

国际电信联盟

ITU-T

国际电信联盟
电信标准化部门

Y.2014

(03/2010)

Y系列：全球信息基础设施、
互联网协议问题、下一代网络、物联网和智慧城市
下一代网络 – 框架和功能结构模型

下一代网络的网络附加控制功能

ITU-T Y.2014 建议书

ITU-T



ITU-T Y系列建议书

全球信息基础设施、互联网协议问题、下一代网络、物联网和智慧城市

全球信息基础设施	
概要	Y.100–Y.199
业务、应用和中间件	Y.200–Y.299
网络方面	Y.300–Y.399
接口和协议	Y.400–Y.499
编号、寻址和命名	Y.500–Y.599
运营、管理和维护	Y.600–Y.699
安全	Y.700–Y.799
性能	Y.800–Y.899
互联网的协议问题	
概要	Y.1000–Y.1099
业务和应用	Y.1100–Y.1199
体系、接入、网络能力和资源管理	Y.1200–Y.1299
传输	Y.1300–Y.1399
互通	Y.1400–Y.1499
服务质量和网络性能	Y.1500–Y.1599
信令	Y.1600–Y.1699
运营、管理和维护	Y.1700–Y.1799
计费	Y.1800–Y.1899
通过NGN提供IPTV	Y.1900–Y.1999
下一代网络	
框架和功能体系模型	Y.2000–Y.2099
服务质量和性能	Y.2100–Y.2199
业务方面：业务能力和业务体系	Y.2200–Y.2249
业务方面：NGN中业务和网络的互操作性	Y.2250–Y.2299
编号、命名和寻址	Y.2300–Y.2399
网络管理	Y.2400–Y.2499
网络控制体系和协议	Y.2500–Y.2599
基于分组的网络	Y.2600–Y.2699
安全	Y.2700–Y.2799
通用移动性	Y.2800–Y.2899
运营商开放环境	Y.2900–Y.2999
未来网络	Y.3000–Y.3499
云计算	Y.3500–Y.3999

欲进一步了解详细信息，请查阅ITU-T建议书清单。

ITU-T Y.2014 建议书

下一代网络的网络附加控制功能

摘要

ITU-T Y.2014建议书阐述了下一代网络功能结构的网络附加控制功能（NACF），并确认了与NACF相关的接入场景。

此版本特别纳入了ITU-T Y.2014 (2008)建议书的扩展，分别探讨与支持IPTV业务和移动业务相关的组播和移动性问题。

历史沿革

版本	建议书	批准日期	研究组
1.0	ITU-T Y.2014	2008-05-07	13
2.0	ITU-T Y.2014	2010-03-16	13

关键词

功能结构，网络附加，下一代网络（NGN）

前言

国际电信联盟（ITU）是从事电信和信息通信技术（ICT）领域工作的联合国专门机构。ITU-T（国际电信联盟电信标准化部门）是国际电信联盟的常设机构，负责研究技术、操作和资费问题，并且为在世界范围内实现电信标准化，发表有关上述研究项目的建议书。

每四年一届的世界电信标准化全会（WTSA）确定ITU-T各研究组的研究课题，再由各研究组制定有关这些课题的建议书。

WTSA第1号决议规定了批准建议书须遵循的程序。

属ITU-T研究范围的某些信息技术领域的必要标准，是与国际标准化组织（ISO）和国际电工技术委员会（IEC）合作制定的。

注

本建议书为简明扼要起见而使用的“主管部门”一词，既指电信主管部门，又指经认可的运营机构。

遵守本建议书的规定是以自愿为基础的，但建议书可能包含某些强制性条款（以确保例如互操作性或适用性等），只有满足所有强制性条款的规定，才能达到遵守建议书的目的。“应该”或“必须”等其它一些强制性用语及其否定形式被用于表达特定要求。使用此类用语不表示要求任何一方遵守本建议书。

知识产权

国际电联提请注意：本建议书的应用或实施可能涉及使用已申报的知识产权。国际电联对无论是其成员还是建议书制定程序之外的其它机构提出的有关已申报的知识产权的证据、有效性或适用性不表示意见。

至本建议书批准之日止，国际电联尚未收到实施本建议书可能需要的受专利保护的知识产权的通知。但需要提醒实施者注意的是，这可能并非最新信息，因此特大力提倡他们通过下列网址查询电信标准化局（TSB）的专利数据库：<http://www.itu.int/ITU-T/ipr/>。

© 国际电联 2021

版权所有。未经国际电联事先书面许可，不得以任何手段复制本出版物的任何部分。

目录

页码

1	范围	1
2	参考文献	1
3	定义	2
3.1	其他地方定义的术语	2
3.2	本建议书定义的术语	2
4	缩略语和首字母缩略词	2
5	惯例	4
6	一般描述	4
6.1	高级功能概述	4
6.2	NACF的高层概念	5
6.3	移动性, 游牧性	5
6.4	接入网级别注册	6
7	功能架构	7
7.1	概述	7
7.2	功能实体	8
8	参考点	16
8.1	内部NACF参考点	16
8.2	NACF与资源和接纳控制功能(RACF)之间的参考点	30
8.3	NACF和服务控制功能之间的参考点	30
8.4	NACF和CPE之间的参考点	33
8.5	NACF与移动管理和控制功能 (MMCF) 之间的参考点	34
9	安全考虑	35
附录I	– 到网络角色的映射	36
附录II	– 信息流	39
II.1	高级信息流	39
II.2	基于PPP的认证	40
II.3	DHCP模式	41
附录III	– 物理配置	42
III.1	PPP 案例	42
III.2	包含DHCP配置的PPP	43
III.3	DHCP (选项1)	43
III.4	DHCP (选项2)	44

III.5 基于PANA的配置	44
附录IV – ITU-T Y.2014建议书和ETSI ES 282 004 v2.0.0之间的整体映射	46
参考文献.....	47

下一代网络的网络附加控制功能

1 范围

本建议书阐述了[ITU-T Y.2012]定义的下一代网络（NGN）的网络附加控制功能（NACF）组件，并确认了与NAC相关的接入场景。

本建议书纳入了与其他NGN组件（RACF、MMCF和SCF）的参考点，为固定、游牧和移动终端/用户提供网络附加功能。

2 参考文献

下列ITU-T建议书和其它参考文献的条款，因在本建议书中的引用而构成本建议书的条款。在出版时，所指出的版本是有效的。所有的建议书和其它参考文献均可能被修订，本建议书的使用者应查证是否有可能使用下列建议书或其它参考文献的最新版本。当前有效的ITU-T建议书清单定期出版。本建议书引用的文件自成一体时不具备建议书的地位。

- [ITU-T Q.1761] ITU-T Q.1761 (2004)建议书，固定和现有IMT-2000系统的融合原则和要求
- [ITU-T X.800] ITU-T X.800 (1991)建议书，CCITT应用的开放系统互连（OSI）安全体系结构
- [ITU-T Y.1541] ITU-T Y.1541 (2006)建议书，基于IP业务的网络性能目标
- [ITU-T Y.1910] ITU-T Y.1910 (2008) 建议书，IPTV功能架构
- [ITU-T Y.2012] ITU-T Y.2012 (2006) 建议书，下一代网络的功能要求和架构第1版
- [ITU-T Y.2018] ITU-T Y.2018 (2009) 建议书，NGN传输层中的移动性管理和控制框架与架构
- [ITU-T Y.2021] ITU-T Y.2021 (2006) 建议书，用于下一代网络的IMS
- [ITU-T Y.2111] ITU-T Y.2111 (2008) 建议书，下一代网络资源和允许控制功能
- [ITU-T Y.2701] ITU-T Y.2701 (2007) 建议书，下一代网络（NGN）的安全性要求第1版
- [ITU-T Y.2702] ITU-T Y.2702 (2008) 建议书，下一代网络（NGN）的认证和授权要求第1版

3 定义

3.1 其他地方定义的术语

本建议书使用以下其他地方定义的术语：

3.1.1 授权[ITU-T X.800]：权限的授予，包括基于访问权限的访问许可。

注 – 在一些情况下（比如紧急呼叫服务），无需认证或身份识别即可给予授权。

3.1.2 游牧性[ITU-T Q.1761]：用户在移动后改变网络接入点的能力；当改变网络接入点时，用户的服务会话完全停止，然后重新开始，即，不可能产生切换。一般认为的正常使用模式是用户在移动至另一个接入点或更换终端之前关闭服务会话。这是固移融合情况下所指的移动性。

3.2 本建议书定义的术语

本建议书定义了如下术语：

3.2.1 认证：一种特性，通过该特性可为实体或一方创建带有所需保证的正确标识符。被认证方可以是用户、客户、本地环境或服务网络。

3.2.2 用户驻地设备（CPE）：使用户可以接入 NGN 提供的服务的一台或多台设备。

注 – 包括通常称为家庭网关(HGW)或终端(TE)等的用户控制设备，但不包括网络控制实体，例如接入网关等。

3.2.3 显式认证：要求被认证的一方执行一个认证过程（以验证该方声称的身份）的认证。

3.2.4 家庭网关（HGW）：用户驻地设备（CPN）和接入网之间的网关。

注 – 家庭网关可采用最简单的形式（桥接或路由调制解调器）以及更高级的形式（集成接入设备）。

3.2.5 隐式认证：基于双方已建立的信任关系或双方创建的认证程序的一个或多个输出成果的认证。

3.2.6 线路识别：基于信任配置创建线路标识符的过程。

4 缩略语和首字母缩略词

本建议书使用以下缩略语和首字母缩略词：

AAA	认证、授权和计费
ABG-FE	接入边界网关功能实体
ACL	接入控制列表
AM-FE	接入管理功能实体
AN	接入网
AN-FE	接入节点管理
API	应用编程接口

AR-FE	接入中继功能实体
ATM	异步传输模式
CoS	业务类别
CPE	客户驻地设备
CPN	客户驻地网
DHCP	动态主机配置协议
DNS	域名服务器
EAP	可扩展验证协议
EN-FE	边缘节点功能实体
FQDN	完全限定域名
FTP	文件传输协议
GTP	GPRS 隧道协议
HDC-FE	切换决策和控制功能实体
HGW	家庭网关
HGWC-FE	家庭网关配置功能实体
HTTP	超文本传输协议
ID	标识符
IMS	IP 多媒体子系统
IP	互联网协议
IPTV	互连网协议电视
MAC	媒体接入控制
MIP	移动互联网协议
MLM-FE	移动位置管理功能实体
MLM-FE(P)	执行代理移动位置管理角色的MLM-FE实例
MMCF	移动性管理和控制功能
MPLS	多协议标签交换
NACF	网络附加控制功能
NAC-FE	网络接入配置功能
NGN	下一代网络
NID-FE	网络信息分发功能实体
PAA	PANA 认证代理
PaC	PANA 客户端
PANA	网络接入认证信息承载协议
P-CSCF	代理呼叫会话控制功能

PD-FE	决策功能实体
PE-FE	策略执行功能实体
PIA	永久IP地址
PPP	点到点协议
QoS	服务质量
RACF	资源和接纳控制功能
SADS	服务和应用发现与选择
SCF	服务控制功能
SLA	服务水平协议
SUP-FE	服务用户配置文件功能实体
TAA-FE	传输认证和授权功能实体
TE	终端设备
TFTP	简单文件传输协议
TIA	临时IP地址
TLM-FE	传输位置管理功能实体
TUP-FE	传输用户配置文件功能实体
VC	虚拟信道
VCI	虚拟信道标识符
VPI	虚拟路径标识符
VPN	虚拟专用网络
WLAN	无线局域网

5 惯例

本建议书未使用特定惯例。

6 一般描述

6.1 高级功能概述

NACF提供以下功能：

- 动态配置IP地址和其他CPE配置参数。
- 经用户许可，自动发现CPE功能和其他参数。
- 在IP层（可能还有其他层）对终端用户和网络进行认证。认证时，终端用户和网络附件之间相互认证。
- 基于用户配置文件的网络接入授权。
- 基于用户配置文件的接入网配置。
- IP层位置管理。

上文提到的用户配置文件仅与传输接入网订阅有关，在本建议书的其余部分被称为“传输订阅配置文件”。

组件在整个NGN架构中的位置见[ITU-T Y.2012]，图1供参考。

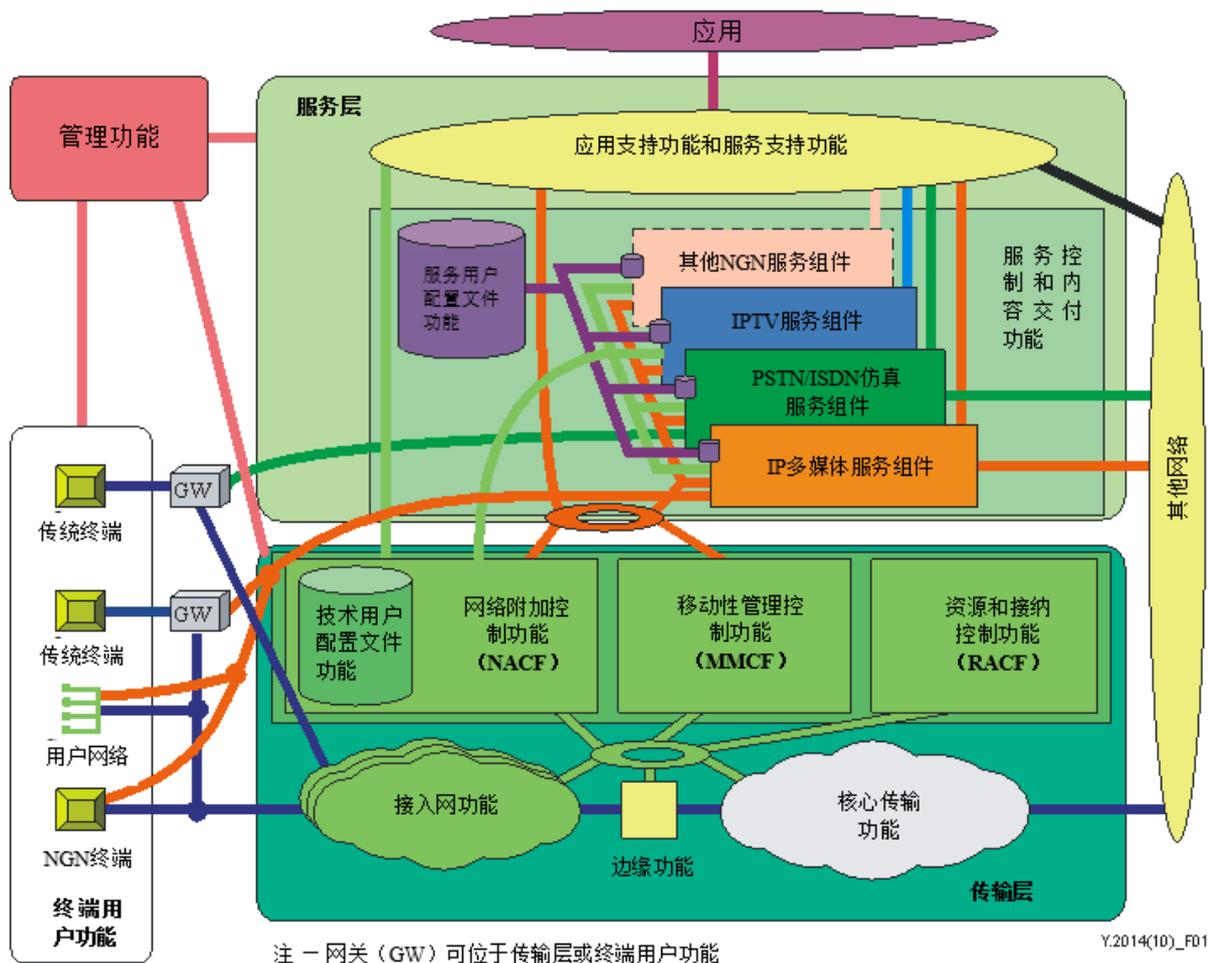


图1 - 包括NACF在内的NGN组件

6.2 NACF的高层概念

NACF为接入NGN服务提供了访问级别注册和CPE初始化。NACF提供网络级识别和认证，管理接入网IP地址空间，并对访问会话进行认证。NACF还向CPE宣布NGN服务层组件的联络点。

通过NACF控制的网络附件以NACF存储的隐式或显式用户识别和认证为基础。

6.3 移动性，游牧性

在本建议书中，NACF提供的移动性管理功能仅限于一个终端移动到不同接入点和接入网（可能为不同接入网提供商所有）的能力，以及用户使用不同终端设备、接入点和接入网来检索NGN服务（甚至是来自其他网络运营商的服务）的能力。

在本建议书中，移动性包括对接入网之间的切换和会话持续性的支持，以及游牧性，不排除使用接入网内提供的移动能力。

NACF架构不承担任何业务角色。然而，为应对游牧性、漫游以及移动性要求，NACF结构可被映射到固定宽带接入环境中的各种功能网络角色上。附录I描述了游牧性、漫游以及移动性要求的影响。

6.4 接入网级别注册

NACF注册涉及CPE和NACF之间的确认、认证和授权过程，从而控制对NACF的访问。为NACF定义了两种类型的认证：隐式认证，比如基于线路识别的认证；显式认证，例如基于EAP [b-IETF RFC 3748]的认证。NACF必须知道用于认证的标识符和凭证之间的关系，从而使认证解决方案成为可能。

显式认证是在CPE和NACF之间操作，要求在CPE和NACF之间执行一个信令发送程序。隐式认证可由NACF根据到CPE的连接的线路识别来执行。采用哪种形式的身份验证取决于运营商策略。

隐式和显式的认证均可独立用于NACF认证机制。

6.4.1 隐式认证

取决于接入网配置，尤其是有线宽带接入网配置，隐式接入认证可仅依靠通过物理或逻辑标识的第2层(L2)传输层的隐式认证进行。CPE可直接接入网络，不需要显式认证过程。

采用哪种隐式认证方式取决于运营商策略。

6.4.1.1 线路识别

线路识别是一种隐式认证方式。线路识别确保接入线路获得认证，并可从家庭网关接入(HGW)。线路识别依靠HGW和接入网之间的L2连接的激活。

线路认证确保接入线路获得认证，并可从HGW接入。线路ID用于线路认证。是否采用线路认证取决于运营商的政策。

6.4.2 显式认证

若HGW为路由调制解调器而用户驻地网(CPN)为专用IP域，则由HGW发起认证。若HGW为桥接，当接入网(AN)已知CPN中的IP域时，每个TE都对NACF进行认证。

为实现显式认证解决方案，NACF必须知道用于认证的标识符和凭证之间的关系。用于显式认证的标识符取决于采用的认证机制和CPE所连接的接入网。两个标识符示例如下：

- 用户标识符和凭证。
- CPE标识符。

使用的显式认证机制类型取决于接入网配置和运营商策略。

6.4.3 HGW远程网络配置

HGW接入NGN业务层组件初始化时，需要执行此流程。

6.4.4 NGN服务层组件发现

作为网络注册流程的组成部分，NACF需要具备向CPE宣布NGN服务层组件的联络信息的能力。若NGN服务层组件为IMS服务组件[ITU-T Y.2021]，则NACF提供的联系信息识别的是P-CSCF。另一方面，若使用IPTV服务组件[ITU-T Y.1910]，则NACF提供的联系信息识别的是服务和应用发现和选择(SADS)功能块。

NACF提供的联系信息，采取联络点IP地址或联络点完全限定域名(FQDN)的形式。在后一种情况下，NACF提供了能够将该FQDN解析为联络点IP地址的DNS服务器的IP地址。

或者，到NGN服务层组件的联络点可在CPE中静态配置，例如使用完全限定域名和DNS解析来检索联络点的IP地址。该选项在非漫游情况下适用。

7 功能架构

7.1 概述

图2描述了NACF功能架构，包含功能实体和相关参考点。未显示充电功能的参考点。

附录II描述了与网路附件相关的信息流，附录III描述了功能NACF架构适用的可能的物理配置。

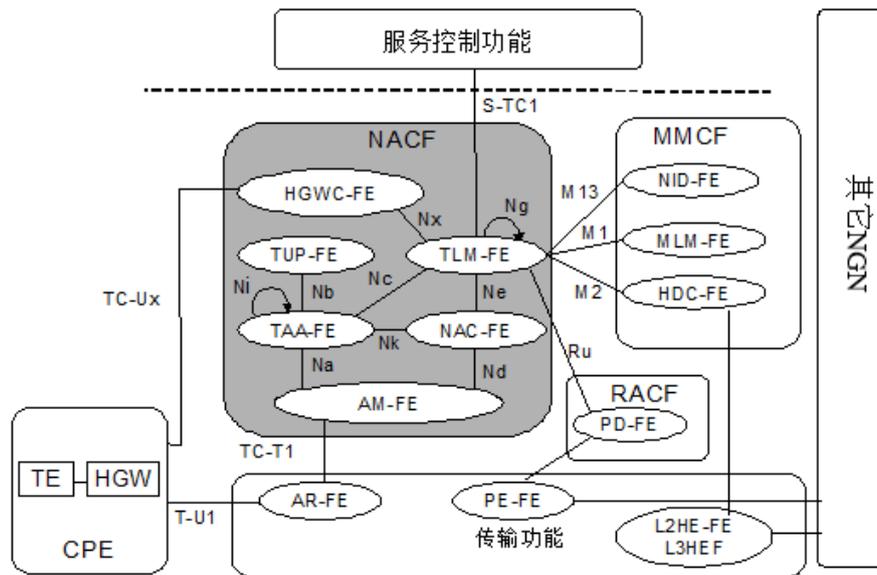


图 2 – NACF功能结构

NACF由以下功能实体构成：

- 网络接入控制功能实体（NAC-FE）
- 接入管理功能实体（AM-FE）
- 传输位置管理功能实体（TLM-FE）
- 传输认证和授权功能实体（TAA-FE）
- 传输用户配置文件功能实体（TUP-FE）
- 家庭网关配置功能实体（HGWC-FE）

NACF与下列NGN组件和实体互动：

- S-TC1参考点的服务控制功能（SCF）（例如，IMS服务组件[ITU-T Y.2021]的SCF），用于导出访问会话信息；
- Ru参考点的资源和接纳控制功能（RACF）[ITU-T Y.2111]，用于导出传输订阅配置文件信息；
- M1、M2和M13参考点的移动性管理控制功能(MMCF) [ITU-T Y.2018]，用于导出关于移动性管理的若干类型的信息；
- 充当到/从CPE的中继的传输功能（即，访问中继功能实体(AR-FE) [ITU-T Y.2012]），用于地址分配、认证和授权（TC-T1和T-U1参考点）；
- TC-Ux参考点的用户驻地设备（CPE），用于配置。

一个或多个功能实体可以映射到单个物理实体。如果一个功能实体由两个物理实体实施，这些物理实体之间的接口不在标准化的范围之内。

图2未展示管理域。NACF中的功能实体可在两个管理域之间分配。附录I描述了游牧性和漫游对NACF分布的影响，即，访问NGN与家庭NGN接入网之间的NACF分配。注意，NACF和RACF之间的Ru参考点[ITU-T Y.2111]，以及NACF和MMCF之间的M1、M和M13参考点[ITU-T Y.2018]为域内参考点。

NGN架构不要求单独的NACF实例来支持多接入网络。但这并不妨碍运营商部署多接入网络常见的NACF功能（例如，不同接入网共用一个用户配置文件数据库）。

7.2 功能实体

7.2.1 网络接入配置功能实体（NAC-FE）

NAC-FE负责到CPE的IP地址分配。它还可以分配其他网络配置参数，如DNS服务器地址、特定服务层组件的信令代理地址（例如，P-CSCF和SADS分别接入IMS服务组件[ITU-T Y.2021]和IPTV服务组件[ITU-T Y.1910]时的地址）。

NAC-FE应能够提供CPE接入网络信息。该信息唯一标识CPE所连接的接入网。CPE可发送该信息至SCF，作为定位TLM-FE的线索。

SCF基于CPE的IP地址或/和基于SCF从其接收IP分组的接入网的信息来定位TLM-FE（例如，P-CSCF-FE可能有面向不同接入网的多个逻辑/物理接口）。SCF通过参考点S-TC1向TLM-FE执行一个“位置信息查询”。该查询的密钥是CPE使用的IP地址。

NAC-FE可对TE定位两种IP地址：永久IP地址（PIA）和临时IP地址（TIA），以支持移动性。永久IP地址一旦被指配给TE，在TE移动期间就不会发生变化。然而，应注意，在某些情况下，可能会向同一个TE分配不同的永久IP地址，例如，当TE被重启时。MIP [b-IETF RFC 3220]的家庭地址就是永久IP的一个示例。另一方面，每当TE移动到一个新的子网中，就会为TE指配一个不同的临时IP地址。MIP的转交地址就是临时IP地址的一个示例。如果在认证过程中需要指配一个地址的话，NAC-FE可使用相关的TAA-FE来分配IP地址。

注1 – 到CPE的接入网标识符的传输由到现有协议的扩展（例如，新的DHCP选项，或使用DHCP选项120 [b-IETF RFC 2131]）决定。

注2 – DHCP服务器或RADIUS服务器是典型的NAC-FE实现。

7.2.2 接入管理功能实体（AM-FE）

AM-FE终止CPE和NACF之间第2层连接，以注册和初始化CPE。第2层连接可被用于监测网络层的网络附件。在这种情况下，CPE和AM-FE之间的第2层连接为跨异构网络环境的上层实体构建统一框架，便于发现和选择地理区域内存在的多种类型的接入网。重要的是，要注意CPE和AM-FE之间的每一个通信关系都并非意味着一个特定的传输机制。

基于这一连接，AM-FE可收集关于链路标识符、链路参数、TE位置、主机配置参数等接入网信息。主机配置信息还可包括先前分配的已认证数据和位置管理 – 其传输订阅配置文件信息已在之前的接入网中提供。在更大的范围内，接入网信息的目标是帮助较高层级的移动性管理功能，以获取异构网络的全局视图，从而实现跨这些网络的游牧性。

AM-FE将CPE发出的网络访问请求转换为可被NACF理解的格式。它根据请求类型，向/从TAA-FE和NAC-FE转发分配IP地址和可能的附加网络配置参数的请求。AM-FE将请求转发至TAA-FE，对用户进行认证、授权，或拒绝网络访问，并检索用户特定访问配置参数]。AM-FE还可向转发的请求增加链路层参数和主机配置参数。

接入网信息可在NAC-FE和TAA-FE的网络发现/注册中提供帮助。CPE和AM-FE均可对移动性管理的连接做出决策，并重复使用网络注册/认证数据，以快速恢复，无须重复执行注册/认证/配置的整个过程。CPE可进一步使用网络信息，在CPE中执行移动性管理流程。

注1 – 在采用PPP [b-IETF RFC 1661]的情况下，AM-FE终止了PPP连接，并提供与NACF参考点的互通，例如，使用AAA协议（RADIUS [b-IETF RFC 2865]或Diameter [b-IETF RFC 3588]）。如果TAA-FE在一个RADIUS服务器中执行，则AM-FE用作RADIUS客户端（AM-FE终止PPP，并将其转换为Na参考点上的一个信令信息）。

注2 – 如采用IEEE 802.1X [b-IEEE 802.1X]/PANA [b-IETF RFC 4058]，线路识别可采用隐式执行。隐式认证可仅使用通过第2层传输层的物理或逻辑标识的到CPE的访问线路。

注3 – 若连接了一个移动接入网（例如3GPP接入[b-3GPP TS 23.401], [b-3GPP TS 23.402]），认证可在转换AM-FE中的网络接入请求后执行。详细信息正在研究中。

7.2.3 传输位置管理功能实体（TLM-FE）

TLM-FE注册分配给CPE的IP地址与NAC-FE提供的相关网络位置信息（例如接入传输设备特性、逻辑连接识别符、边缘PE-FE设备身份验证等）之间的关联。TLM-FE注册从NAC-FE处接收到的传输位置信息与地理位置信息之间的关联。TLM-FE还可存储已被分配IP地址的用户/CPE的标识符（从TAA-FE接收到的信息），以及传输订阅配置文件信息和关于位置信息的隐私偏好。若TLM-FE不存储用户/CPE的标识符/配置文件，则要求TLM-FE能够从TAA-FE检索这一信息。详细的TAA-FE信息模式见第7.2.3.1段。

为支持位置查询的层次结构，TLM-FE可扮演多个角色，即，家庭角色、本地角色，或二者兼有。在扮演家庭角色时，TLM-FE存储一个指针，指向为附件扮演本地角色的TLM-FE实例。存取域中的用户/CPE的当前位置信息存储并绑定在本地TLM-FE中。因此，当用户/CPE在同一存取域中移动时，只有本地TLM-FE的位置绑定信息需要更新，而家庭TLM-FE的位置绑定信息不需要更新。

TLM-FE对来自业务控制功能的位置查询做出响应。当这些功能之一（例如P-CSCF）需要查询终端设备的本地信息时，它将首先询问家庭TLM-FE。家庭TLM-FE随后根据终端设备所属的本地TLM-FE的索引，向本地TLM-FE查询其所附加的网络中的终端设备的详细位置信息。TLM-FE交付的实际信息可能采取多种形式（例如，网络位置、地理坐标、邮政地址等），取决于与请求程序的协议和用户对于其位置隐私的偏好。

另一方面，为支持游牧性/漫游，家庭网络的SCF接入访问网络中的TLM-FE，通过家庭网络中的TLM-FE-proxy获取位置信息，如图I.5所示。

此外，为支持移动性，本地TLM-FE之间的互动在Ng参考点上进行。

注1 – TLM-FE从相关用户网络位置特征中检索地理信息在本建议书的范围之外。

注2 – 地理信息的形式多种多样，取决于访问类型和应用。

TLM-FE确认TE的当前网络位置，并对其移动进行追踪。当TE在网络中的连接点发生变化时，TLM-FE更新分配给TE的IP地址与相关网络位置信息的关联。同时，更新网络位置信息和地理位置信息之间的关联。

当TE被附加到一个新接入网，并被分配了一个新的临时IP地址，且位置信息存储在新TLM-FE中时，旧TLM-FE可向新TLM-FE传输相关的上下文信息。这些信息包括QoS配置文件、用户偏好等。与此同时，新TLM-FE可向更新的绑定信息的服务控制功能发出通知。

可向TLM-FE告知接入控制列表（ACL）。ACL由服务控制功能和/或者管理实体基于TUP-FE中的用户配置文件生成。用户是否订阅某个组播群组就是用户配置文件的一个例

子。ACL可由数据包源地址、目的地地址或上层协议和端口号构成。TLM-FE告知PD-FE要下载至AN-FE、EN-FE和ABG-FE的ACL。

AN-FE、EN-FE和ABG-FE根据PD-FE提供的ACL来决定是否转发或屏蔽每个包。若用户想要加入一个组播群组，则AN-FE、EN-FE或ABG-FE转发或/和处理该请求。如果不批准，该请求被丢弃，此服务请求以失败告终。

7.2.3.1 信息模型

TLM-FE保存了大量表示活跃的访问会话的记录。这些记录包含从NAC-FE和TAA-FE接收到的信息、关于已订阅特定事件和其他静态配置数据的SCF列表的信息。表1标识了会为每个访问会话存储哪些信息元素。

注 – 在使用PPP [b-IETF RFC 1661]的情况下，可提供从TAA-FE到TLM-FE的物理连接标识符。

表 1 – TLM-FE信息模型

访问会话描述	
从NAC-FE收到的信息组件	
全局唯一IP地址信息	一组IP地址信息，用于定位CPE所附的接入网。
– 唯一IP地址	用于识别所附CPE的IP地址。
– 地址域	IP地址的寻址域（例如，子网前缀或VPN ID）。
物理连接标识符（可选）	CPE附加的接入传输网络的物理连接的本地标识符（例如PE-FE设备的IP地址、MAC地址或链路ID和物理端口）。
逻辑连接标识符	CPE所连接的接入传输网的逻辑连接的本地标识符（例如，ATM VPI/VCI、PPP、MPLS 标签、GTP隧道和逻辑端口）。可被用于定位第2层连接和特定附加CPE的相关网络设备。
CPE类型	已分配IP地址的CPE类型。
从TAA-FE/TUP-FE接收的信息	
传输订阅用户标识符	附加的CPE的全局唯一标识符。本标识符可用于为CPE定位传输订阅信息。
本地连接标识符	CPE所连接的接入传输网的逻辑连接的本地标识符（例如，ATM VPI/VCI、PPP、MPLS标签、GTP隧道和逻辑端口）。
移动服务参数（可选）（注8）	
– MLM-FE(C)地址（注9）	包含移动地址绑定信息的MLM-FE实例的地址。
– MLM-FE(P)地址（注9）	发送位置注册的MLM-FE实例的地址
从TAA-FE/TUP-FE收到的信息	
– 建钥资料（注9）	用于UE和MMCF之间的安全关联的资料。
– 移动协议类型	TE或CPE可支持的移动协议类型，例如基于主机或基于网络的移动性。
– 锚点地址（可选）	.UE角度的上层隧道端点地址。
– 隧道端点地址（可选）（注10）	作为UE代理的网络节点的隧穿端点地址（下层隧道端点）。

表 1 – TLM-FE信息模型

访问会话描述	
隐私指示器（注1）	表明位置信息是否可被导出至服务和应用。
传输资源订阅（注2和3）	
– 传输订阅配置文件ID（注4）	一组传输订阅配置文件信息的标识符。
– 传输订阅配置文件描述（注4）	
– 网络服务类别	表示CPE订阅的网络服务类别（例如，高级服务、金牌服务、银牌服务、常规服务等。可包括QoS性能类别（例如[ITU-T Y.1541]中定义的类别）。
– 订阅的上行带宽	CPE订阅的上行连接最大带宽。
– 订阅的下行带宽	CPE订阅的下行连接最大带宽。
– 优先级	任何预留请求允许的最大优先级。
– 请求程序名称	识别传输资源订阅允许的请求程序。
默认配置（可选）	
– 默认配置标识符（注5）	默认配置的标识符。
– 默认配置描述（注5）	
– 默认接入控制列表：获准目的地列表	默认允许直通的目标IP地址、端口、前缀和端口范围列表。（注6）
– 默认接入控制列表：被拒绝的目的地和组播流的列表	默认向其发送流量会被拒绝的目标IP地址、端口、前缀和端口范围列表。在组播的情况下，IP-组播列表地址列表和/或者必须拒绝向所附加的用户设备发送流量的（源IP地址、IP-组播组地址）对的列表。列表中的地址范围获得支持。
– 默认上行带宽	默认可用于上行连接的最大带宽。
– 默认下行带宽	默认可用于下行连接的最大带宽。
从物理连接标识符推导出的静态信息	
位置信息	
默认传输订阅用户标识符	
从逻辑连接标识符推导出的静态信息	
RACF联络点	要推送传输订阅配置文件的RACF元素的地址。
接入网类型	CPE所附的接入网类型。
附加接入域名	CPE所附接入网域名或提供商名称
事件管理信息	
事件管理信息（注7）	

表 1 – TLM-FE信息模型

访问会话描述	
– 事件	监测的事件类型
– SCF身份	本事件发生时需通知的SCF列表
<p>注1 – 根据应用的安全级别，指示应用是否可以访问位置信息。</p> <p>注2 – 访问会话可能包含对于多个传输来源订阅的描述。</p> <p>注3 – NACF并不知道实际可用的带宽。RACF可根据逻辑连接标识符推导出该信息。</p> <p>注4 – 可包含传输订阅配置文件ID或传输订阅配置文件描述，但不可同时包含二者。</p> <p>注5 – 可包含默认配置标识符或默认配置标识符描述，但不可同时包含二者。</p> <p>注6 – 如果这两个列表均不显示某一目的地，则这些地址的门设置由RACF控制决定。</p> <p>注7 – 可存储超过一个事件和相关的SCF身份识别。</p> <p>注8 – 仅在使用移动服务时可用。</p> <p>注9 – 仅在使用基于主机的移动时可用。</p> <p>注10 – 若隧道端点地址以静态方式提供，或者MLM-FE可使用自身机制获取该信息，则不需要该信息。仅在采用基于网络的移动时可用。</p>	

许多记录可包含相同的物理连接标识符和/或逻辑连接标识符和/或传输用户标识符，因为订阅用户可使用相同或不同的接入物理连接在相同或不同的接入逻辑连接（例如，ATM VC）上创建超过一个IP接入会话。TLM-FE不需要在此类记录之间创建任何链接 – 虽然可以为优化其存储能力而这么做。

7.2.3.2 TLM-FE状态模型

TLM-FE在管理访问记录时的行为可由本段描述的状态模型表示。状态模型并非为了限制TLM-FE的执行。执行可使用不同的模型，只要显示相同的外部行为即可。

本状态模型定义了一个由五种状态构成的会话状态机（SSM）：

- 空 (*Null*) :该状态表示访问记录不存在。
- *Wait_For_Bind_Indication_and_Profile*:当接收到一个事件（例如，登录事件）的订阅请求而创建访问记录时，如果关联的传输订阅用户标识符或全局唯一IP地址信息的会话记录不存在，则将进入此状态。会创建一个分记录，TLM-FE等待Bind_Indication事件。
- *Wait_For_Bind_Indication*:接收传输订阅配置文件信息创建了一个访问记录时，如果关联的传输订阅用户标识符或全局唯一IP地址信息会话记录不存在，则将进入此状态。会创建一个分记录，TLM-FE等待Bind_Indication事件。
- *Wait_For_Profile_Information*:此状态表示传输订阅配置文件信息的部分会话记录丢失。
- *Active_Session*:此状态表示访问会话的完整描述可用的会话记录。

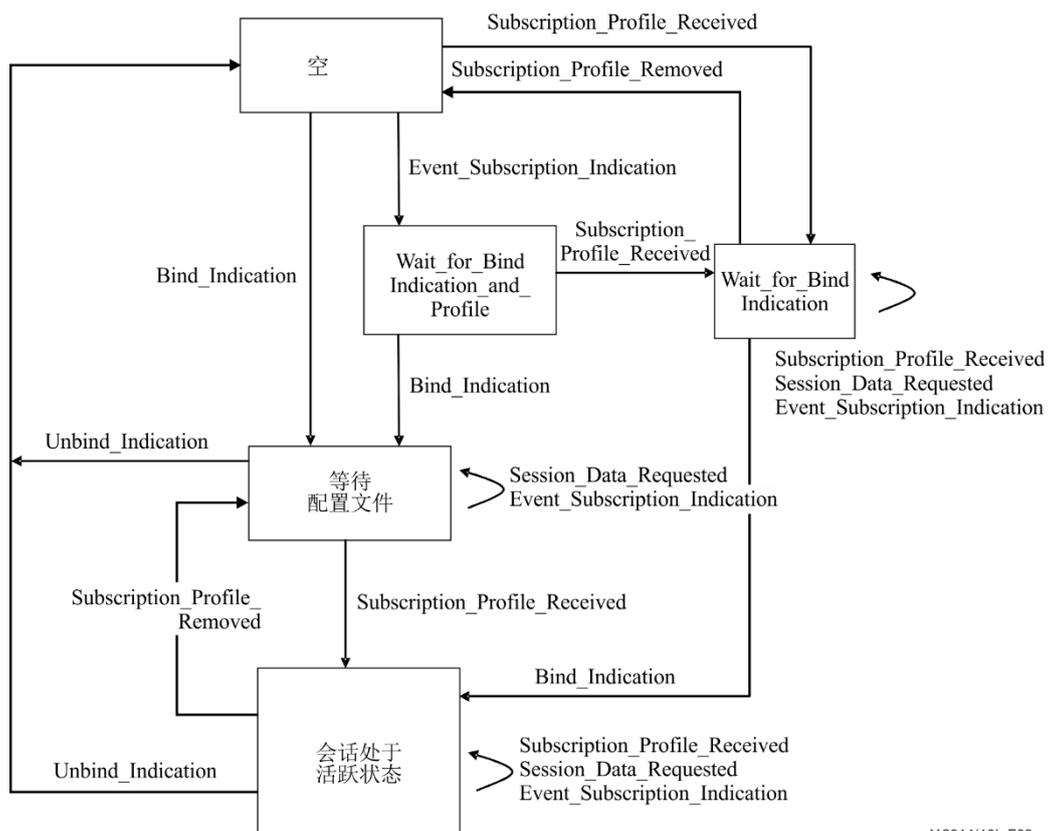
TLM-FE在S-TC1、Ru、Ne和Nc参考点发送和接收信息流。传入信息流将基于传输订阅用户标识符或它们包含的全局唯一IP地址信息路由到会话状态机（SSM）。

当出现指示未知传输订阅用户标识符或全局唯一IP地址信息的Bind_Indication或Event_Subscription_Indication事件时，将创建SSM实例。

以下事件由TLM-FE会话状态机处理，并导致状态之间的转换：

- **Event_Subscription_Indication:** 当从SCF接收到事件注册请求信息流(参见第8.3.1段)时，将发生此事件。
注 – 当实际TLM-FE事件发生时，通知事件请求信息流被发送回AF。这不会导致任何状态转换。
- **Bind_Indication:** 当Ne参考点收到绑定指示信息流（见第8.1.2段）时，将发生此事件。
- **Unbind_Indication:** 当Ne参考点接收到解绑指示信息流，或当进行绑定信息查询时收到否定确认（见第8.1.2段）时，将发生此事件。
- **Subscription_Profile_Received:** 当Nc参考点异步接收到传输资源信息指示信息流时，或者发送了传输资源信息请求信息流，或者当内部配置数据表明默认传输订阅用户配置文件适用时，将发生此事件。
- **Subscription_Profile_Removed:** 当Nc参考点接收到传输资源释放通知信息流时，将发生此事件。
- **Session_Data_Requested:** 当Ru参考点接收到传输资源信息请求信息流，或S-TC1参考点接收到信息查询请求信息流时，发生此事件。造成信息查询响应或传输资源信息指示信息流通过S-TC1或Ru参考点发送。

图3提供了基于上述事件的状态转换的概述。



Y.2014(10)_F03

图3 – 访问记录管理的TLM-FE状态模型

7.2.4 传输认证和授权功能实体 (TAA-FE)

TAA-FE根据传输订阅配置文件执行网络访问的用户认证以及授权检查。对于每个用户，TAA-FE从TUP-FE中包含的传输订阅配置文件信息中检索认证数据和访问授权信息。TAA-FE还可收集每个经NACF认证的用户的计费数据。

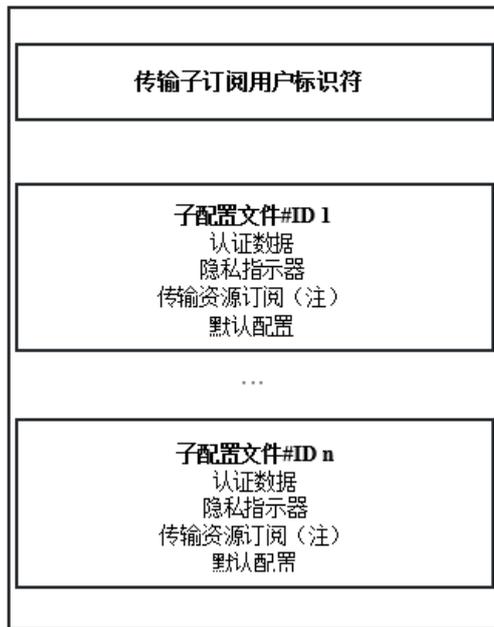
对于TE，TAA可支持IP地址或IP前缀的分配。在基于主机的移动性架构和基于网络的移动性架构的认证过程中，可分别要求分配IP地址和IP前缀。对于基于主机的移动性架构，TAA-FE可要求NAC-FE分配IP。对于基于主机的移动性架构和基于网络的移动性架构，TAA可仅使用作为用户配置文件信息保存在TUP-FE中的IP地址或IP前缀。为动态分配IP地址，TAA-FE可要求NAC-FE分配IP地址。在这种情况下，每次只要地址被请求，即使来自同一个TE，该IP地址也可能被更改。然而，为静态分配IP地址或IP前缀，TAA-FE可使用作为用户配置文件信息保存在TUP-FE中的IP地址或IP前缀。

TAA-FE还可被用作代理。当作为代理时，TAA-FE可定位作为服务器、保存有TUP-FE订阅认证数据的TAA-FE，并与之通信。TAA-FE代理可向作为服务器的TAA-FE转发从AM-FE接收的访问和授权请求，以及计费信息。接收到的来自作为服务器的TAA-FE的响应将通过TAA-FE-proxy返回至AM-FE。TAA-FE代理和TAA-FE服务器之间的通信通过Ni参考点进行。

注 – 若采用PPP [b-IETF RFC 1661]，则AM-FE终止PPP，并将其转换为Na参考点的信令信息。假设TAA-FE能够通过内部参考点联系NAC-FE，获取IP地址（TAA-FE和NAC-FE在PPP示例中是内部函数）。Nd参考点不承载DHCP信令[b-IETF RFC 2131]，反而Na参考点被用于向AM-FE提供IP配置信息。

7.2.5 传输用户配置文件功能实体 (TUP-FE)

TUP-FE是包含订阅认证数据（传输订阅用户识别符、支持的认证方法列表、密钥材料等）和与所要求的网络访问配置相关的信息（该数据被称“传输订阅配置文件”）的功能实体。传输订阅配置文件可包括TE的网络配置信息，例如IP地址或IP前缀。通过在TUP-FE中保存IP地址或IP前缀，IP地址或IP前缀可被唯一分配至TE，而不是通过NAC-FE被动态分配。传输订阅配置文件可被细分为子配置文件（见图4），每个子配置文件都与一个或多个逻辑连接标识符相关联。对逻辑连接标识符的支持是可选的。



注：每个子配置文件可包含超过一组传输资源订阅

图4 – TUP-FE中的传输订阅配置文件

TUP-FE响应TAA-FE关于完整配置文件或特定子配置文件的查询。在后一种情况下，TAA-FE（或TAA-FE-proxy）负责从逻辑连接标识符推导出子配置文件标识符。

TUP-FE可与SUP-FE放在同一位置（见[ITU-T Y.2012]描述）。

7.2.6 家庭网关配置功能实体（HGWC-FE）

在HGW的初始化和更新过程中使用HGWC-FE。它还为HGW提供附加配置信息（例如，HGW内部防火墙的配置，IP数据包的QoS标记等）。这些数据与NAC-FE提供的网络配置数据不同。

HGWC-FE的功能还包括：

- HGWC-FE控制和监测HGW的当前配置。
- HGWC-FE存储各类配置数据，因此可以决定HGW设置或下载那些配置参数或配置文件。HGWC-FE根据订阅用户信息和/或者应用类别来了解HGW和配置文件之间的关联。
- HGWC-FE具备向/从HGW设置（SET）/获取（GET）配置参数的机制。

建议HGWC-FE具备一种在帮助各种目的的配置文件（如固件更新或供应商特定配置文件）下载的机制。

HGWC-FE还可处理HGW就TE可用性发出的通知。HGWC-FE确实可以通过HGW以间接方式，或直接为TE提供配置信息。还可触发维护检测和处理HGW或TE发送的结果。

HGWC-FE还可与TLM-FE互动，以检索关于HGW以及与其相关联的访问的信息。在这种情况下，HGWC-FE使用第8.1.7段中描述的流程。从TLM-FE检索到的信息（例如物理连接标识符和/或者传输订阅用户标识符）可被用作对要提供给HGW的配置数据的选择的输入。

7.2.6.1 NACF中的优化认证

在网络附加过程中，HGW向NACF发起访问请求，而TAA-FE执行网络访问级别认证和授权。如成功，用于在HGW和HGWC-FE之间进行保护的安全关联（SA）可以在TAA-FE和HGW之间协商。

随后，TAA-FE通过Nc参考点将SA推送到TLM-FE，然后TLM-FE通过Nx参考点向HGWC-FE通知SA。

HGW和HGWC-FE之间的管理信息交换由SA双向认证。

注意，该程序是可选的。

7.2.7 访问中继功能实体（AR-FE）

AR-FE是CPE和NACF之间的中继。它接收CPE发出的网络访问请求，并将请求转发给NACF。在转发请求之前，AR-FE还可以插入本地配置信息。AR-FE的功能性描述见[ITU-T Y.2012]。

注 – 当使用PPP [b-IETF RFC 1661]时，AR-FE可用作PPPoE中继。当使用DHCP [b-IETF RFC 2131]时，AR-FE用作DHCP中继代理。

8 参考点

8.1 内部NACF参考点

8.1.1 参考点AM-FE – NAC-FE（Nd）

Nd参考点使AM-FE能够请求NAC-FE为CPE分配IP地址以及其他网络配置参数。

8.1.2 参考点NAC-FE – TLM-FE（Ne）

Ne参考点使NAC-FE能够在TLM-FE中注册分配的IP地址和CPE之间的绑定以及其他传输相关信息，例如逻辑/物理端口地址。

TLM-FE到NAC-FE的参考点使用以下信息流：

- 绑定指示
- 绑定确认
- 解绑指示
- 绑定信息查询
- 绑定信息查询确认

8.1.2.1 绑定指示

表2描述了绑定指示信息流中包含的元素。

表2 – 绑定指示 (NAC-FE → TLM-FE)

全局唯一IP地址信息	一组IP地址信息，用于定位CPE所附的接入网。
– 唯一IP地址	分配给附加的CPE的IP地址。
– 地址域	其中的IP地址具有重要意义的寻址域
物理连接标识符 (可选)	CPE附加的接入传输网络的物理连接的本地标识符 (例如PE-FE设备的IP地址、MAC地址或链路ID和物理端口)。
逻辑连接标识符 (注1)	CPE附加的接入传输网的逻辑连接的本地标识符 (例如，ATM VPI/VCI、PPP、MPLS 标签、GTP隧道和逻辑端口)。
CPE类型 (可选) (注2)	CPE的类型。
注1 – 若NAC-FE作为DHCP服务器实现，则该参数映射到DHCP选项82、子选项1和2[b-IETF RFC 2131]。	
注2 – 若NAC-FE作为DHCP服务器实现，则该参数映射到DHCP option 77 [b-IETF RFC 2131]。	

8.1.2.2 绑定确认

绑定确认信息流传达可发送回CPE的信息。TLM-FE从TAA-FE接收根据绑定指示返回的信息，或由TLM-FE通过TAA-FE从TUP-FE检索。

表3描述了绑定确认信息流中包含的元素。

表3 – 绑定确认 (TLM-FE → NAC-FE)

HGWC-FE地址 (可选)	HGWC-FE实体的地址，CPE可以从中检索配置数据。
地理位置信息 (可选)	地理位置信息。
P-CSCF身份 (可选)	用于访问IMS服务的P-CSCF的标识符[ITU-T Y.2021]。
SADS身份 (可选)	用于访问IPTV服务的SADS标识符[ITU-T Y.1910]。

8.1.2.3 解绑指示

当IP地址和CPE之间的绑定到期时，或者当底层PPP连接或第2层连接被释放时，NAC-FE发送解除绑定指示信息流。

表4描述了解绑指示信息流中包含的元素。

表 4 – 解绑指示 (NAC-FE → TLM-FE)

全局唯一IP地址信息	一组IP地址信息，用于定位CPE所附的接入网。
– 唯一IP地址	用于确定附加的CPE的IP地址。
– 地址域	IP地址的寻址域 (例如，子网前缀或者VPN ID)。

8.1.2.4 绑定信息查询

TLM-FE使用绑定信息查询信息流来向NAC-FE请求绑定信息（例如，在恢复流程的语境中）。

表5描述了绑定信息查询信息流中包含的元素。

表5 – 绑定信息查询（TLM-FE → NAC-FE）

全局唯一IP地址信息	一组IP地址信息，用于定位CPE所附的接入网。
– 唯一IP地址	用于确定附加的CPE的IP地址。
– 地址域	IP地址的寻址域（例如，子网前缀或者VPN ID）。

8.1.2.5 绑定信息查询确认

NAC-FE使用绑定信息查询确认信息流来向TLM-FE通知绑定信息查询请求的结果。当信息查询成功时，确认信息流包含表6中描述的信息。

Table 6 – 绑定信息查询确认（NAC-FE → TLM-FE）

物理连接标识符（可选）	CPE附加的接入传输网络的物理连接的本地标识符（例如PE-FE设备的IP地址、MAC地址或链路ID和物理端口）。
逻辑连接标识符（注1）	CPE所连接的接入传输网的逻辑连接的本地标识符（例如，ATM VPI/VCI、PPP、MPLS标签、GTP隧道和逻辑端口）。
CPE类型（可选）（注2）	CPE的类型。
注1 – CPE所连接的接入传输网的逻辑连接的本地标识符（例如，ATM VPI/VCI、PPP、MPLS标签、GTP隧道和逻辑端口）。	
注2 – 若NAC-FE作为DHCP服务器执行，则该参数映射到DHCP选项77 [b-IETF RFC 2131]。	

8.1.2.6 移动服务参数指示

用户成功认证后，使用移动服务参数指示信息流从TLM-FE向NAC-FE推送移动服务信息。

表7描述了移动服务参数指示信息流中包含的元素。

图7 – 移动服务参数指示 (TLM-FE → NAC-FE)

传输订阅用户标识符	附加的CPE的全局唯一标识符。该标识符可用于为CPE定位传输订阅信息。
全局唯一IP地址标识符	附加的CPE的全局唯一标识符。该标识符可用于为CPE定位传输订阅信息。
– 唯一IP地址	用于识别附加的CPE的IP地址。
– 地址域	IP地址的寻址域 (例如子网前缀或VPN ID)。
移动服务参数 (可选) (注2)	
– MLM-FE(C)地址 (注3)	包含移动地址绑定信息的MLM-FE实例的地址。
– MLM-FE(P)地址 (注3)	发送位置注册的MLM-FE实例的地址。
– 建钥资料 (注3)	用于UE和MMCF之间的安全关联的资料。
– 移动协议类型	TE或CPE可支持的移动协议类型, 例如基于主机或基于网络的移动性。
– 锚点地址 (可选)	UE角度的上层隧道端点地址。
– 隧道端点地址 (可选) (注4)	作为UE代理的网络节点的隧穿端点地址 (下层隧道端点)。
<p>注1 – 若被TAA-FE检索到, 则可纳入全局唯一IP地址信息。从MMCF角度, 该信息与永久IP地址一致。</p> <p>注2 – 只有采用移动服务适用。</p> <p>注3 – 只有采用基于主机的移动适用。</p> <p>注4 – 若隧道端点地址以静态方式提供, 或者MLM-FE可使用自身机制获取该信息, 则不需要该信息。仅在采用基于网络的移动时适用。</p>	

8.1.3 参考点AM-FE – TAA-FE (Na)

Na参考点使AM-FE能够向TAA-FE请求用户认证和传输订阅信息检查。

8.1.4 参考点TAA-FE – TLM-FE (Nc)

Nc参考点使TLM-FE能够就TAA-FE提供的位置信息隐私, 注册订阅用户与相应偏好之间的关联。参考点Nc亦被用于注册传输资源订阅信息。TLM-FE可从TAA-FE检索传输资源订阅信息。

TAA-FE – TAA-FE和TLM-FE之间的关系可以在拉模式或推模式下操作。当TAA-FE参与网络访问请求的处理时使用推模式, 以授权或拒绝对网络的访问 (例如, 在使用显式认证时)。当使用隐式认证或在支持TLM-FE恢复流程时使用拉模式。

Nc参考点使用以下信息流：

- 传输资源信息指示
- 传输资源信息请求
- 传输资源信息响应
- 传输资源释放通知

8.1.4.1 传输资源信息指示

用户成功认证后，传输资源信息指示信息流被用于从TAA-FE向TLM-FE推送传输订阅信息。TAA-FE可决定在相同的传输资源信息指示信息流中，以配置文件标识符的形式发送一些传输订阅配置文件（因为假设TLM-FE中的实际传输订阅配置文件信息可用），以完整配置文件形式发送一些其他的传输订阅配置文件。TAA-FE从TUP-FE检索该信息。

表8描述了传输资源信息指示信息流中包含的元素。

注 – 在采用case PPP [b-IETF RFC 1661]的情况下，TAA-FE可向TLM-FE提供物理连接标识符。

表8 – 传输资源信息指示（TAA-FE → TLM-FE）

传输订阅用户标识符	附加CPE的全局唯一标识符。该标识符可用于为CPE定位传输订阅信息。
全局唯一IP地址信息 (注1)	一组IP地址信息，用于定位CPE附加的接入网
- 唯一IP地址	用于确定附加的CPE的IP地址。
- 地址域	IP地址的寻址域（例如子网前缀或VPN ID）。
逻辑连接标识符	CPE所连接的接入传输网的逻辑连接的本地标识符（例如，ATM VPI/VCI、PPP、MPLS 标签、GTP隧道和逻辑端口）。
移动服务参数 (可选) (注7)	
- MLM-FE(C)地址 (注8)	包含移动地址绑定信息的MLM-FE实例的地址。
- MLM-FE(P)地址 (注8)	发送位置注册的MLM-FE实例的地址。
- 建钥资料 (注8)	用于UE和MMCF之间的安全关联的资料。
- 移动协议类型	TE或CPE可支持的移动协议类型，例如基于主机或基于网络的移动性。
- 锚点地址 (可选)	UE角度的上层隧道端点地址。
- 隧道端点地址 (可选) (注9)	作为UE代理的网络节点的隧穿端点地址（下层隧道端点）。
家庭TLM-FE联络点	家庭TLM-FE的FQDN或IP地址。
本地TLM-FE联络点	本地TLM-FE的FQDN或IP地址。
隐私指示器	表明位置信息是否可被导出至服务和应用。

表8 – 传输资源信息指示 (TAA-FE → TLM-FE)

安全关联 (可选)	HGW和TAA-FE在网络访问认证和授权过程中协商的安全关联。
传输资源订阅 (可选) (注2)	
– 传输订阅配置文件ID (注3)	一组传输订阅配置文件信息的标识符。
– 传输订阅配置文件描述 (注3)	
– 网络服务类别	表示CPE订阅的网络服务类别 (例如, 高级服务、金牌服务、银牌服务、常规服务等)。可包括QoS性能类别 (例如[ITU-T Y.1541]中定义的类别)。
– 订阅的上行带宽	CPE订阅的上行连接最大带宽。
– 订阅的下行带宽	CPE订阅的下行连接最大带宽。
– 优先级	任何预留请求允许的最大优先级。
– 请求程序名称	识别传输资源订阅允许的请求程序。
默认配置 (可选) (注4)	
– 默认配置标识符 (注5)	默认配置的标识符。
– 默认配置描述 (注5)	
– 默认接入控制列表: 获 准目的地和组播流	可发送流量的默认目的地IP地址和/或者端口和/或者前缀和/或者端口范围列表。在组播的情况下, IP组播群组地址列表和/或者可通过附加的用户设备接受到流量的 (源IP地址、IP-组播组地址) 对。列表中的地址范围获得支持。(注6)。
– 默认接入控制列表: 被 拒绝的目的地和组播流	默认情况下流量被拒绝的目的地IP地址、端口、前缀和端口范围列表。在组播的情况下, IP-组播列表地址列表和/或者必须拒绝向附加的用户设备发送流量的 (源IP地址、IP-组播组地址) 对的列表。列表中的地址范围获得支持。(注6)。
– 默认上行带宽	默认可用于上行连接的最大带宽。
– 默认下行带宽	默认可用于下行连接的最大带宽。
<p>注1 – 在使用PPP [b-IETF RFC 1661]的情况下, 要求TAA-FE向TLM-FE提供全局唯一IP地址信息。在使用DHCP [b-IETF RFC 2131]的情况下, 该参数可选。</p> <p>注2 – 传输资源订阅可包含多个传输订阅配置文件。</p> <p>注3 – 可包含传输订阅配置文件ID或传输订阅配置文件描述, 但不可同时包含二者。</p> <p>注4 – 在收到服务/应用的资源预留请求之前, RACF使用该信息来配置传输功能。</p> <p>注5 – 可包含默认配置标识符或默认配置标识符描述, 但不可同时包含二者。</p> <p>注6 – 如果这两个列表均不显示某一目的地, 则这些地址的门设置由RACF控制决定。</p> <p>注7 – 仅在使用移动服务时可用。</p> <p>注8 – 仅在使用基于主机的移动服务时可用。</p> <p>注9 – 若隧道端点地址以静态方式提供, 或者MLM-FE可使用自身机制获取该信息, 则不需要该信息。仅在采用基于网络的移动时可用。</p>	

8.1.4.2 传输资源信息请求

TLM-FE使用传输资源信息请求信息流来向TAA-FE请求传输订阅配置文件信息。当TLM-FE和TAA-FE之间的关系在拉模式下操作，或在TLM-FE恢复程序的语境中时使用该信息流。

表9描述了传输资源信息请求信息流中包含的元素。

表9 – 传输资源信息请求 (TLM-FE → TAA-FE)

全局唯一IP地址信息 (注1)	一组IP地址信息，用于定位CPE附加的接入网
– 唯一IP地址	用于识别所附CPE的IP地址
– 地址域	IP地址的寻址域 (例如，子网前缀或VPN ID)。
逻辑连接标识符	CPE所连接的接入传输网的逻辑连接的本地标识符 (例如，ATM VPI/VCI、PPP、MPLS标签、GTP隧道和逻辑端口)。
传输订阅用户标识符 (注2)	附加的CPE的全局唯一标识符。本标识符可用于为CPE定位传输订阅信息。
注1 – 若信息流被用于支持恢复流程，且参考点在推模式下操作，则须包含全局唯一IP地址信息。	
注2 – 若参考点在拉模式下操作，则须包含传输订阅用户标识符。	

8.1.4.3 传输资源信息响应

TAA-FE使用传输资源信息响应信息流向TLM-FE提供传输订阅信息，以响应传输资源信息请求。

表10描述了传输资源信息响应信息流中包含的元素。

注 – 在使用PPP [b-IETF RFC 1661]的情况下，TAA-FE可向TLM-FE提供物理连接标识符。

表10 – 传输资源信息响应 (TAA-FE → TLM-FE)

传输订阅用户标识符	附加的CPE的全局唯一标识符。本标识符可用于为CPE定位传输订阅信息。
全局唯一IP地址信息 (注1)	一组IP地址信息，用于定位CPE所附的接入网。
– 唯一IP地址	用于识别所附CPE的IP地址。
– 地址域	IP地址的寻址域 (例如，子网前缀或VPN ID)。
逻辑连接标识符	CPE所连接的接入传输网的逻辑连接的本地标识符 (例如，ATM VPI/VCI、PPP、MPLS 标签、GTP隧道和逻辑端口)。
移动服务参数 (可选) (注7)	
– MLM-FE(C)地址 (注8)	包含移动地址绑定信息的MLM-FE实例的地址。
– MLM-FE(P)地址 (注8)	发送位置注册的MLM-FE实例的地址。

表10 – 传输资源信息响应 (TAA-FE → TLM-FE)

– 建钥资料 (注8)	用于UE和MMCF之间的安全关联的资料。
– 移动协议类型	TE或CPE可支持的移动协议类型，例如基于主机或基于网络的移动性。
– 锚点地址 (可选)	UE角度的上层隧道端点地址。
– 隧道端点地址 (可选) (注9)	作为UE代理的网络节点的隧穿端点地址 (下层隧道端点)。
隐私指示器	表明位置信息是否可被导出至服务和应用。
安全关联 (可选)	HGW和TAA-FE在网络访问认证和授权过程中发起的安全关联。
传输资源订阅 (可选) (注2)	
– 传输订阅配置文件ID (注3)	一组传输订阅配置文件信息的标识符。
– 传输订阅配置文件描述 (注3)	
– 网络服务类别	表示CPE订阅的网络服务类别 (例如，高级服务、金牌服务、银牌服务、常规服务等)。可包括QoS性能类别 (例如[ITU-T Y.1541]中定义的类别)。
– 订阅的上行带宽	CPE订阅的上行连接最大带宽。
– 订阅的下行带宽	CPE订阅的下行连接最大带宽。
– 优先级	任何预留请求允许的最大优先级。
– 请求程序名称	识别传输资源订阅允许的请求程序。
默认配置 (可选) (注4)	
– 默认配置标识符 (注5)	默认配置的标识符。
– 默认配置描述 (注5)	
– 默认接入控制列表：获 准目的地和组播列表	可发送流量的默认目的地IP地址和/或者端口和/或者前缀和/或者端口范围列表。在组播的情况下，IP组播群组地址列表和/或者可通过附加的用户设备接受到流量的 (源IP地址、IP-组播组地址) 对列表。列表中的地址范围获得支持。(注6)。
– 默认接入控制列表：被 拒绝的目的地和组播流的 列表	默认情况下流量被拒绝的目的地IP地址、端口、前缀和端口范围列表。在组播的情况下，IP-组播列表地址列表和/或者必须拒绝向附加的用户设备发送流量的 (源IP地址、IP-组播组地址) 对的列表。列表中的地址范围获得支持。(注6)
– 默认上行带宽	默认可用于上行连接的最大带宽。
– 默认下行带宽	默认可用于下行连接的最大带宽。

表10 – 传输资源信息响应 (TAA-FE → TLM-FE)

注 – 在使用PPP [b-IETF RFC 1661]的情况下，TAA-FE须向TLM-FE提供全局唯一IP地址信息。在使用DHCP [b-IETF RFC 2131]的情况下，该参数可选。
注2 – 传输资源订阅可包含多个传输订阅配置文件。
注3 – 可包含传输订阅配置文件ID或传输订阅配置文件描述，但不可同时包含二者。
注4 – 在收到服务/应用的资源预留请求之前，RACF使用该信息来配置传输功能。
注5 – 可包含默认配置标识符或默认配置标识符描述，但不可同时包含二者。
注6 – 如果这两个列表均不显示某一目的地，则这些地址的门设置由RACF控制决定。
注7 – 仅在使用移动服务时可用。
注8 – 仅在使用基于主机的移动服务时可用。
注9 – 若隧道端点地址以静态方式提供，或者MLM-FE可使用自身机制获取该信息，则不需要该信息。仅在采用基于网络的移动时可用。

8.1.4.4 传输资源释放通知

TAA-FE使用传输资源释放通知信息流来向TLM-FE请求删除其保存的关于CPE的信息。该事件是网络管理操作的结果。

表11描述了传输资源释放通知信息流中包含的元素。

表11 – 传输资源释放通知 (TAA-FE → TLM-FE)

全局唯一IP地址信息 (注)	一组IP地址信息，用于定位CPE所附的接入网。
– 唯一IP地址	用于确定所附加的CPE的IP地址。
– 地址域	IP地址的寻址域 (例如，子网前缀或VPN ID)。
本地连接标识符 (可选)	CPE所连接的接入传输网的逻辑连接的本地标识符 (例如，ATM VPI/VCI、PPP、MPLS标签、GTP隧道和逻辑端口)。
传输订阅用户标识符 (注)	附加的CPE的全局唯一标识符。该标识符可用于为CPE定位传输订阅信息。
注 – 包含全局唯一IP地址信息或传输订阅用户标识符。	

8.1.5 参考点NAC-FE – TAA-FE (Nk)

本建议书未规定Nk参考点。

8.1.6 参考点TAA-FE – TAA-FE (Ni)

本参考点旨在被用于可能位于不同管理域的TAA-FE-proxy和TAA-FE-server之间。该参考点使TAA-FE-proxy能够基于传输订阅配置文件，向TAA-FE-server请求用户认证和授权。它还使TAA-FE-proxy能够将特定用户会话的计费数据转发给TAA-FE-server，或转发TLM-FE发出的请求。

TAA-FE-proxy将通过Na参考点从AM-FE接收的访问和授权请求以及计费消息转发到通过Ni参考点的TAA-FE-server。通过Ni参考点从TAA-FE-server返回的响应将通过Na参考点转发给AM-FE。TAA-FE-proxy和TAA-FE-server之间需要建立双边信任关系，以协助进行这一交换。

该参考点支持TAA-FE-proxy和TAA-FE-server之间的AAA消息交换。

注 – RADIUS [b-IETF RFC 2865]和Diameter [b-IETF RFC 3588]是该参考点协议的两个可能选项。

8.1.6.1 Ni上的信息交换

表12给出了Ni参考点上交换的信息组件。

表12 – Ni参考点

信息组件	描述
传输订阅用户标识符	附加的CPE的全局唯一标识符。该标识符可用于为CPE定位传输订阅信息。
隐私指示器	表明位置信息是否可被导出至服务和应用。
全局唯一IP地址信息	一组IP地址信息，用于定位CPE所附的接入网。
– 唯一IP地址	用于识别所附CPE的IP地址。
– 地址域	IP地址的寻址域（例如，子网前缀或VPN ID）。
移动服务参数（可选）（注6）	
– MLM-FE(C)地址（注7）	包含移动地址绑定信息的MLM-FE实例的地址。
– MLM-FE(P)地址（注7）	发送位置注册的MLM-FE实例的地址。
– 建钥资料（注7）	用于UE和MMCF之间的安全关联的资料。
– 移动协议类型	TE或CPE可支持的移动协议类型，例如基于主机或基于网络的移动性。
– 锚点地址（可选）	UE角度的上层隧道端点地址。
– 隧道端点地址（可选）（注8）	作为UE代理的网络节点的隧穿端点地址（下层隧道端点）。
家庭TLM-FE联络点	家庭TLM-FE的FQDN或IP地址。
互通信息（可选）	当CPE被附加到一个访问网络时用于识别网络和服务附件信息的一组互通信息（例如，IPTV服务控制协议、SADS身份等）
传输资源订阅 （可选）（注1）	
– 传输订阅配置文件ID（注2）	一组传输订阅配置文件信息的标识符。
– 传输订阅配置文件描述（注2）	
– 网络服务类别	表示所附CPE订阅的网络服务类别（例如，高级服务、金牌服务、银牌服务、常规服务等）。可包括QoS性能类别（例如[ITU-T Y.1541]中定义的类别）。
– 订阅的上行带宽	CPE订阅的上行连接最大带宽。
– 订阅的下行带宽	CPE订阅的下行连接最大带宽。

表12 – Ni参考点

信息组件	描述
– 优先级	任何预留请求允许的最大优先级。
– 请求程序名称	识别传输资源订阅允许的请求程序。
默认配置 (可选) (注3)	
– 默认配置标识符 (注4)	默认配置的标识符。
– 默认配置描述 (注4)	
– 默认接入控制列表: 获准目的地和组播流	默认可发送流量的目的地IP地址和/或者端口和/或者前缀和/或者端口范围列表。在组播的情况下, IP组播群组地址列表和/或者可通过附加的用户设备接受到流量的(源IP地址、IP-组播组地址)对。列表中的地址范围获得支持。(注: 5)。
– 默认接入控制列表: 被拒绝的目的地和组播流	默认情况下流量被拒绝的目的地IP地址、端口、前缀和端口范围列表。在组播的情况下, IP-组播列表地址列表和/或者必须拒绝向所附加的用户设备发送流量的(源IP地址、IP-组播组地址)对的列表。列表中的地址范围获得支持。(注5)。
– 默认上行带宽	默认可用于上行连接的最大带宽。
– 默认下行带宽	默认可用于下行连接的最大带宽。
<p>注1 – 传输资源订阅可包含多个配置文件。</p> <p>注2 – 可包含传输订阅配置文件ID或传输订阅配置文件描述, 但不可同时包含二者。</p> <p>注3 – 在收到服务/应用的资源预留请求之前, RACF使用该信息来配置传输功能。</p> <p>注4 – 可包含默认配置标识符或默认配置标识符描述, 但不可同时包含二者。</p> <p>注5 – 如果这两个列表均不显示某一目的地, 则这些地址的门设置由RACF控制决定。</p> <p>注6 – 仅在使用移动服务时可用。</p> <p>注7 – 仅在使用基于主机的移动时可用。</p> <p>注8 – 若隧道端点地址以静态方式提供, 或者MLM-FE可使用自身机制获取该信息, 则不需要该信息。仅在采用基于网络的移动时可用。</p>	

8.1.7 参考点HGWC-FE – TLM-FE (Nx)

Nx参考点使HGWC-FE能够从TLM-FE检索信息。注意, Nx参考点的性质与S-TC1参考点类似(见第8.3.1段)。在这种情况下, HGWC-FE表现为一种特殊类型的服务控制功能。

8.1.7.1 信息查询请求

表13描述了信息查询请求信息流中包含的信息。

表13 – 信息查询请求 (HGWC-FE → TLM-FE)

全局唯一IP地址信息	一组IP地址信息，用于定位CPE所附的接入网。
– 唯一IP地址	用于识别所附CPE的IP地址。
– 地址域	IP地址的寻址域（例如，子网前缀或VPN ID）。
SCF身份	表明家庭网关配置应用。

8.1.7.2 信息查询响应

表14描述了信息查询响应信息流中包含的信息。

表14 – 信息查询响应 (TLM-FE → HGWC-FE)

传输订阅用户标识符	附加的CPE的全局唯一标识符。本标识符可用于为CPE定位传输订阅信息。
物理连接标识符	CPE附加的接入传输网络的物理连接的本地标识符（例如PE-FE设备的IP地址、MAC地址或链路ID和物理端口）。
逻辑连接标识符	CPE所连接的接入传输网的逻辑连接的本地标识符（例如，ATM VPI/VCI、PPP、MPLS 标签、GTP隧道和逻辑端口）。

8.1.8 参考点TLM-FE – TLM-FE (Ng)

Ng参考点实现本地和家庭TLM-FE之间的通信。

可能产生五种操作：从本地TLM-FE到家庭TLM-FE的位置注册、位置查询和移除位置信息；从家庭TLM-FE到本地TLM-FE的位置查询，以及从本地TLM-FE到本地TLM-FE的位置情境指示。

8.1.8.1 位置注册

表15描述了位置注册信息流的内容。

表15 – 位置注册 (本地TLM-FE → 家庭TLM-FE)

全局唯一IP地址信息	一组IP地址信息，用于定位CPE所附的接入网。
– 唯一IP地址	用于识别所附CPE的IP地址。
– 地址域	IP地址的寻址域（例如，子网前缀或者VPN ID）。
传输订阅用户标识符	请求IP连接的CPE的全局唯一标识符。
附加的接入域名	CPE附加的接入域名或提供商名称。
本地TLM-FE联络点	本地TLM-FE的FQDN或IP地址。

8.1.8.2 位置查询

表16描述了位置查询信息流的内容。

表16 – 位置查询（家庭TLM-FE → 本地TLM-FE）

全局唯一IP地址信息	一组IP地址信息，用于定位CPE所附的接入网。
– 唯一IP地址	用于识别所附CPE的IP地址。
– 地址域	IP地址的寻址域（例如，子网前缀或者VPN ID）。
传输订阅用户标识符	所附CPE的全局唯一标识符。
附加的接入域名	CPE附加的接入域名或提供商名称。
本地TLM-FE联络点	本地TLM-FE的FQDN或IP地址。

8.1.8.3 位置查询响应

位置查询响应信息流与S-TC1参考点上的信息查询响应一致（见第8.3.1.2段）。

8.1.8.4 移除位置信息

表17描述了移除位置信息流的内容。

表17 – 移除位置（本地 TLM-FE → 家庭 TLM-FE）

全局唯一IP地址信息	与附加到网络的用户相关的UNI对应的全局唯一地址。
– 唯一IP地址	用于识别CPE的IP地址。
– 地址域	IP地址的寻址域（例如，子网前缀或者VPN ID）。
传输订阅用户标识符	请求传输资源的CPE的全局唯一标识符。本标识符可用于为CPE定位传输订阅信息。

8.1.8.5 位置情境指示

表18描述了位置情境交换信息流的内容。

表18 – 位置情境指示（本地TLM-FE →本地TLM-FE）

全局唯一IP地址信息	一组IP地址信息，用于定位CPE所附的接入网。
– 唯一IP地址	用于识别所附CPE的IP地址。
– 地址域	IP地址的寻址域（例如，子网前缀或者VPN ID）。
传输订阅用户标识符	所附CPE的全局唯一标识符。
附加的接入域名	接入域名或访问网络的提供商名称
本地TLM-FE联络点	本地TLM-FE的FQDN或IP地址

表18 – 位置情境指示（本地TLM-FE →本地TLM-FE）

隐私指示器 (注1)	表明位置信息是否可被导出至服务和应用。
传输资源订阅 (注2和3)	
– 传输订阅配置文件ID (注4)	一组传输订阅配置文件信息的标识符
– 传输订阅配置文件描述 (注4)	
– 网络服务类别	表示CPE订阅的网络服务类别（例如，高级服务、金牌服务、银牌服务、常规服务等）。可包括QoS性能类别（例如[ITU-T Y.1541]中定义的类别）。
– 订阅的上行带宽	CPE订阅的上行连接最大带宽。
– 订阅的下行带宽	CPE订阅的上行连接最大带宽。
– 优先级	任何预留请求允许的最大优先级。
– 请求程序名称	识别传输资源订阅允许的请求程序。
默认配置（可选）	
– 默认配置标识符 (注5)	默认配置的标识符。
– 默认配置描述 (注5)	
– 默认接入控制列表：获准目的地和组播流	默认允许直通的目标IP地址、端口、前缀和端口范围列表。在组播的情况下，IP组播群组地址列表和/或者可通过附加的用户设备接受到流量的（源IP地址、IP-组播组地址）对。列表中的地址范围获得支持。（注6）。
– 默认接入控制列表：被拒绝的目的地和组播流的列表	默认情况下流量被拒绝的目的地IP地址、端口、前缀和端口范围列表。在组播的情况下，IP-组播列表地址列表和/或者必须拒绝向附加的用户设备发送流量的（源IP地址、IP-组播组地址）对的列表。列表中的地址范围获得支持。（注6）
– 默认上行带宽	默认可用于上行连接的最大带宽。
– 默认下行带宽	默认可用于下行连接的最大带宽。

表18 – 位置情境指示（本地TLM-FE →本地TLM-FE）

注1 – 根据应用的安全级别，指示应用是否可以访问位置信息。
注2 – 传输资源订阅可包含多个传输订阅配置文件。
注3 – 可包含传输订阅配置文件ID或传输订阅配置文件描述，但不可同时包含二者。
注4 – 收到服务/应用的资源预留请求之前，RACF使用该信息来配置传输功能。
注5 – 可包含默认配置标识符或默认配置标识符描述，但不可同时包含二者。
注6 – 如果这两个列表均不显示某一目的地，则这些地址的门设置由RACF控制决定。

8.1.9 参考点TUP-FE – TAA-FE (Nb)

本建议书未规定Nb参考点，即TAA-FE 和TUP-FE不是同位置就是通过非标准化的接口连接。

8.2 NACF与资源和接纳控制功能(RACF)之间的参考点

8.2.1 TLM-FE和RACF之间的参考点(Ru)

Ru参考点允许PD-FE与NACF互动，用于检查CPE传输订阅配置文件信息和到分配的IP地址的逻辑/物理端口地址的绑定信息。

Ru参考点是域内参考点。

Ru参考点允许以下信息交换：

- NACF推送传输订阅配置文件信息到PD-FE。
- PD-FE从NACF中提取传输订阅配置文件信息。

欲进一步了解详细信息，请参阅[ITU-T Y.2111]的第8.4段。

8.3 NACF和服务控制功能之间的参考点

8.3.1 TLM-FE和服务控制功能（S-TC1）之间的参考点

S-TC1参考点使业务控制功能（SCF）能够从TLM-FE检索用于访问此类业务控制功能的IP连接会话的特性的信息（例如，网络位置信息）。TLM-FE提供的位置信息的形式取决于请求程序。

S-TC1参考点使用以下信息流：

- 信息查询请求
- 信息查询响应
- 事件注册请求
- 事件注册响应
- 通知事件请求
- 通知事件响应

8.3.1.1 信息查询请求

表19描述了信息查询请求信息流中包含的信息。

表19 – 信息查询请求 (SCF → TLM-FE)

全局唯一IP地址信息 (注1)	一组IP地址信息, 用于定位CPE所附的接入网。
– 唯一IP地址	用于识别所附CPE的IP地址。
– 地址域	IP地址的寻址域 (例如子网前缀或VPN ID) (注2)。
传输预定用户标识符 (注1)	所附CPE的全局唯一标识符。
SCF身份	请求服务控制功能的标识符。
注1 – 包含全局唯一IP地址信息或传输订阅用户标识符。	
注2 – SCF可使用配置数据 (在这种情况下, SCF服务的所有终端设备都属于同一个寻址域) 或接收触发位置查询的服务请求的物理或逻辑接口来获悉寻址域。	

8.3.1.2 信息查询响应

表20描述了信息查询响应信息流中包含的信息。

表20 – 信息查询响应 (TLM-FE → SCF)

传输订阅用户标识符 (可选)	附加的CPE的全局唯一标识符 (注1)。
位置信息 (可选) (注2)	采用适合于请求服务控制功能的形式的位置信息 (或指向此类信息的指针)。
RACF联络点 (可选)	发送资源请求的RACF实体的FQDN或IP地址 (例如, PD-FE地址)。
CPE类型 (可选)	CPE的类型。
接入网类型 (可选)	CPE附加的接入网类型。
物理连接标识符 (可选)	CPE附加的接入传输网络的物理连接的本地标识符 (例如PE-FE设备的IP地址、MAC地址或链路ID和物理端口)。
逻辑连接标识符 (可选)	CPE所连接的接入传输网的逻辑连接的本地标识符 (例如, ATM VPI/VCI、PPP、MPLS标签、GTP隧道和逻辑端口)。
注1 – SCF在与RACF互动时可使用该标识符。	
注2 – 是否披露位置信息由请求应用和订阅用户的隐私限制决定。隐私限制由TLM-FE中存储的隐私指示器定义。	

8.3.1.3 事件注册请求

表21描述了事件注册请求信息流中包含的信息。若SCF是P-CSCF [ITU-T Y.2021], 则本信息流不适用。

表21 – 事件注册请求(SCF → TLM-FE)

订阅持续时间	特定事件的订阅处于活动状态的持续时间。
传输订阅用户标识符（可选） （注1）	所附CPE的全局唯一标识符。
事件	事件中继/通知描述的事件类型（例如用户登录事件）和格式。
全局唯一IP地址信息（可选） （注1）	一组IP地址信息，用于定位CPE所附的接入网。
– 唯一IP地址	用于识别所附CPE的IP地址。
– 地址域	IP地址的寻址域（例如子网前缀或VPN ID）（注2）。
SCF身份（可选）	请求服务控制功能的标识符。
注1 – 要求至少提供两个识别符（“传输订阅用户识别符”或“全局唯一IP地址信息”）中的一个。	
注2 – SCF使用配置数据（在这种情况下，SCF服务的所有用户设备都属于同一个寻址域）或通过接收相关服务请求的物理或逻辑接口来获悉寻址域。	

8.3.1.4 事件注册响应

表22描述了事件注册响应信息流中包含的信息。若SCF是P-CSCF [ITU-T Y.2021].，则该信息流不适用。

表22 – 事件注册响应（TLM-FE → SCF）

更新行为	事件的管理行为/信息：例如，ACTIVATED（成功收到事件注册和激活“事件”的事件通知。）
传输订阅用户标识符（注）	所附CPE的全局唯一标识符。
事件	事件类型（例如，用户登录事件）
全局唯一IP地址信息（可选）	一组IP地址信息，用于定位CPE所附的接入网。
– 唯一IP地址	用于识别所附CPE的IP地址。
– 地址域	IP地址的寻址域（例如子网前缀或VPN ID）
注 – 要求至少提供两个识别符（“传输订阅用户识别符”或“全局唯一IP地址信息”）中的一个。	

8.3.1.5 通知事件请求

表23描述了通知事件请求信息流中包含的信息。若SCF是P-CSCF [ITU-T Y.2021]，则本信息流不适用。

表23 – 通知事件请求 (TLM-FE → SCF)

全局唯一IP地址信息 (可选)	一组IP地址信息, 用于定位CPE所附的接入网。
– 唯一IP地址	用于识别所附CPE的IP地址。
– 地址域	IP地址的寻址域 (例如子网前缀或VPN ID)。
传输订阅用户标识符	所附CPE的全局唯一标识符。
事件	事件类型 (例如, 用户登录事件)

8.3.1.6 通知事件响应

表24描述了通知事件响应信息流中包含的信息。若SCF是P-CSCF [ITU-T Y.2021], 则本信息流不适用。

表24 – 通知事件响应 (SCF → TLM-FE)

全局唯一IP地址信息	一组IP地址信息, 用于定位CPE所附的接入网。
– 唯一IP地址	用于识别所附CPE的IP地址。
– 地址域	IP地址的寻址域 (例如子网前缀或VPN ID)。
传输订阅用户标识符	所附CPE的全局唯一标识符。
事件	事件类型。
结果	结果代码 (例如, 成功、永久失效等)。

8.4 NACF和CPE之间的参考点

8.4.1 用于认证和IP地址分配的参考点 (T-U1和TC-T1)

NACF和CPE之间没有直接的参考点用于支持认证和IP地址分配。NACF和CPE之间的通信通过传输功能中的接入中继功能实体 (AR-FE) 进行, 涉及CPE和AR-FE之间的T-U1参考点和AR-FE和NACF之间的TC-T1参考点。

CPE侧的TC-T1参考点可通过HGW或TE终止。当TE与AR-FE直接连接时可使用TE来终止。

T-U1参考点使CPE能够发起对IP地址分配和可能的其他网络配置参数的请求, 以接入网络。这些请求由AR-FE接收, 并通过TC-T1参考点中继至NACF中的AM-FE。

IP地址分配和网络配置参数的请求采用DHCP [b-IETF RFC 2131]或PPP [b-IETF RFC 1661]请求格式。

若采用DHCP, 传输功能包含作为CPE中的DHCP客户端和NACF中的DHCP服务器之间的DHCP中继的接入中继功能实体 (AR-FE)。

在向TC-T1参考点上的NACF发送请求之前, AR-FE可将网络位置信息添加到T-U1参考点上从CPE接收的信息中。T-U1参考点使CPE能够向NACF提供用户凭证 (密码、令牌、证书等), 以执行网络访问认证。T-U1参考点还可让NACF为CPE提供认证参数, 以便在需要执行手动认证流程时进行网络认证。AM-FE根据认证结果授权或拒接至CPE的网络访问。

注 – 当NACF和CPE之间使用DHCP分配IP地址和配置CPE时，IEEE 802.1X [b-IEEE 802.1X]和PANA [b-IETF RFC 4058]是NACF和CPE之间认证的候选协议。

8.4.2 HGWC-FE和CPE (TC-Ux) 之间的参考点

TC-Ux参考点允许HGWC-FE配置HGW、触发维护测试、监控性能和接收通知。在HGW初始化和更新期间使用TC-Ux参考点，为HGW提供T-U1参考点上无法获得的额外网络配置信息，从而使HGW能够访问NGN服务控制功能。

HGWC-FE还可管理连接到一个HGW的TE设备（通过HGW间接连接，或直接连接至TE），用于配置、维护、性能监控和通知。

TC-Ux参考点支持以下流程：

- 向HGWC-FE发送HGW识别/认证(例如，为了从HGWC-FE发送适当的配置信息(固件升级)。
- 例如，在一个HGW接受远程配置之前，对HGW进行HGWC-FE认证。
- 从HGWC-FE触发维护测试，并从HGW报告测试结果。
- 配置HGW。
- 向HGWC-FE告知TE可用性。
- 配置和升级TE。
- 从HGWC-FE触发维护测试，并从TE报告测试结果。

注 – TR-069 [b-DSL Forum TR-069]、HTTP [b-IETF RFC 2616]、FTP [b-IETF RFC 959] 和TFTP [b-IETF RFC 783]是该参考点的候选协议。

8.5 NACF与移动管理和控制功能 (MMCF) 之间的参考点

8.5.1 TLM-FE和MLM-FE(P) (M1)之间的参考点

M1参考点允许TLM-FE与MLM-FE(P)互动，以推送移动服务参数，例如建钥资料、锚点地址等。

M1参考点是域内参考点。

M1参考点允许如下信息交换：

- TLM-FE向MLM-FE(P)推送移动服务参数信息。

欲进一步了解详细信息，请参阅[ITU-T Y.2018]第6.5段。

8.5.2 TLM-FE和HDC-FE (M2)之间的参考点

M2参考点允许TLM-FE与HDC-FE互动，以推送移动服务参数，例如建钥资料，以支持HDC-FE和UE之间所需的安全关联。

M2参考点是域内参考点。

M2参考点允许以下信息交换：

- TLM-FE向HDC-FE推送移动服务参数信息。

欲进一步了解详细信息，请参阅[ITU-T Y.2018]第6.5段。

8.5.3 TLM-FE和NID-FE (M13)之间的参考点

M13参考点允许TLM-FE与NID-FE互动，以推送移动服务参数，例如建钥资料，以支持HID-FE和UE之间所需的安全关联。

M13参考点是域内参考点。

M13参考点允许以下信息交换：

- TLM-FE向NID-FE推送移动服务参数信息。

欲进一步了解详细信息，请参阅[ITU-T Y.2018]第6.5段。

9 安全考虑

NACF功能需求和架构中的安全需求由NGN [ITU-T Y.2701]的安全需求以及NGN授权和认证的安全需求[ITU-T Y.2702]来应对。

附录I

到网络角色的映射

(本附录不构成本建议书的组成部分)

NACF架构不承担任何业务角色。然而，为应对游牧性和漫游需求，NACF架构可被映射至固定宽带接入环境中存在的各种功能的网络角色上，如图I.1所示。

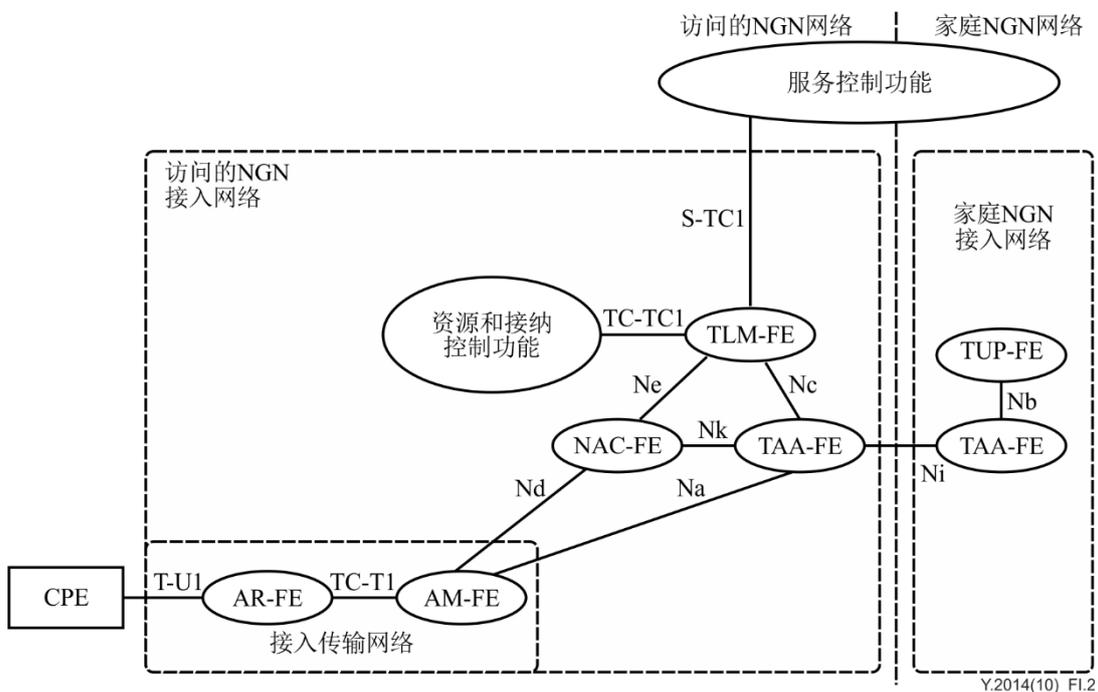


图I.1 - NGN中的功能网络角色

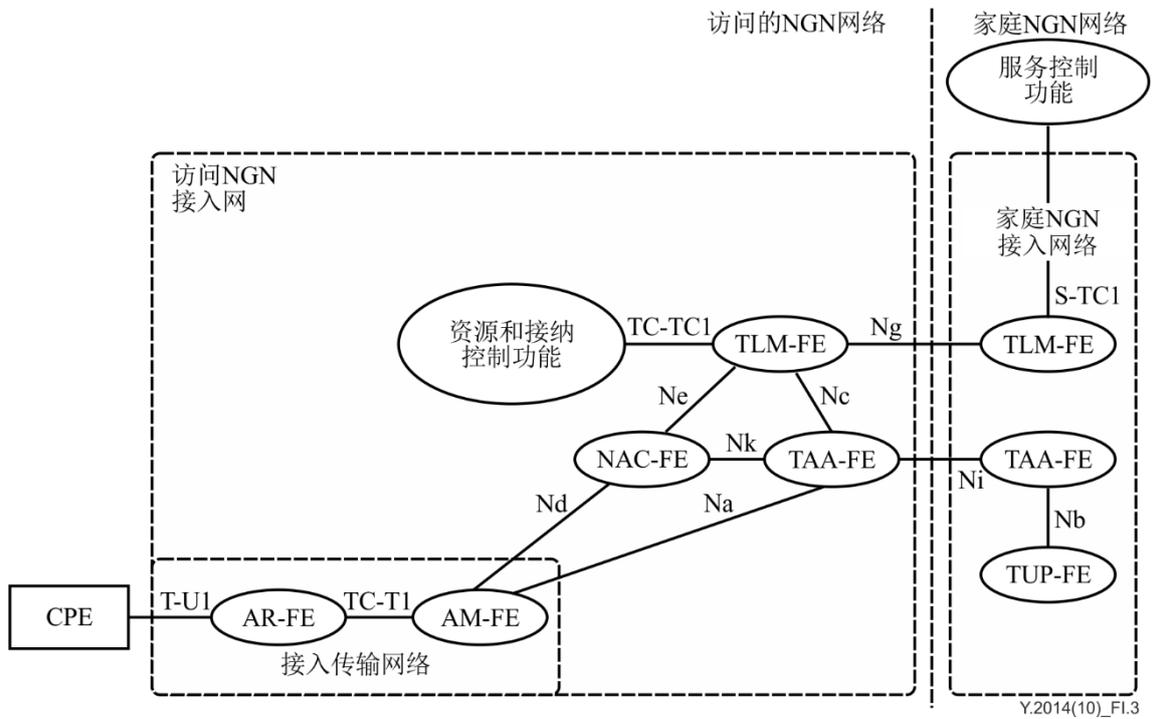
图I.2和I.3给出了NACF的映射。这些图中的接入网示例为xDSL接入网或WLAN热点。

图I.2显示了场景1。在该场景中，访问的NGN网络提供（部分）服务控制功能。图I.3阐释了场景2。在该场景中，家庭NGN网络提供了服务控制功能。

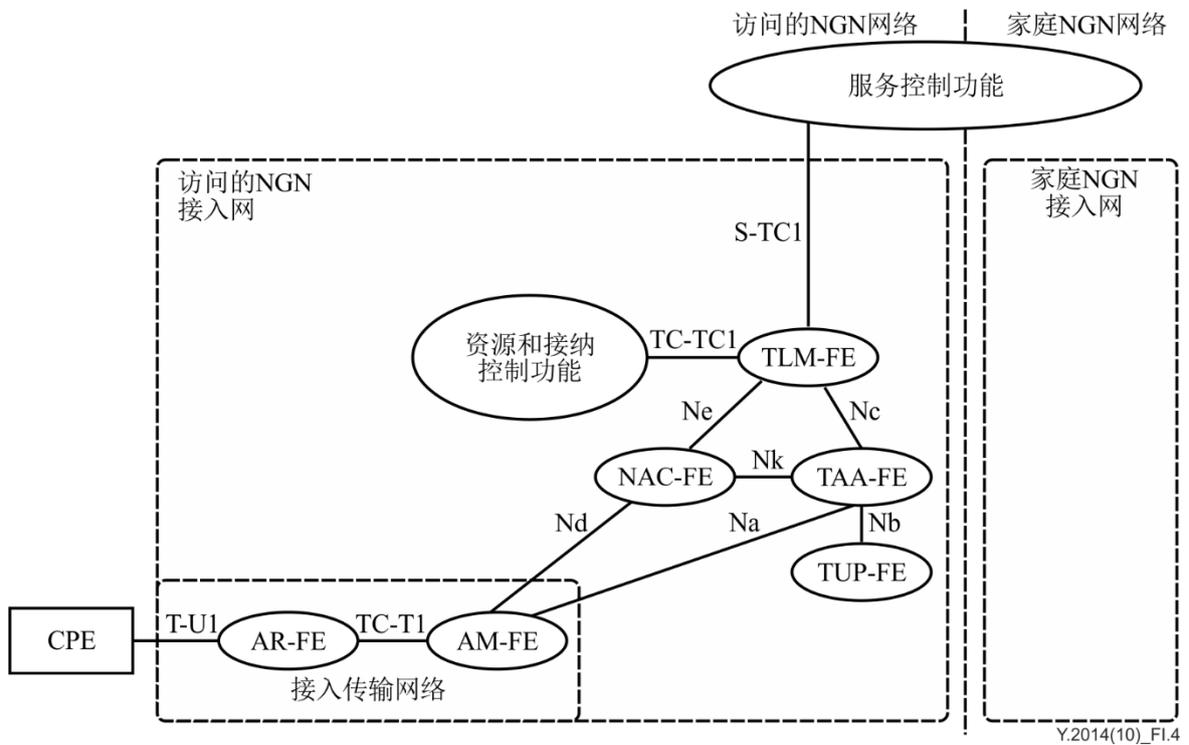
图I.4和I.5均展示了场景3和4。在这两个场景中，访问CPE不执行接入认证。在图I.4中，访问CPE可通过服务控制功能级别的漫游协议访问其家庭服务。不过，该定义在本建议书范围之外。图I.5给出了一个场景。在该场景中，家庭网络的服务控制功能接入被访问网络中的TLM-FE，通过家庭网络的TLM-FE-proxy获取位置信息。此处使用Ng参考点作为TLM-FE到TLM-FE的参考点。



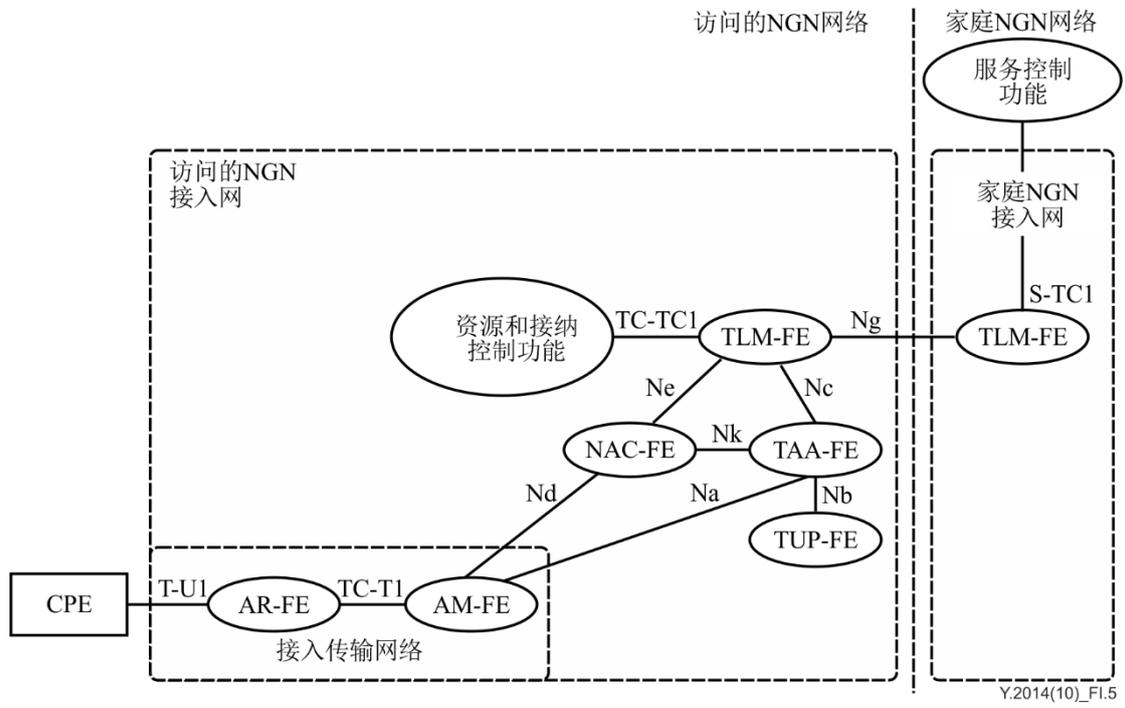
图I.2 - 映射到功能网络角色上的NACF - 场景1



图I.3 – 映射到功能网络角色上的NACF – 场景2
(由家庭网络提供的NGN服务)



图I.4 – 映射到功能网络角色上的NACF – 场景3



图I.5 – 映射到功能网络角色上的NACF – 场景4

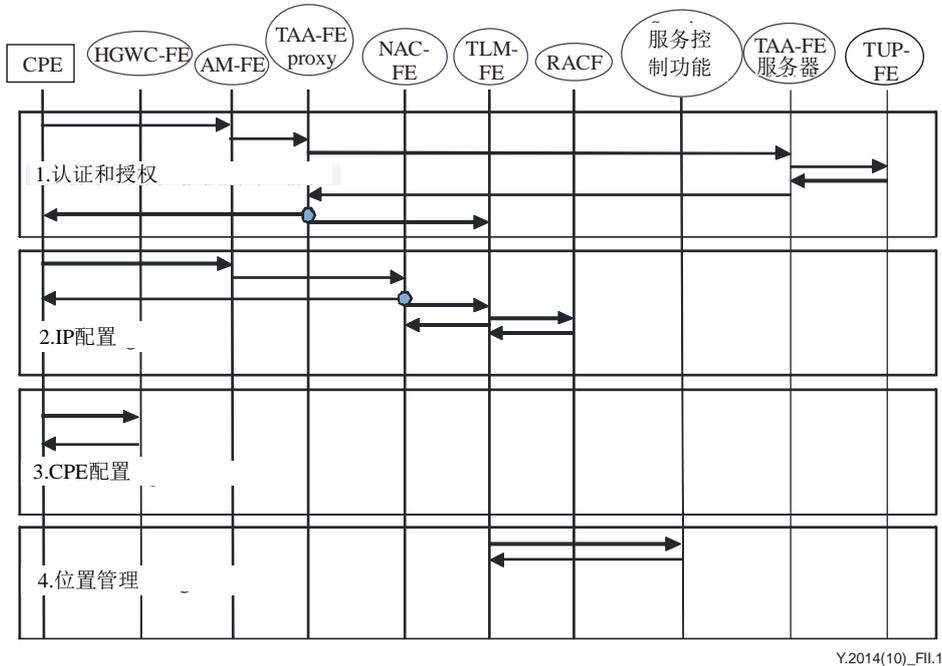
附录II

信息流

(本附录不构成本建议书的组成部分)

II.1 高级信息流

本段提供了高级信息流。该信息流定义网络附加过程以及在NACF中和面向RACF的传输订阅配置文件信息的分发。



图II.1 – 高级信息流

NACF依靠网络附加过程的多个阶段来实现。图II.1显示了高级信息流和NACF的不同流程。这些阶段可以按不同于图II.1所示的顺序使用，取决于技术（例如[b-IEEE 802.1X]、[b-IETF RFC 4058]等）和使用的配置。

1. 在网络附加过程的第一阶段，对CPE进行认证和授权。认证过程采用第6、7、8段描述的机制和身份进行。这说明采用的是线路认证和/或接入认证。适用的标识符为用户或CPE标识符提供的用户标识符和凭证。第1步还包括根据传输订阅配置文件，对网络访问进行授权。可从家庭NGN网络下载与QoS等相关的特定传输订阅配置文件至访问的NGN网络（从TAA-FE-server到TAA-FE-proxy模式）。当认证成功，且CPE被授权使用接入网资源，则基于传输订阅配置文件执行接入网配置。这还说明，需要通过Nc参考点，将认证用户特定传输订阅配置文件信息转发至TLM-FE。配置文件信息至少包括逻辑连接标识符（即线路ID）、传输订阅用户标识符和传输资源订阅信息—该信息可以从家庭NGN网络下载的QoS配置文件，或者默认配置文件，以及边缘PE-FE设备的身份识别。

注1 – 1步可在IP地址分配流程（第2步）之前或期间发生

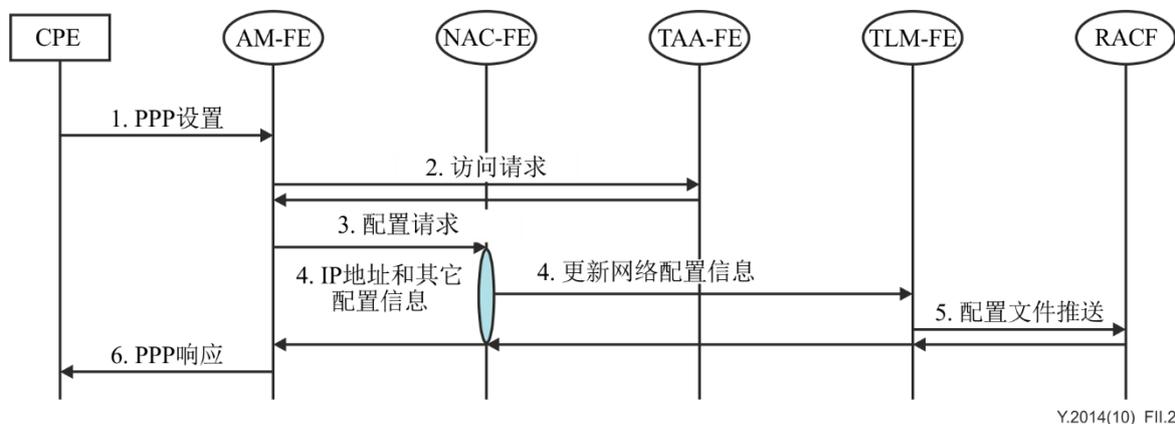
- 以动态方式向CPE提供IP地址和IP配置信息。在第2步期间，NAC-FE分配IP配置信息。NAC-FE通过TC-T1参考点，从信令接收逻辑连接标识符（即线路ID），并在指配的IP配置信息和逻辑连接标识符之间创建映射。该映射信息通过Ne参考点转发至TLM-FE。TLM-FE将该信息与传输预定用户标识符和传输预定配置文件相关联，并通过Ru参考点，将此信息推送至RACF。RACF根据接收到的发自TLM-FE的传输订阅配置文件信息来配置其功能。
- HGWC-FE可配置HGW参数。
- NGN服务控制功能通过S-TC1参考点，从TLM-FE检索位置信息。若NGN服务控制功能需要访问不同域的位置信息，检索位置信息的信令需要通过检索该信息的NGN服务控制功能位于相同网络中的TLM-FE代理来转发。检索位置信息的主要参数是传输订阅用户标识符和/或者NACF分配给CPE的IP地址。

注2 – 欲进一步了解关于移动附加的流程的信息，请参阅[ITU-T Y.2018]第7.2段。

II.2 基于PPP的认证

本段提供了应用PPP时NACF的示例信息流[b-IETF RFC 1661]。这些示例并未打算涵盖NACF在基于PPP的认证中的完整功能。

注 – 仅为示例。



Y.2014(10)_FII.2

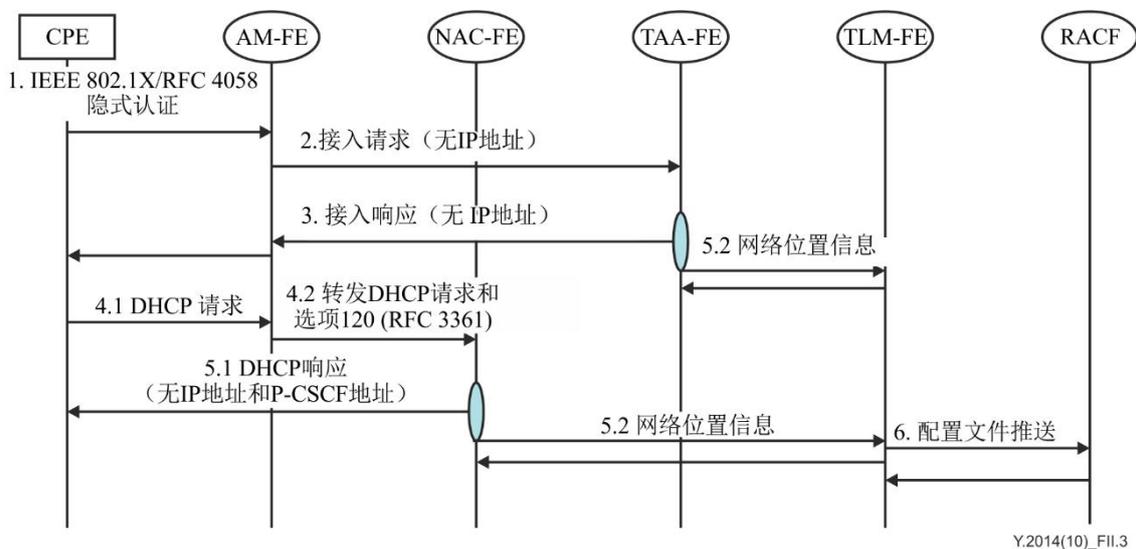
图II.2 – 基于PPP的网络附件

- CPE发起PPP请求，以申请IP地址。PPP用于接入和线路识别。
- AM-FE中继将PPP请求转换为对TAA-FE进行认证的接入请求。
- AM-FE向NAC-FE发出配置请求，以获取IP地址和其他参数，在这种情境下，包括NGN业务控制功能的IP地址（例如P-CSCF）。
- NAC-FE分配IP地址，并对AM-FE做出回应。NAC-FE还向TLM-FE发送指配的IP地址、线路ID和边缘PE-FE设备身份验证的绑定信息。

5. TLM-FE通过Ru参考点向RACF推动绑定信息。
6. AM-FE向CPE发送PPP回应，包括分配的IP以及其他参数，包括NGN服务控制的IP地址（例如，P-CSCF）。

II.3 DHCP模式

本段提供使用DHCP场景的NACF的信息流示例。这些示例并未打算涵盖NACF在DHCP模式下的完整功能。



图II.3 – 使用[b-IEEE 802.1X]的基于DHCP的网络附件
/[b-IETF RFC 4058]/隐式接入认证

1. CPE发起基于[b-IEEE 802.1X]/[b-IETF RFC 4058]的认证。或者，在游牧性不适用的情况下，线路认证可被隐式执行。
2. AM-FE联系TAA-FE进行认证。
3. 在成功认证之后，TAA-FE使用认证结果来做出响应。TAA-FE将CPE被认证的消息告知TLM-FE。
4. CPE使用DHCP请求来请求获取IP地址（根据流程4.1），并通过DHCP选项120请求NGN业务控制功能（例如P-CSCF）的地址（根据流程4.2）。该请求由AM-FE中继至操作DHCP服务器的NAC-FE。
5. NAC-FE为CPE分配IP地址并做出响应。NAC-FE还把将IP地址分配给3）中指示的CPE的消息通知TLM-FE。
6. TLM-FE通过Ru参考点，向RACF推送分配的IP地址、线路ID和边缘PE-FE设备身份验证之间的绑定信息。

NAC-FE提供NGN服务控制功能联络点（例如P-CSC-FE）的FQDN或IP地址，由AM-FE中继至CPE。

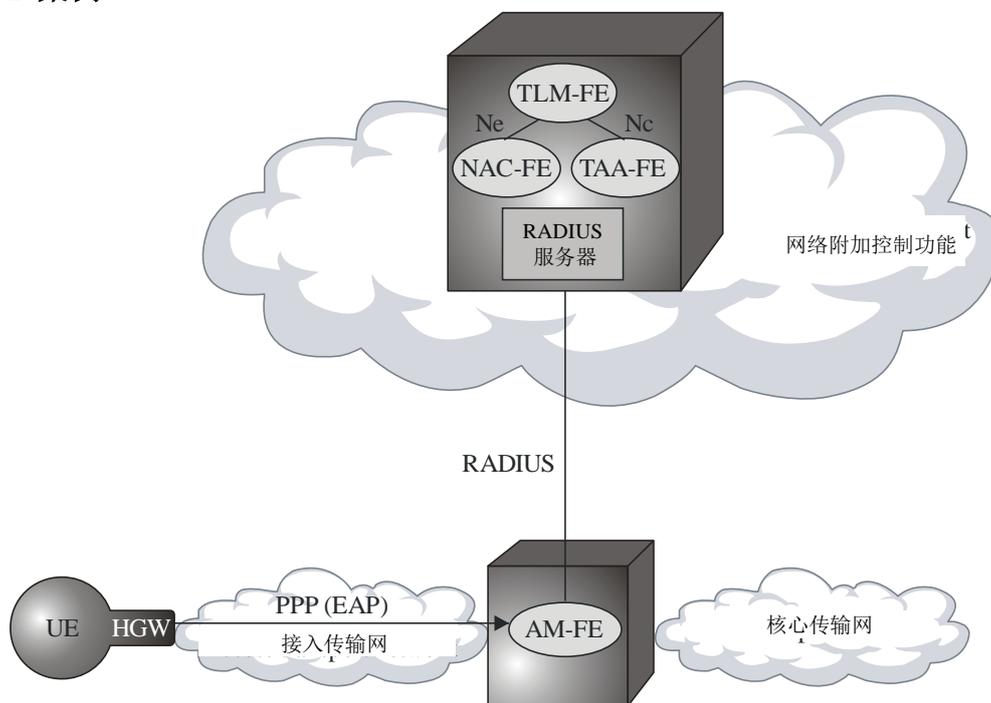
附录III

物理配置

(本附录不构成本建议书的组成部分)

本附录参考EAP [b-IETF RFC 3748]作为认证方法。NACF使用哪种身份验证机制有待进一步研究。

III.1 PPP 案例

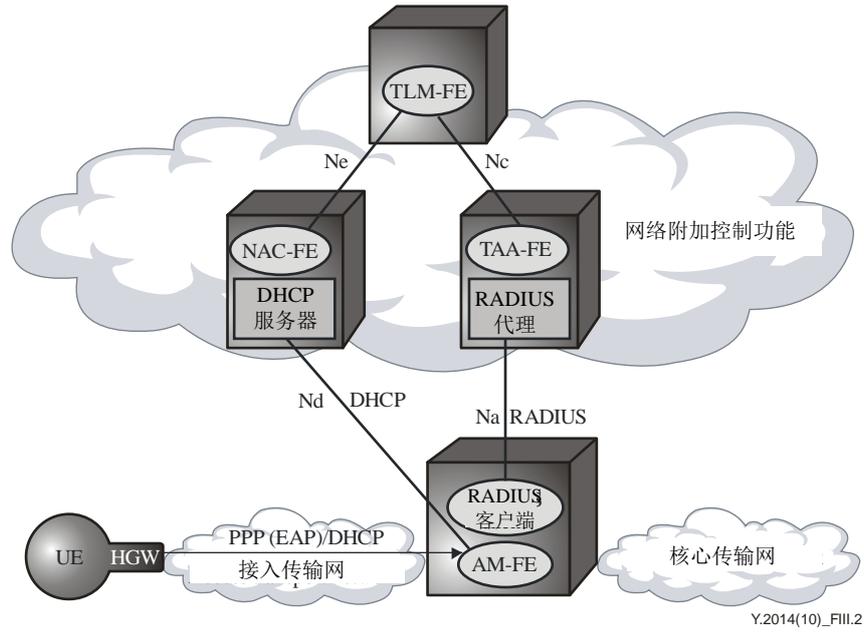


注-为简单起见，未展示RACF接口。

Y.2014(10)_FIII.1

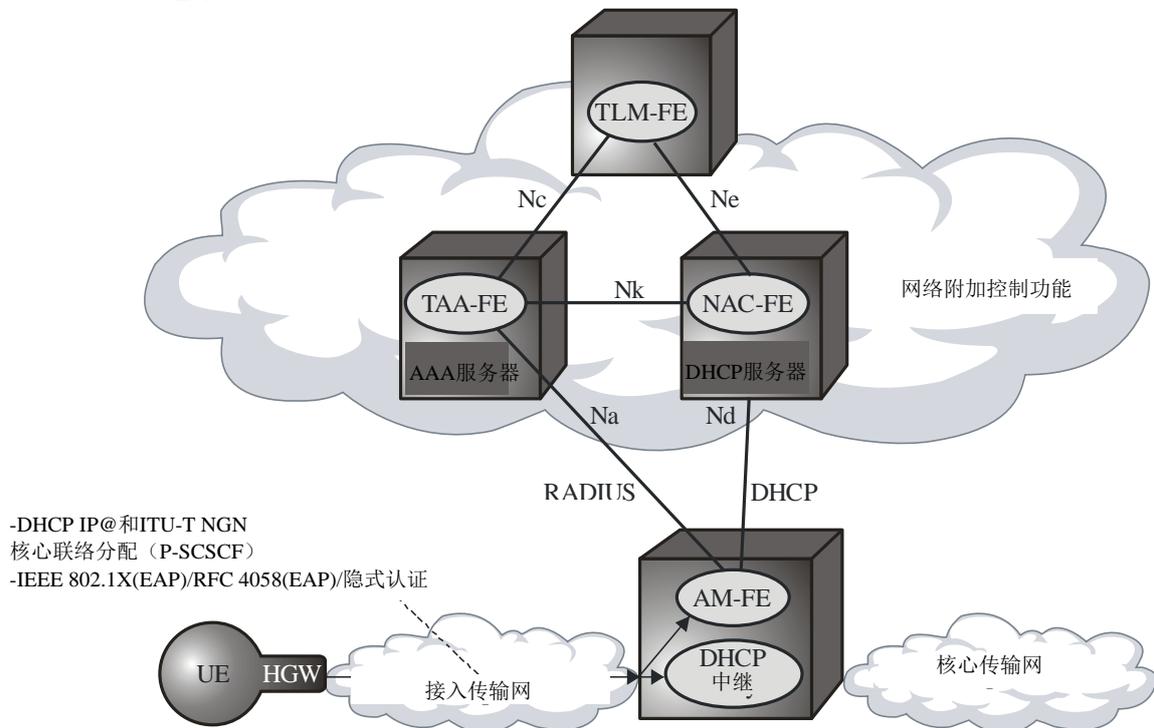
图III.1 – 基于PPP的配置

III.2 包含DHCP配置的PPP



图III.2 – 使用基于DHCP的IP配置的基于PPP的配置（到HGW的NGN服务功能联络点的分配）

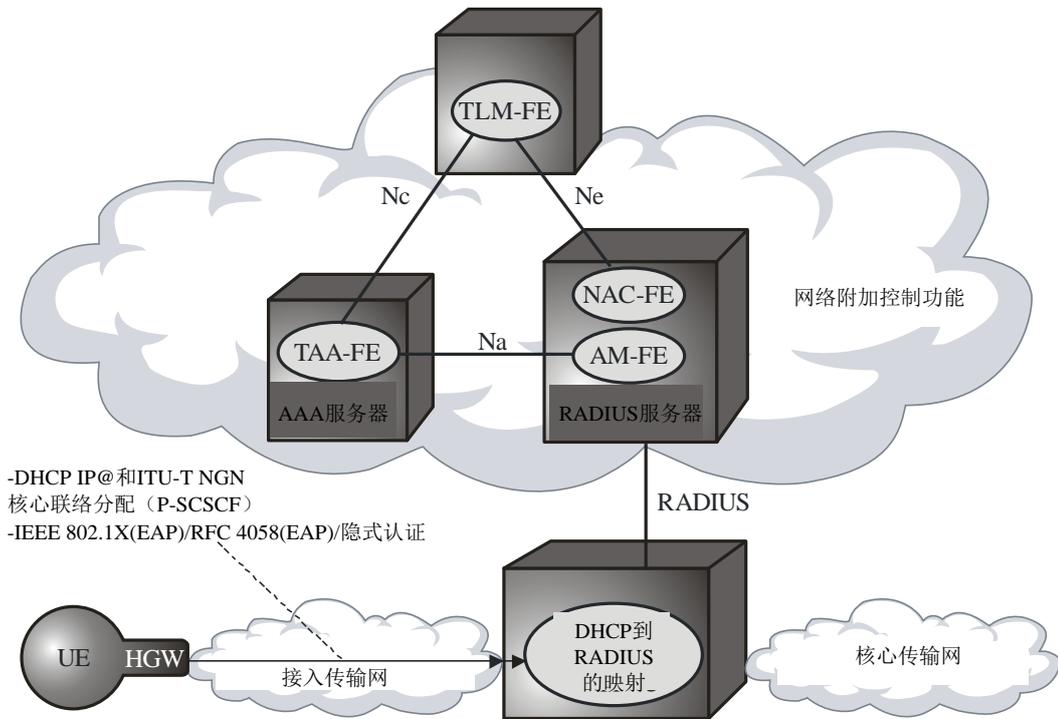
III.3 DHCP（选项1）



注-为简单起见，未展示RACF接口。

图III.3 – 基于DHCP的配置（选项1）

III.4 DHCP（选项2）



注-为简单起见，未展示RACF接口。

Y.2014(10)_FIII.4

图III.4 – 基于DHCP的配置（选项2）

III.5 基于PANA的配置

在基于DHCP的实现中，可通过使用在IETF [IETF RFC 4058]中定义的PANA（网络接入认证承载协议），在IP层提供用户认证。此IP协议承载安装在终端用户设备中的PANA客户端（PaC）和传输面板中的PANA认证代理（PAA）之间的EAP [b-IETF RFC 3748]。此PANA信令经过一个控制未授权用户对网络的访问的执行点（EP）。

PAA咨询认证服务器，以验证PaC的凭证和权限。若认证服务器和PAA在同一物理设备上，则一个API就足够进行交互。若它们被分开，则可使用RADIUS或Diameter用于交互。

一旦用户成功通过认证并被授权访问网络，PAA就向EP发送配置信息，以修改应用于终端用户设备的输入和输出流量上的每个数据包的执行策略（即，过滤器）。

图III.5描述了一种基于PANA的NACF物理配置的实现：

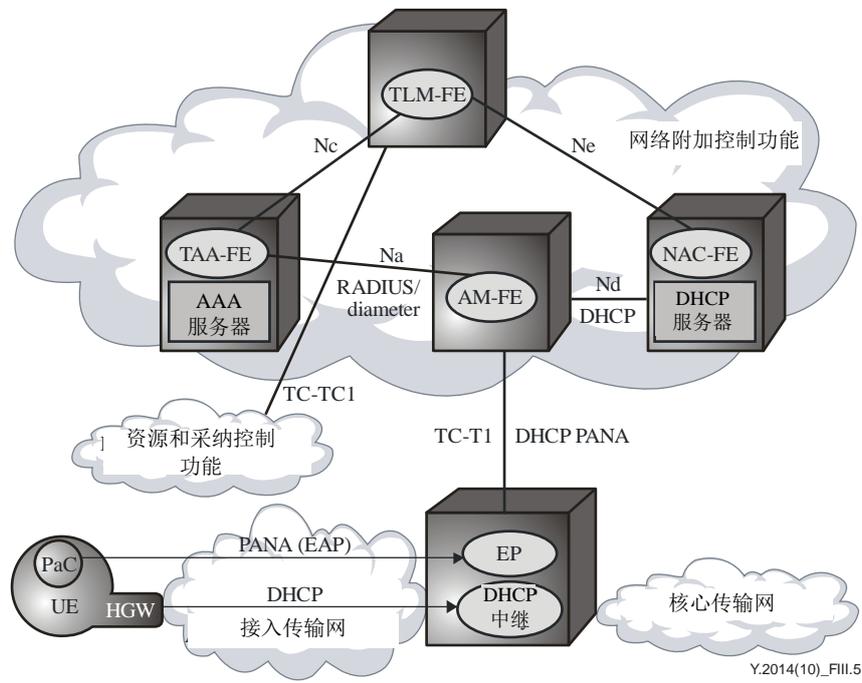


图 III.5 – 基于PANA的配置

附录IV

ITU-T Y.2014建议书和ETSI ES 282 004 v2.0.0之间的整体映射

(本附录不构成本建议书的组成部分)

下表提供了本建议书中指定的NACF与[b ETSI ES 282 004]中指定的网络附件子系统(NASS)之间的高级映射。

表 IV.1

ETSI ES 282 004 v2.0.0	建议书ITU-T Y.2014
功能实体	
ARF	AR-FE [ITU-T Y.2012]
AMF	AM-FE
NACF	NAC-FE
UAAF	TAA-FE
PBDF	TUP-FE
CLF	TLM-FE
CNGCF	HGWC-FE
CNG	HGW
参考点	
NACF-AMF: a1	NAC-FE/AM-FE: Nd
NACF-CLF: a2	NAC-FE/TLM-FE: Ne
AMF-UAAF: a3	AM-FE/TAA-FE: Na
UAAF-CLF: a4	TAA-FE/TLM-FE: Nc
UAAF-PBDF:未定义	TAA-FE/TUP-FE: Nb. 详情有待进一步研究。
NACF-UAAF:未定义	NAC-FE/TAA-FE: Nk. 详情有待进一步研究。
ARF-AMF: e1	AR-FE-AM-FE: TC-T1
UE-ARF: e1	CPE/AR-FE: T-U1 [ITU-T Y.2012]
AF (e.g., P-CSCF)-CLF: e2	服务控制功能(SCF)/TLM-FE: S-TC1
CLF-CLF: e2	TLM-FE/TLM-FE: Ng
CNGCF-CLF: e2	HGWC-FE/TLM-FE: Nx
CNGCF-UE: e3	HGWC-FE/CPE: TC-Ux
CLF-RACS: e4	TLM-FE/RACF: Ru
UAAF-UAAF: e5	TAA-FE/TAA-FE: Ni

参考文件

- [b-3GPP TS 23.401] 3GPP TS 23.401 (in force), *General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access.*
- [b-3GPP TS 23.402] 3GPP TS 23.402 (in force), *Architecture enhancements for non-3GPP accesses.*
- [b-DSL Forum TR-069] DSL Forum TR-069 (2006), *CPE WAN Management Protocol v1.1.*
- [b-IEEE 802.1X] IEEE 802.1X – 2004, *IEEE Standard for Local and Metropolitan Area Networks – Port-Based Network Access Control.*
- [b-IETF RFC 4058] IETF RFC 4058 (2005), *Protocol for Carrying Authentication for Network Access (PANA) Requirements.*
- [b-ETSI ES 282 004] ETSI ES 282 004 v2.0.0 (2008-02), *Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Functional Architecture; Network Attachment Sub System (NASS).*
- [b-IETF RFC 783] IETF RFC 783 (1981), *The TFTP Protocol (Revision 2).*
- [b-IETF RFC 959] IETF RFC 959 (1985), *File Transfer Protocol (FTP).*
- [b-IETF RFC 1661] IETF RFC 1661 (1994), *The Point-to-Point Protocol (PPP).*
- [b-IETF RFC 2131] IETF RFC 2131 (1997), *Dynamic Host Configuration Protocol.*
- [b-IETF RFC 2616] IETF RFC 2616 (1999), *Hypertext Transfer Protocol – HTTP/1.1.*
- [b-IETF RFC 2865] IETF RFC 2865 (2000), *Remote Authentication Dial In User Service (RADIUS).*
- [b-IETF RFC 3220] IETF RFC 3220 (2002), *IP Mobility Support for IPv4.*
- [b-IETF RFC 3588] IETF RFC 3588 (2003), *Diameter Base Protocol.*
- [b-IETF RFC 3748] IETF RFC 3748 (2004), *Extensible Authentication Protocol (EAP).*

ITU-T系列建议书

A系列	ITU-T工作的组织
D系列	资费和结算原则以及国际电信/ICT经济 and 政策问题
E系列	综合网络运行、电话业务、业务运行和人为因素
F系列	非话电信业务
G系列	传输系统和媒质、数字系统和网络
H系列	视听和多媒体系统
I系列	综合业务数字网
J系列	有线网和电视、声音节目及其他多媒体信号的传输
K系列	干扰的防护
L系列	环境和ICT、气候变化、电子废物、节能；线缆和外部设备的其他组件的建设、安装和保护
M系列	电信管理，包括电信网管管理和网络维护
N系列	维护：国际声音节目和电视传输电路
O系列	测量设备技术规程
P系列	电话传输质量、电话装置、本地线路网络
Q系列	交换和信令以及相关的测量与测试
R系列	电报传输
S系列	电报业务终端设备
T系列	远程信息处理业务的终端设备
U系列	电报交换
V系列	电话网上的数据通信
X系列	数据网络、开放系统通信和安全
Y系列	全球信息基础设施、互联网协议问题、下一代网络、物联网和智慧城市
Z系列	用于电信系统的语言和一般软件问题