HSS AAA 系统原理概述

HUAWEI

培训目标

- 学完本课程后，您应该能：
  - 了解**HSS9860**在**LTE**网络中的地位
  - 了解**UIM**在**eHRPDF**网络中的地位
  - 熟悉华为**HSS9860/UIM**的系统结构和逻辑结构，及其中各个组成部分功能和关系

目录

目　录

一 定位

1.1 HSS9860 定位

HSS9860定位

- **HSS9860**是大容量归属用户签约数据管理设备，采用先进的软、硬件技术，具备丰富的业务提供能力和强大的组网能力。
- **HSS9860**定位于用户签约数据的管理和融合，为终端用户接入各种网络提供移动性管理、鉴权、签约数据管理等功能。支持**3GPP UDC**融合架构，即**FE**、**BE**分离。
- 配合华为公司的**VoLTE**解决方案，提供**CSFB**、**SRVCC**、**SVLTE**等功能。
- **HSS9860**可应用于物联网，是**M2M**（**Machine to Machine**）通信的终端归属位置寄存器，负责存储物联网终端用户的业务签约信息，并负责将终端状态信息同步给物联网运营管理平台。

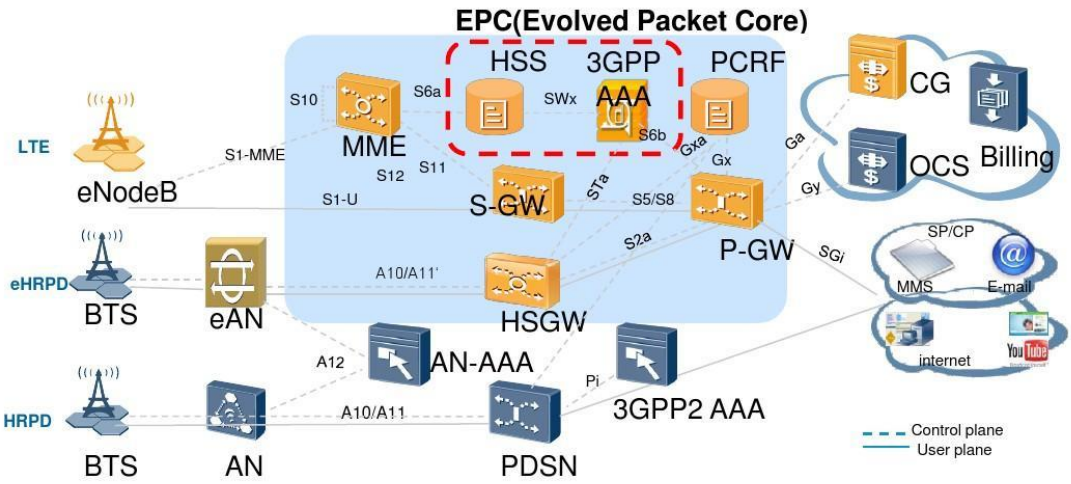
1.2 UIM 定位

UIM定位

- UIM是Unified Identity Management的简称，是指**统一身份管理**业务。
- UIM（Unified Identity Management）产品应用于华为公司IDM（Identity Management）解决方案，可以跨不同的网络、不同的业务平台提供统一的ID管理，从而简化网络中的ID管理及鉴权管理，提升用户业务体验，提高网络安全。
- UIM主要功能是通过RADIUS/Diameter协议和接入设备配合，对用户访问网络的权限进行控制，对认证、授权和计费三种功能提供一致性管理。

1.3 网络位置

HSS9860/UIM在LTE/EPC网络中的位置



- **HUAWEI HSS9860** 实现**EPC(3GPP R8)**网络中的**HSS**功能.
- 为**LTE**接入提供**S6a**接口。
- 为**Non-3GPP**接入**(WLAN、WiMAX、CDMA)**等网络接入提供**SWx**接口。

二 接口和协议

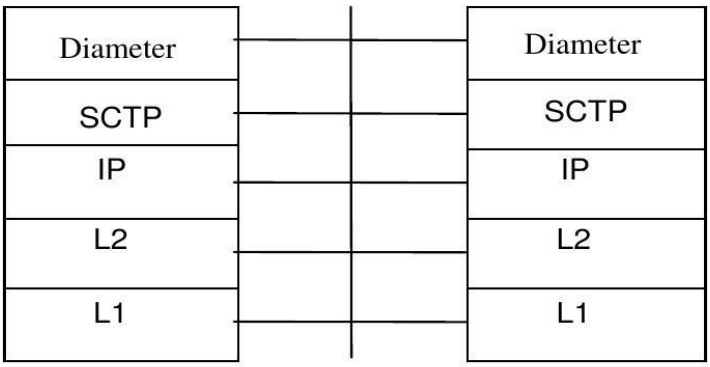
2.1 EPS 的业务接口

EPS网络中的业务接口

接口	协议	作用
S6a（HSS-MME）	Diameter（SCTP）	LTE移动性管理、鉴权、签约数据管理
SWx（HSS-AAA）	Diameter（SCTP）	Non-3GPP接入移动性管理、鉴权、签约数据管理
STa（AAA-HSGW）	Diameter（SCTP）	完成可信Non-3GPP网络的鉴权和授权
S6b（AAA-P-GW）	Diameter（SCTP）	认证完成后PGW用于更新PGW地址到HSS
BOSS对接	MML（私有）,SOAP（公有）	
PGW Web LMT	MML	

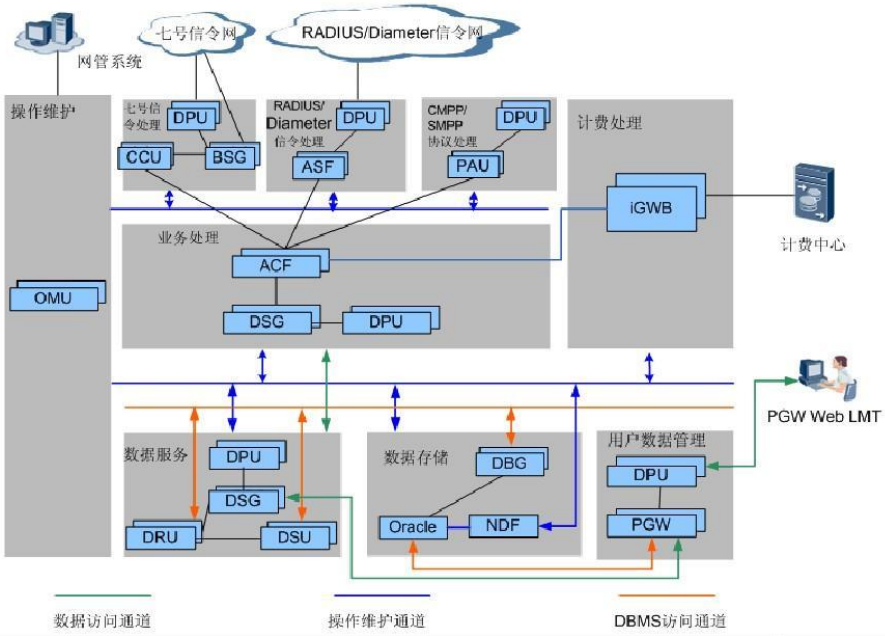
2.2 Diameter 协议栈

Diameter协议栈



三 HSS9860 协议结构

UIM内部逻辑结构

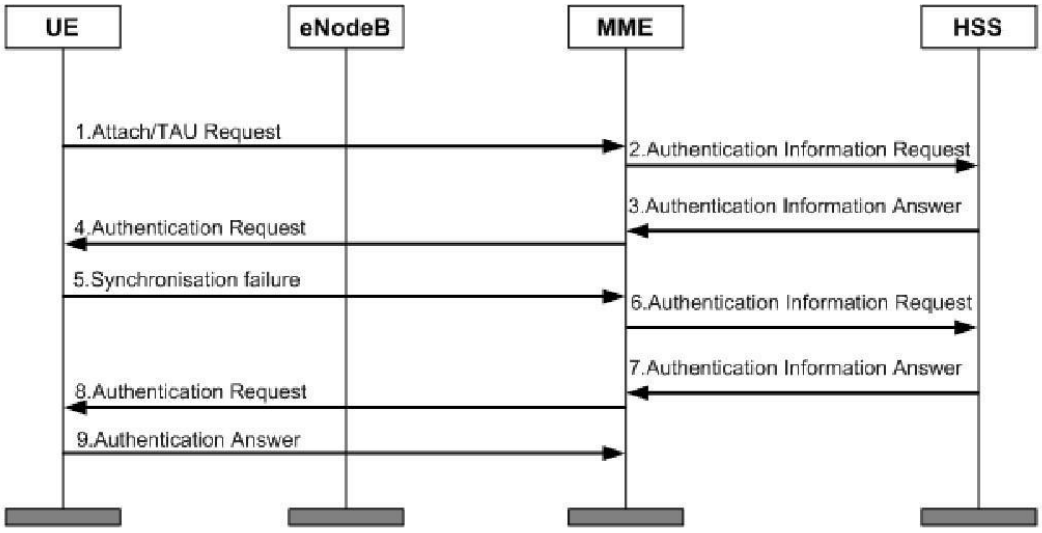


四 功能特性

目　录

4.1 EPS-AKA 鉴权（EPS 鉴权）

EPS-AKA鉴权（EPS鉴权）



4.2 通配 APN 功能

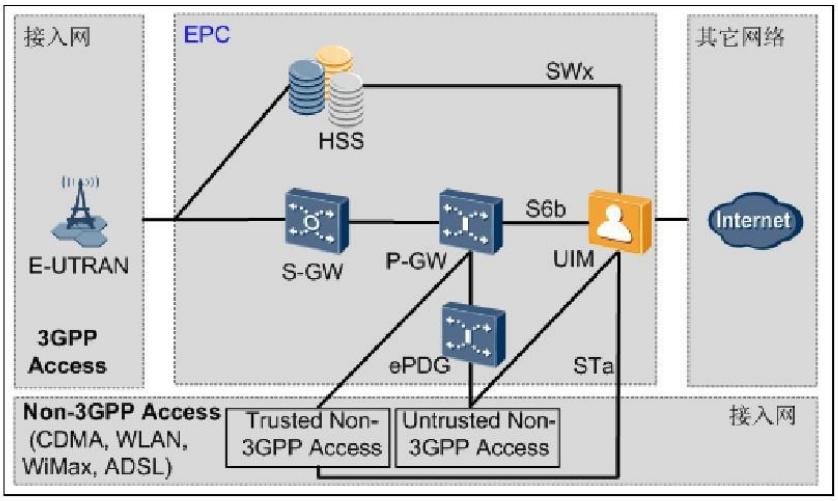
通配APN功能

- 给用户签约**APN(Access Point Name)**时，使用通配符“*”表示通配**APN**。签约通配**APN**后,用户根据实际情况选择合适的**APN**接入网络。
- 具体的业务实现主要是由**MME**来完成的，**SAE-HSS**只负责签约信息的存储和下发。

4.3 Non-3GPP 接入

Non-3GPP接入功能

Non-3GPP接入功能组网图



HUAWEI

Non-3GPP接入功能

UIM能够实现对Non-3GPP接入用户的认证，使之安全接入EPC（Evolved Packet Core）网络EPC是3G的后续演进技术，给用户提供了速率更高、时延更低的分组数据业务，支持语音、视频、数据文件交换等业务。

- STa接口 用于Non-3GPP接入网络和UIM之间，完成Non-3GPP接入用户的认证和授权。
- SWx接口 用于UIM和HSS之间。Non-3GPP用户通过UIM从HSS获取鉴权向量和用户数据，当HSS中的Non-3GPP用户销户或者用户数据发生变化时，HSS会通过该接口通知UIM注销用户或者更新其中的用户数据。
- S6b接口 用于P-GW（Packet Data Network Gateway）和UIM之间，将P-GW的地址更新到HSS，使用户在3GPP网络和Non-3GPP网络间切换时，不会出现PDN连接断连。

五 关键业务流程

5.1 S6A 接口

关键业务流程（S6a接口）

移动性管理过程	消息名称	简写
位置管理	Update-Location-Request/Answer	ULR/ULA
	Cancel-Location-Request/Answer	CLR/CLA
	Purge-UE-Request/Answer	PUR/PUA
用户数据管理	Insert Subscriber Data-Request/Answer	IDR/IDA
	Delete-Subscriber-Data-Request/Answer	DSR/DSA
鉴权管理	Authentication-Information-Request/Answer	AIR/AIA
故障恢复	Reset-Request/Answer	RSR/RSA
通知	Notify-Request/Answer	NOR/NOA

5.1.1 鉴权管理 AIR/AIA

鉴权管理消息AIR/AIA

- AIR/AIA消息流向（此消息由MME/S4-SGSN触发）
  - AIR：MME/S4-SGSN流向HSS
  - AIA：HSS流向MME/S4-SGSN
- AIR/AIA消息功能：
  - 当MME/S4-SGSN请求鉴权信息时会触发AIR消息，HSS收到AIR消息，会将用户的鉴权信息打包到AIA消息中发送给MME/S4-SGSN。

5.1.2 位置管理 ULR/ULA/CLR/CLA/PUR/PUA

位置管理消息ULR/ULA

- ULR/ULA消息流向（此消息由MME/S4-SGSN触发）
  - ULR：MME/S4-SGSN流向HSS
  - ULA：HSS流向MME/S4-SGSN
- ULR/ULA消息功能：
  - 当用户的位置信息发生改变时（MME局间切换、MME到S4SGSN切换等），MME/S4-SGSN触发ULR消息，通知HSS当前服务用户的MME/S4-SGSN标识。
  - 当HSS收到ULR消息时，会响应ULA消息，通知MME/S4-SGSN更新用户数据。
  - MME/S4-SGSN触发ULR消息为HSS提供其他用户数据，如用户终端信息。
  - 位置更新完成后，用户终端信息、用户当前所处的MME/S4SGSN地址信息（MME host、MME realm）将在HSS中进行更新。

位置管理消息CLR/CLA

- CLR/CLA消息流向（此消息由HSS触发）
  - CLR：HSS流向MME/S4-SGSN
  - CLA：MME/S4-SGSN流向HSS
- CLR/CLA消息功能：
  - HSS通知MME/S4-SGSN某个用户被操作员销户或者补卡。
  - 如果UE移动到了新的MME/S4-SGSN区域，HSS会通知以前的MME/S4-SGSN取消当前用户位置登记。

位置管理消息PUR/PUA

- **PUR/PUA**消息流向（此消息由**MME/S4-SGSN**触发）
  - **PUR**：**MME/S4-SGSN**流向**HSS**
  - **PUA**：**HSS**流向**MME/S4-SGSN**
- **PUR/PUA**消息功能：
  - 如果用户长时间不活动，**MME/S4-SGSN**会清除用户数据，同时发送**PUR**消息通知**HSS**将用户的**PURGE**标志位置位。

5.1.3 用户数据管理 IDR/IDA/DSR/DSA

用户数据管理消息IDR/IDA

- IDR/IDA消息流向（此消息由HSS触发）
  - IDR：HSS流向MME/S4-SGSN
  - IDA：MME/S4-SGSN流向HSS
- IDR/IDA消息功能：
  - 在下面的情况下，HSS触发IDR消息通知MME/S4-SGSN更新用户数据（具体命令可参考ULR消息中对打包Subscription-Data 信元部分的描述）
    - 用户签约了新的数据，或者签约数据发生变化。（具体命令可参考ULR消息中对打包Subscription-Data 信元部分的描述）
    - 运营商给用户启用、改变或者删除了ODB。
    - 运营商给用户开启了全网跟踪。

用户数据管理消息DSR/DSA

- DSR/DSA消息流向（此消息由HSS触发）
  - DSR：HSS流向MME/S4-SGSN
  - DSA：MME/S4-SGSN流向HSS
- DSR/DSA消息功能：
  - 当需要删除在MME/S4-SGSN中存储的HSS用户签约清单时，HSS会触发DSR/DSA消息流程，需要删除的用户签约清单包括：
    - 在MME/S4-SGSN中用户的EPS签约数据（APN配置签约数据）的子集或者全部 （MOD OPTGPRS）
    - 区域漫游签约信息。（MOD PLMNRSZI）
    - 用户计费特征。（MOD OPTGPRS）
    - SRVCC的会话传输号码。（MOD STNSR）
    - 用户全网跟踪数据。（在LMT客户端上HSS网元下执行RMV UTRCTSK）

5.1.4 故障恢复消息 RSR/RSA

故障恢复消息RSR/RSA

- RSR/RSA消息流向（此消息由HSS触发,由操作员手动触发）
  - RSR：HSS流向MME/S4-SGSN
  - RSA：MME/S4-SGSN流向HSS
- RSR/RSA消息功能：
  - 当HSS重启时，可以由操作员在OMU上执行SND RESET消息，通知MME/S4-SGSN HSS已经重启过。

5.1.5 通知管理 NOR/NOA

通知管理消息NOR/NOA

- NOR/NOA消息流向（此消息由MME/S4-SGSN触发）
  - NOR：MME/S4-SGSN流向HSS
  - NOA：HSS流向MME/S4-SGSN
- NOR/NOA消息功能：
  - 当MME/S4-SGSN局间位置更新没有发生的条件下，该消息被用在MME/S4-SGSN和HSS之间，由MME/S4-SGSN主动发起。HSS需要被通知到：
    - 用户终端信息的更新（IMEI，IMEISV）。
    - APN的PDN GW的指派、变化。

5.2 SWX 接口

关键业务流程（Swx接口）

消息	使用场景
MAR	该消息用于请求认证、授权信息，由3GPP AAA服务器发送至HSS。
MAA	该消息用于响应多媒体认证授权请求命令，由HSS发送至3GPP AAA服务器。
PPR	该消息用于请求更新签约数据，由HSS发送至3GPP AAA服务器。
PPA	该消息用于响应用户签约数据更新请求命令。由3GPP AAA服务器发送至HSS。
SAR	该消息用于请求HSS注册当前正在为用户提供服务的3GPP AAA服务器名称，由3GPP AAA服务器发送至HSS。
SAA	该消息用于响应服务器指派请求命令。SAA消息由HSS发送至3GPP AAA。
RTR	该消息用于请求注销一个用户。RTR消息由HSS发送至3GPP AAA。
RTA	该消息用于响应注册终止请求命令。RTA消息由3GPP AAA发送至HSS。

5.2.1 Non-3gpp 鉴权 MAR/MMA

Non-3GPP鉴权 MAR/MAA

- MAR/MAA消息流向（此消息由AAA触发）
  - MAR：AAA流向HSS
  - MAA：HSS流向AAA
- MAR/MAA消息功能：
  - 当AAA请求鉴权信息时会触发MAR消息，HSS收到MAR消息，会根据MAR请求消息计算相应的鉴权向量，将计算的鉴权向量打包到MAA消息中发送给AAA，并且HSS还会将MAR消息携带的AAA host和AAA realm信息保存至HSS。
  - SWx接口的MAR消息除了鉴权功能外，还兼带一部分注册功能，即，HSS会比较已经保存的AAA host和AAA realm信息和此次MAR消息中的AAA地址信息，如果不同则返回失败，拒绝此次鉴权消息。

5.2.2 Non-3GPP 接入注册 SAR/SAA

Non-3GPP接入注册 SAR/SAA

- **SAR/SAA**消息流向（此消息由**AAA**触发）
  - **SAR**：**AAA**流向**HSS**
  - **SAA**：**HSS**流向**AAA**
- **SAR/SAA**消息功能：

（**1**）用户注册时，**AAA**向**HSS**发送注册通知

（**2**）**AAA**需要从**HSS**获取授权信息时，通过该流程向**HSS**请求授权信息

（**3**）用户去注册时，**AAA**向**HSS**发送去注册通知

（**4**）**P-GW**的地址信息发生更新时，**AAA**通过该流程更新数据到**HSS**中

（**5**）**HSS**发生故障时，**AAA**通过该消息通知**HSS**更新**PDN-GW**信息以完成数据恢复动作

5.2.3 签约数据更新 PPR/PPA

HSS发起的签约数据更新请求流程PPR/PPA

- **PPR/PPA**消息流向（此消息由**HSS**触发）
  - **PPR**：**HSS**流向**AAA**
  - **PPA**： **AAA**流向**HSS**
- **PPR/PPA**消息功能：

  当用户**Non-3GPP**签约数据被修改时，**PPR**消息由**HSS**发起到**AAA**服务器，用于更新在**AAA**服务器中的用户签约信息或者计费信息。

5.2.4 撤销注册流程 RTP/RTA

HSS发起的撤销注册流程 RTR/RTA

- **RTR/RTA**消息流向（此消息由**HSS**触发）
  - **RTR**：**HSS**流向**AAA**
  - **RTA**： **AAA**流向**HSS**
- **RTR/RTA**消息功能：

  该流程用来通知**AAA**删除**Non-3GPP**用户当前的登记状态和所有的关联资源。销户、手动发起**cancel**时都会触发该消息。

5.3 Sta 接口

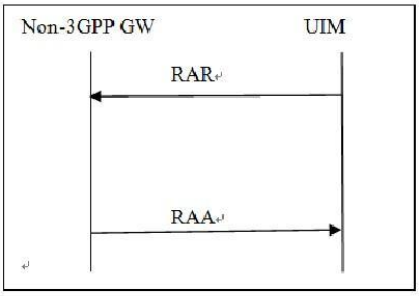
关键业务流程（Sta接口）

功能	消息
Sta接口为HSGW与AAA之间接口，完成可信Non-3GPP网络的鉴权和授权。	DER/DEA ：STa接口基本消息，可信Non-3GPP接入网和3GPP AAA Server认证和授权消息；（鉴权过程） ASR/ASA ：中断会话消息，AAA主动下发ASR，HSGW回复响应；（HSS发起终止会话） STR/STA ：会话终止消息，HSGW发起终止会话；；（HSS发起终止会话） RAR/RAA ：重认证授权，AAA主动下发；；（HSS中数据更新） AAR/AAA ：HSGW发起授权消息；；（HSS中数据更新）

5.3.1 重现认证 RAR/RAA

UIM支持STa接口的RAR/RAA消息

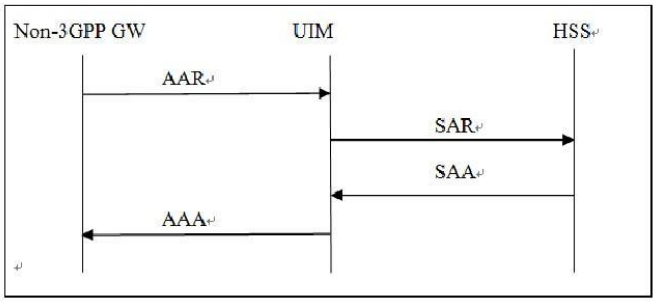
当HSS中的用户数据发生变化，给UIM下发了PPR后，UIM将会给Non-3GPP GW发送RAR通知其用户数据发生了变更，或者UIM根据本地策略周期性下发RAR通知Non-3GPP GW到UIM来重新下载用户数据或者鉴权



5.3.2 AAR/AAA

UIM支持STa接口的AAR/AAA

当HSS中的用户数据发生变化，给UIM下发了PPR后，UIM将会给Non-3GPP GW发送RAR通知其用户数据发生了变更，Non-3GPP GW将会给UIM发送AAR获取用户数据，UIM通过AAA响应将数据下发给Non-3GPP GW。

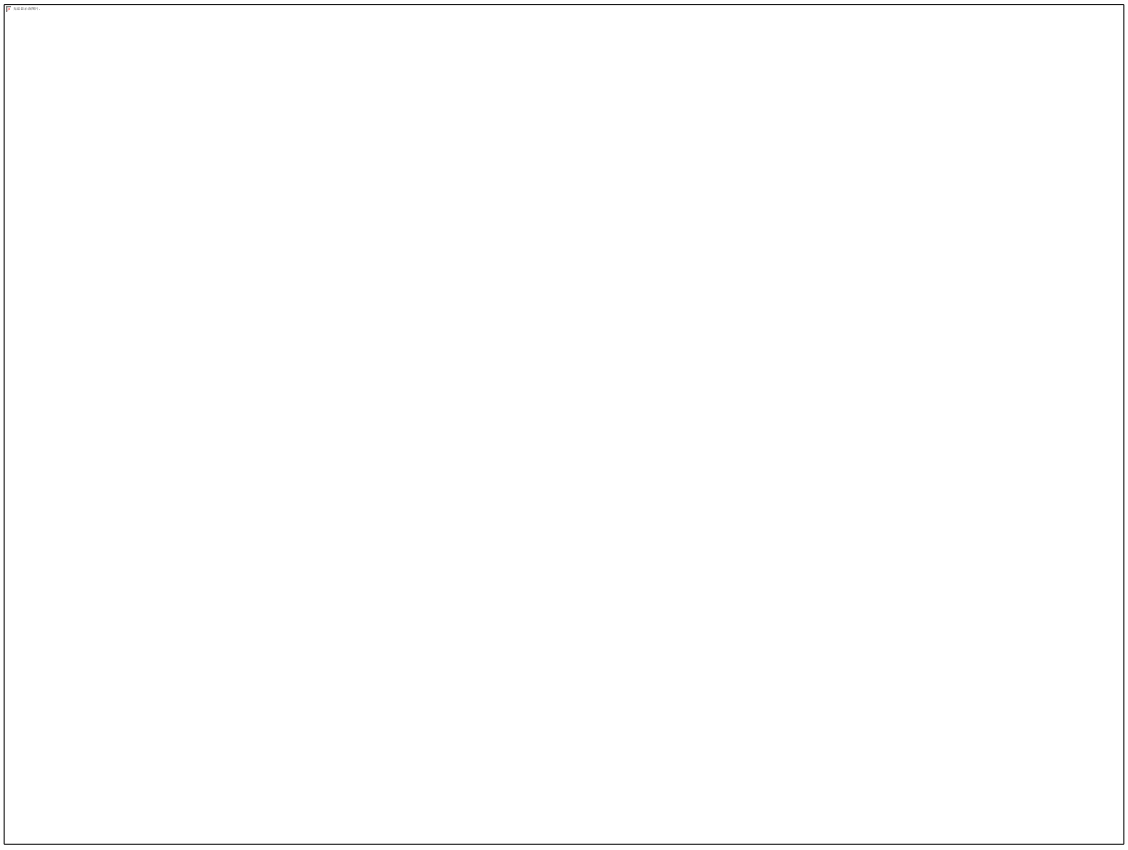


5.4 S6b 接口

关键业务流程（S6b接口）

功能	消息
S6b接口为PGW和AAA之间接口，认证完成后PGW用于更新PGW地址到HSS。	ASR/ASA ： 中断会话消息，AAA主动发起； STR/STA ： 会话终止消息，PDN GW发起终止会话；（终端发起去附着） RAR/RAA ： 重认证授权，AAA主动下发；（HSS中数据更新） AAR/AAA ： 授权消息，从HSS获取用户数据；；（建立PDP连接、HSS中数据更新）

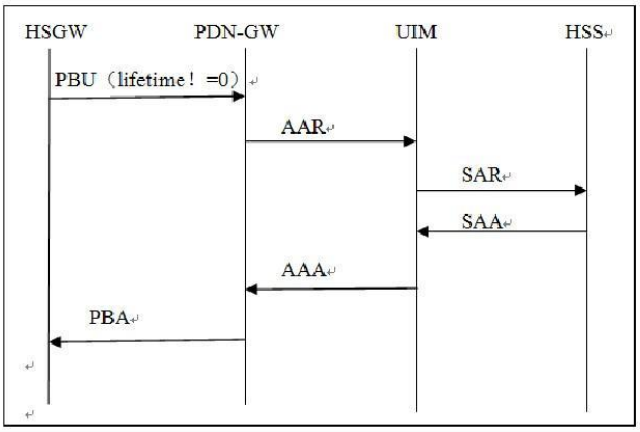
5.4.1 ? ? ?



5.4.2 AAR/AAA

UIM支持S6b接口的AAR/AAA消息

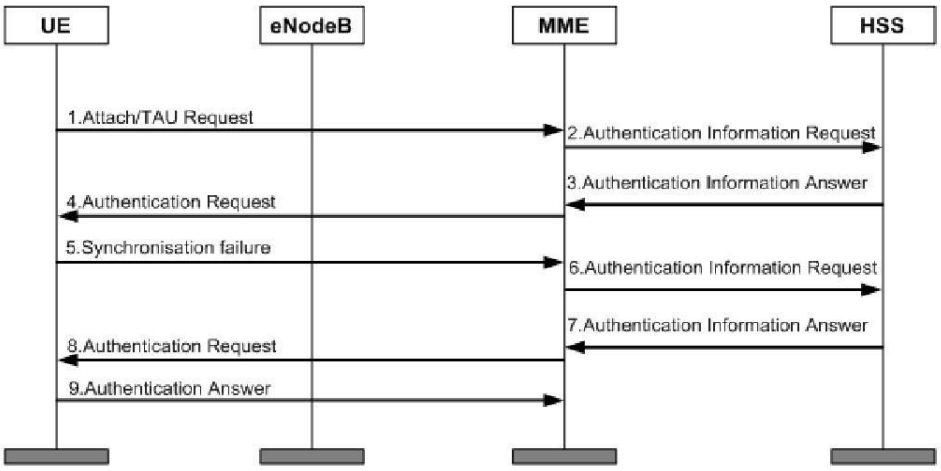
STa接口使用于PDN-GW和AAA Server（UIM）之间，S6b接口的AAR/AAA消息主要用于从UIM中获取用户数据，以及通过UIM向HSS更新PDN-GW的地址。



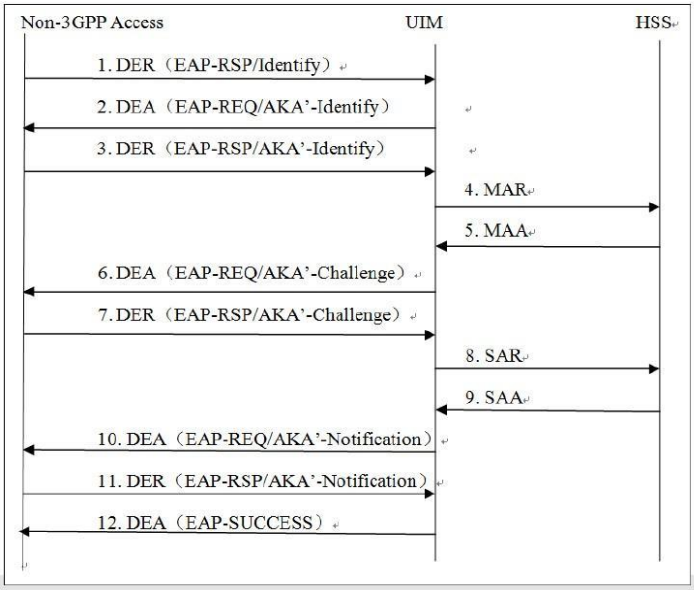
六 关键流程过程

6.1 EPS-AKA 鉴权（EPS 鉴权）

EPS-AKA鉴权（EPS鉴权）



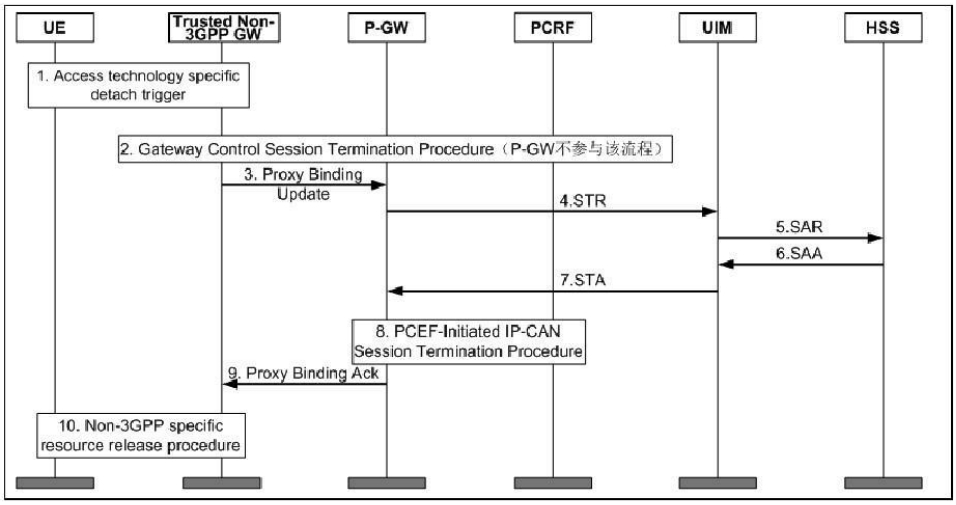
关键业务流程（鉴权认证过程）



采用EAP-AKA'鉴权认证方式。
在认证过程中AAA通过该流程从HSS获取用户的鉴权元组信息和用户数据并下发给HSGW。
UE和HSGW通过EAP消息交互，HSGW与AAA通过DIAMETER消息交互。
UE发送EAP消息到HSGW后，HSGW将EAP消息封装在DER消息的EAP-Payload信元中发送给AAA。
反之，AAA发送DEA消息到HSGW，HSGW从DEA消息的EAP-Payload信元中获取EAP消息，发送给UE。

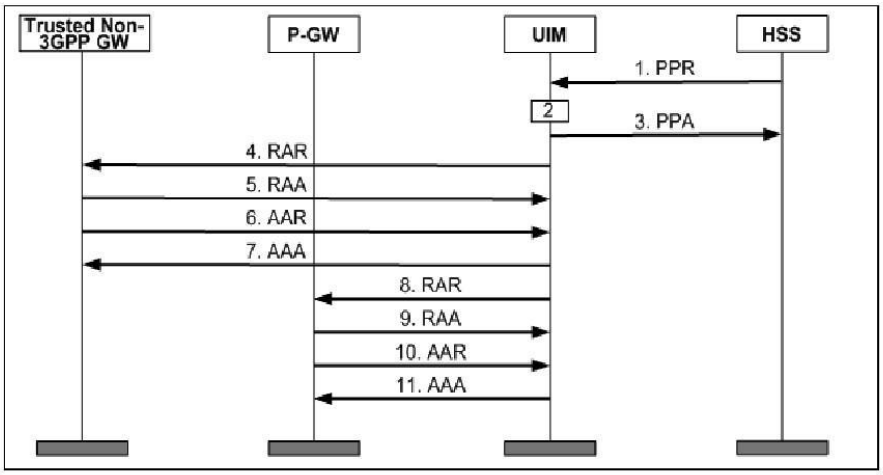
6.2 UE attach

关键业务流程（终端发起去附着）



6.3 HSS 触发用户数据更新

关键业务流程（HSS触发用户数据更新）



谢谢

www.huawei.com