードを見つけます。
 - VNIを検証して、既知のサポート対象ネットワークに対応していることを確認します。
 - 加入者のデータを更新して、新たにアクセスしたネットワークまたはステータスを反映させます。
- 検証が成功すると、HSSは成功した応答を準備します。
- 問題がある場合 (VNIの欠落など)、HSSはエラー応答を準備します。

4. HSSがNotify-Answer(NOA)を送信

- HSSがMMEにNOAメッセージを送信します。
 - DIAMETER_SUCCESS (2001) : 処理の成功を示します。
 - DIAMETER_INVALID_AVP_VALUE (5004): VNIが無効な場合
 - DIAMETER_MISSING_AVP (5005): VNIが欠落しているが必須の場合
 - 障害の原因がVNI AVPである場合、そのAVPが含まれます。
- 結果コード
- AVPの失敗 (該当する場合)

5. MMEによるNotify-Answerの処理

- NOAを受信すると、次のようになります。
 - Result-Codeが成功した場合、MMEは処理を続行します
 - エラーが示された場合、MMEは問題を特定するために失敗したAVP (存在する場合) を分析します

トラブルシューティング

- 主な側面は、すべての「HSSサービス」で「notify request」が「有効」になっているかどうかを確認することです。 次のCLIを実行して、同じことを実行できます。

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

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

- これがチェックされたら、問題をさらにトラブルシューティングするために次のログを要求できます。

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.

問題のあるシナリオ

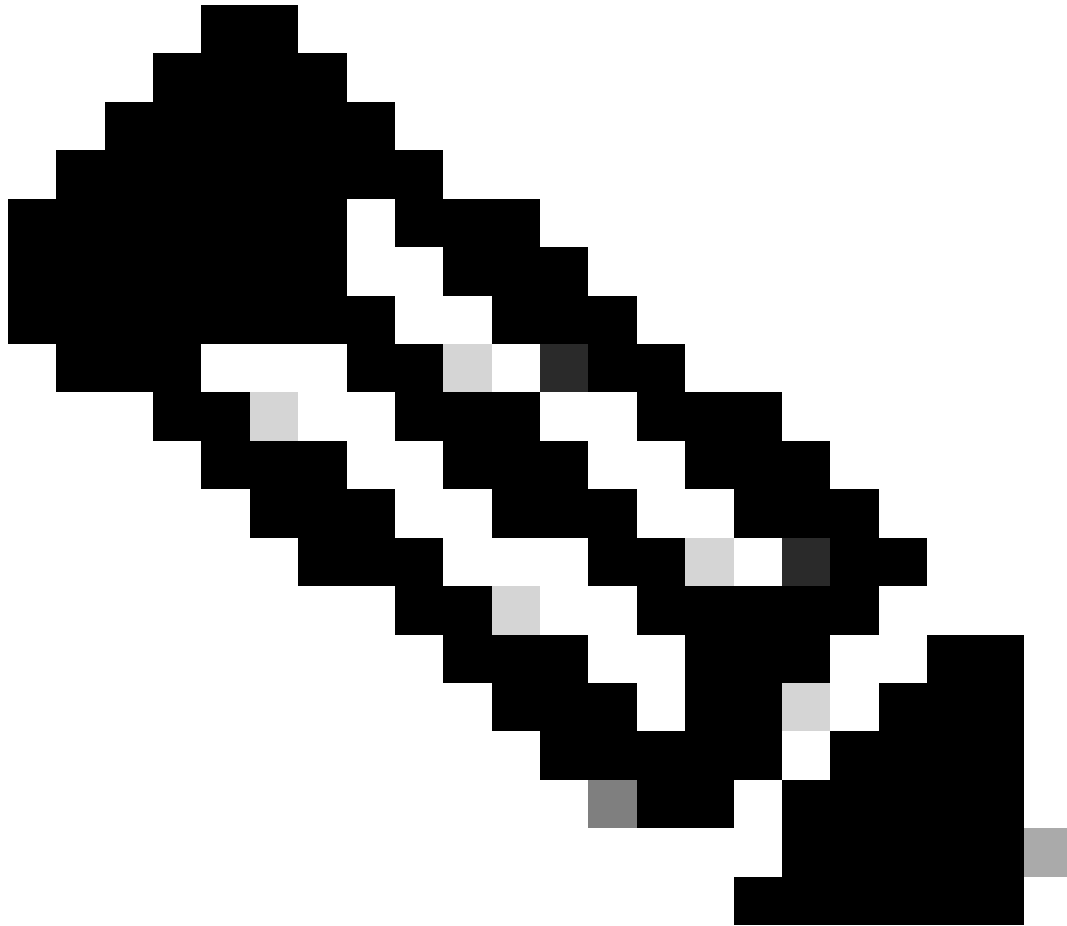
No.	Time	Info
190	2024-11-06 13:02:50.059...	cmd=3GPP-Notify Request(323) flags=RP-- appl=3GPP S...
191	2024-11-06 13:02:50.163...	cmd=3GPP-Notify Answer(323) flags=-P-- appl=3GPP S6...
192	2024-11-06 13:02:50.059...	DATA (TSN=4269) (retransmission)
193	2024-11-06 13:02:50.163...	DATA (TSN=4147) (retransmission)
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]		

問題のあるpcap

この参照パケットキャプチャ(PCAP)では、「notify-answer」の下に「visited-network-Idenfifier」が欠落しているのが確認できます。

パケット190は「Notify request」であり、191は「Notify Answer」です。

このシナリオでのdiameterの結果コードは「Diameter_Missing_AVP」です。この投稿では、「Failed AVP」（訪問先ネットワーク識別子）を参照できます。このAVPは、結果として「data empty」を表示します。



注：失敗したAVPは、グループ化されたAVPであり、特定のAVPでのエラーが原因で要求が拒否された場合や要求が完全に処理されなかった場合に、デバッグ情報を提供します。

Failed-AVPの原因には次のようなものがあります。

- ・ 適切に構築されていないAVP
 - ・ 認識されないまたはサポートされていないAVP
 - ・ 無効なAVP値
 - ・ 必要なAVPが見つかりません
 - ・ 明示的に除外されるAVP
-

-
- ・ 0、1、または0-1回に制限されているが、2回以上の出現があるAVP
-

問題をさらにトラブルシューティングするには、要求されたすべてのログを確認して処理を進める必要があります。

前述のように、まず問題のあるノードのhss-peer-service設定をチェックする必要があります。

リファレンス構成：

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

この設定では、「no diameter update-dictionary-avps」があったことがわかります。この問題は、3gpp-releaseのいずれにもマップされたupdate-dictionaryがないときに明らかになりました。また、CLI「diameter update-dictionary-avps 3gpp-r9/10」が存在し、引き続き問題が明らかなシナリオもいくつか見られます。

そのため、StarOS管理ガイドに従って最新リリースに更新され、問題を修正しました。これはリリース11です。

リファレンス設定を次に示します。

<#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.

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。