

Международный союз электросвязи

# МСЭ-Т

СЕКТОР СТАНДАРТИЗАЦИИ  
ЭЛЕКТРОСВЯЗИ МСЭ

# Y.2014

(03/2010)

СЕРИЯ Y: ГЛОБАЛЬНАЯ ИНФОРМАЦИОННАЯ  
ИНФРАСТРУКТУРА, АСПЕКТЫ ПРОТОКОЛА  
ИНТЕРНЕТ И СЕТИ ПОСЛЕДУЮЩИХ ПОКОЛЕНИЙ

Сети последующих поколений – Структура  
и функциональные модели архитектуры

---

**Функции управления присоединением сетей  
в сетях последующих поколений**

Рекомендация МСЭ-Т Y.2014

## РЕКОМЕНДАЦИИ МСЭ-Т СЕРИИ Y

## ГЛОБАЛЬНАЯ ИНФОРМАЦИОННАЯ ИНФРАСТРУКТУРА, АСПЕКТЫ ПРОТОКОЛА ИНТЕРНЕТ И СЕТИ ПОСЛЕДУЮЩИХ ПОКОЛЕНИЙ

<b>ГЛОБАЛЬНАЯ ИНФОРМАЦИОННАЯ ИНФРАСТРУКТУРА</b>	
Общие положения	Y.100–Y.199
Услуги, приложения и промежуточные программные средства	Y.200–Y.299
Сетевые аспекты	Y.300–Y.399
Интерфейсы и протоколы	Y.400–Y.499
Нумерация, адресация и присваивание имен	Y.500–Y.599
Эксплуатация, управление и техническое обслуживание	Y.600–Y.699
Безопасность	Y.700–Y.799
Рабочие характеристики	Y.800–Y.899
<b>АСПЕКТЫ ПРОТОКОЛА ИНТЕРНЕТ</b>	
Общие положения	Y.1000–Y.1099
Услуги и приложения	Y.1100–Y.1199
Архитектура, доступ, возможности сетей и административное управление ресурсами	Y.1200–Y.1299
Транспортирование	Y.1300–Y.1399
Взаимодействие	Y.1400–Y.1499
Качество обслуживания и сетевые показатели качества	Y.1500–Y.1599
Сигнализация	Y.1600–Y.1699
Эксплуатация, управление и техническое обслуживание	Y.1700–Y.1799
Начисление платы	Y.1800–Y.1899
IPTV по NGN	Y.1900–Y.1999
<b>СЕТИ ПОСЛЕДУЮЩИХ ПОКОЛЕНИЙ</b>	
<b>Структура и функциональные модели архитектуры</b>	<b>Y.2000–Y.2099</b>
Качество обслуживания и рабочие характеристики	Y.2100–Y.2199
Аспекты обслуживания: возможности услуг и архитектура услуг	Y.2200–Y.2249
Аспекты обслуживания: взаимодействие услуг и СПП	Y.2250–Y.2299
Нумерация, присваивание имен и адресация	Y.2300–Y.2399
Управление сетью	Y.2400–Y.2499
Архитектура и протоколы сетевого управления	Y.2500–Y.2599
Пакетные сети	Y.2600–Y.2699
Безопасность	Y.2700–Y.2799
Обобщенная мобильность	Y.2800–Y.2899
Открытая среда операторского класса	Y.2900–Y.2999
<b>БУДУЩИЕ СЕТИ</b>	<b>Y.3000–Y.3499</b>
<b>ОБЛАЧНЫЕ ВЫЧИСЛЕНИЯ</b>	<b>Y.3500–Y.3999</b>
<b>ИНТЕРНЕТ ВЕЩЕЙ И "УМНЫЕ" ГОРОДА И СООБЩЕСТВА</b>	
Общие положения	Y.4000–Y.4049
Определения и терминология	Y.4050–Y.4099
Требования и сценарии использования	Y.4100–Y.4249
Инфраструктура, возможность установления соединений и сети	Y.4250–Y.4399
Структуры, архитектуры и протоколы	Y.4400–Y.4549
Услуги, приложения, вычисления и обработка данных	Y.4550–Y.4699
Управление, контроль и рабочие характеристики	Y.4700–Y.4799
Идентификация и безопасность	Y.4800–Y.4899
Анализ и оценка	Y.4900–Y.4999

Для получения более подробной информации просьба обращаться к перечню Рекомендаций МСЭ-Т.

### Функции управления присоединением сетей в сетях последующих поколений

#### Резюме

В Рекомендации МСЭ-Т Y.2014 описывается компонент функциональной архитектуры СПП, содержащий функции контроля подсоединения к сети (NACF). В настоящей Рекомендации также определяются соответствующие сценарии доступа, относящиеся к NACF.

В частности, в настоящее издание включены расширения к Рекомендации МСЭ-Т Y.2014 (2008 г.) для решения вопросов, связанных с многоадресной передачей и мобильностью при поддержке услуги IPTV и услуги мобильности соответственно.

#### Хронологическая справка

Издание	Рекомендация	Утверждение	Исследовательская комиссия	Уникальный идентификатор*
1.0	МСЭ-Т Y.2014	07.05.2008 г.	13-я	<a href="http://handle.itu.int/11.1002/1000/9348">11.1002/1000/9348</a>
2.0	МСЭ-Т Y.2014	16.03.2010 г.	13-я	<a href="http://handle.itu.int/11.1002/1000/10711">11.1002/1000/10711</a>

#### Ключевые слова

Функциональная архитектура, подсоединение к сети, СПП.

---

\* Для получения доступа к Рекомендации наберите в адресном поле вашего браузера URL: <http://handle.itu.int/>, после которого следует уникальный идентификатор Рекомендации. Например, <http://handle.itu.int/11.1002/1000/11830-en>.

## ПРЕДИСЛОВИЕ

Международный союз электросвязи (МСЭ) является специализированным учреждением Организации Объединенных Наций в области электросвязи и информационно-коммуникационных технологий (ИКТ). Сектор стандартизации электросвязи МСЭ (МСЭ-Т) – постоянный орган МСЭ. МСЭ-Т отвечает за изучение технических, эксплуатационных и тарифных вопросов и за выпуск Рекомендаций по ним в целях стандартизации электросвязи на всемирной основе.

На Всемирной ассамблее по стандартизации электросвязи (ВАСЭ), которая проводится каждые четыре года, определяются темы для изучения исследовательскими комиссиями МСЭ-Т, которые, в свою очередь, вырабатывают Рекомендации по этим темам.

Утверждение Рекомендаций МСЭ-Т осуществляется в соответствии с процедурой, изложенной в Резолюции 1 ВАСЭ.

В некоторых областях информационных технологий, которые входят в компетенцию МСЭ-Т, необходимые стандарты разрабатываются на основе сотрудничества с ИСО и МЭК.

## ПРИМЕЧАНИЕ

В настоящей Рекомендации термин "администрация" используется для краткости и обозначает как администрацию электросвязи, так и признанную эксплуатационную организацию.

Соблюдение положений данной Рекомендации осуществляется на добровольной основе. Однако данная Рекомендация может содержать некоторые обязательные положения (например, для обеспечения функциональной совместимости или возможности применения), и в таком случае соблюдение Рекомендации достигается при выполнении всех указанных положений. Для выражения требований используются слова "следует", "должен" (shall) или некоторые другие обязывающие выражения, такие как "обязан" (must), а также их отрицательные формы. Употребление таких слов не означает, что от какой-либо стороны требуется соблюдение положений данной Рекомендации.

## ПРАВА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

МСЭ обращает внимание на вероятность того, что практическое применение или выполнение настоящей Рекомендации может включать использование заявленного права интеллектуальной собственности. МСЭ не занимает какую бы то ни было позицию относительно подтверждения, действительности или применимости заявленных прав интеллектуальной собственности независимо от того, доказываются ли такие права членами МСЭ или другими сторонами, не относящимися к процессу разработки Рекомендации.

На момент утверждения настоящей Рекомендации МСЭ не получил извещения об интеллектуальной собственности, защищенной патентами, которые могут потребоваться для выполнения настоящей Рекомендации. Однако те, кто будет применять Рекомендацию, должны иметь в виду, что вышесказанное может не отражать самую последнюю информацию, и поэтому им настоятельно рекомендуется обращаться к патентной базе данных БСЭ по адресу <http://www.itu.int/ITU-T/ipr/>.

© ITU 2022

Все права сохранены. Ни одна из частей данной публикации не может быть воспроизведена с помощью каких бы то ни было средств без предварительного письменного разрешения МСЭ.

## СОДЕРЖАНИЕ

	Стр.
1 Сфера применения .....	1
2 Справочные документы .....	1
3 Определения .....	1
3.1 Термины, определенные в других документах .....	1
3.2 Термины, определенные в настоящей Рекомендации .....	2
4 Сокращения и акронимы .....	2
5 Соглашения по терминологии .....	4
6 Общее описание .....	5
6.1 Высокоуровневый обзор функций .....	5
6.2 Высокоуровневые концепции NACF .....	6
6.3 Мобильность, кочевничество .....	6
6.4 Регистрация на уровне сети доступа.....	6
7 Функциональная архитектура.....	7
7.1 Обзор.....	7
7.2 Функциональные объекты .....	9
8 Эталонные точки .....	18
8.1 Внутренние эталонные точки NACF .....	18
8.2 Эталонная точка между NACF и функциями управления ресурсами и допуском (RACF).....	33
8.3 Эталонная точка между NACF и функциями управления обслуживанием .....	34
8.4 Эталонные точки между NACF и CPE .....	37
8.5 Эталонные точки между NACF и функциями управления мобильностью и контроля мобильности (MMCF).....	38
9 Соображения безопасности.....	38
Дополнение I – Отображение на сетевые роли.....	39
Дополнение II – Информационные потоки.....	42
II.1 Высокоуровневые информационные потоки .....	42
II.2 Аутентификация на основе PPP .....	43
II.3 Режим DHCP .....	44
Дополнение III – Физические конфигурации .....	46
III.1 Случай PPP .....	46
III.2 Конфигурация PPP с DHCP .....	47
III.3 DHCP (вариант 1).....	47
III.4 DHCP (вариант 2).....	48
III.5 Конфигурация на основе PANA .....	48
Дополнение IV – Общее соответствие между Рекомендацией МСЭ-Т Y.2014 и стандартом ETSI ES 282 004 v2.0.0.....	50
Библиография .....	51



# Рекомендация МСЭ-Т Y.2014

## Функции управления присоединением сетей в сетях последующих поколений

### 1 Сфера применения

В настоящей Рекомендации описывается компонент функциональной архитектуры СПП, содержащий функции контроля подсоединения к сети (NACF). В ней также определяются соответствующие сценарии доступа, относящиеся к NACF.

В настоящую Рекомендацию включены эталонные точки для взаимодействия с другими компонентами СПП (RACF, MMCF и SCF), обеспечивающими функции подсоединения к сети для фиксированного, перемещаемого/перемещающегося и мобильного оконечного оборудования/пользователя.

### 2 Справочные документы

Указанные ниже Рекомендации МСЭ-Т и другие справочные документы содержат положения, которые путем ссылки на них в данном тексте составляют положения настоящей Рекомендации. На момент публикации указанные издания были действующими. Все Рекомендации и другие источники могут подвергаться пересмотру, поэтому всем пользователям данной Рекомендации предлагается изучить возможность применения последнего издания Рекомендаций и других справочных документов, перечисленных ниже. Список действующих в настоящее время Рекомендаций МСЭ-Т регулярно публикуется. Ссылка на документ в данной Рекомендации не придает ему как отдельному документу статус Рекомендации.

- |                |   |
|----------------|---|
| [ITU-T Q.1761] | Recommendation ITU-T Q.1761 (2004), <i>Principles and requirements for convergence of fixed and existing IMT-2000 systems.</i>          |
| [ITU-T X.800]  | Рекомендация МСЭ-Т X.800 (1991 г.), <i>Архитектура безопасности для взаимосвязи открытых систем для приложений МККТТ.</i>               |
| [ITU-T Y.1541] | Рекомендация МСЭ-Т Y.1541 (2006 г.), <i>Требования к сетевым показателям качества для служб, основанных на протоколе IP.</i>            |
| [ITU-T Y.1910] | Рекомендация МСЭ-Т Y.1910 (2008 г.), <i>Функциональная архитектура IPTV.</i>  |
| [ITU-T Y.2012] | Recommendation ITU-T Y.2012 (2006), <i>Functional requirements and architecture of the NGN release 1.</i>                               |
| [ITU-T Y.2018] | Recommendation ITU-T Y.2018 (2009), <i>Mobility management and control framework and architecture within the NGN transport stratum.</i> |
| [ITU-T Y.2021] | Рекомендация МСЭ-Т Y.2021 (2006 г.), <i>IMS для сетей последующих поколений.</i>  |
| [ITU-T Y.2111] | Рекомендация МСЭ-Т Y.2111 (2008 г.), <i>Функции управления ресурсами и установлением соединений в сетях последующих поколений.</i>      |
| [ITU-T Y.2701] | Рекомендация МСЭ-Т Y.2701 (2007 г.), <i>Требования к безопасности для сетей последующих поколений версии 1.</i>                         |
| [ITU-T Y.2702] | Рекомендация МСЭ-Т Y.2702 (2008 г.), <i>Требования к аутентификации и авторизации для СПП варианта 1.</i>                               |

### 3 Определения

#### 3.1 Термины, определенные в других документах

В настоящей Рекомендации используются следующие термины, определенные в других документах.

**3.1.1 авторизация (authorization) [ITU-T X.800]:** Предоставление прав, которое включает предоставление доступа на основании прав доступа.

ПРИМЕЧАНИЕ. – В некоторых контекстах, например в службах экстренного вызова, авторизация возможна без обязательной аутентификации или идентификации.

**3.1.2 кочевничество (nomadism) [ITU-T Q.1761]:** Возможность для пользователя изменять свой пункт доступа к сети после перемещения; при изменении пункта доступа к сети сеанс обслуживания пользователя полностью останавливается и затем вновь начинается, то есть эстафетная передача вызова невозможна. Считается, что обычный способ использования следующий: пользователь завершает свой сеанс обслуживания до перемещения в другой пункт доступа или смены терминала. Именно о такой мобильности идет речь в случае конвергенции фиксированной и подвижной связи.

## 3.2 Термины, определенные в настоящей Рекомендации

В настоящей Рекомендации определяются следующие термины.

**3.2.1 аутентификация (authentication):** Свойство, посредством которого с требуемой гарантией устанавливается верная идентичность объекта или участвующей стороны. Стороной, проходящей аутентификацию, может являться пользователь, абонент, оператор домашней сети или обслуживающая сеть.

**3.2.2 оборудование в помещении пользователя (customer premises equipment) (CPE):** Одно или несколько устройств, позволяющие пользователю получать доступ к услугам СПП.

ПРИМЕЧАНИЕ. – Сюда входят контролируемые пользователем устройства, например домашний шлюз (HGW), оконечное оборудование (TE) и т. д., но не устройства под контролем сети, такие как шлюзы доступа.

**3.2.3 явная аутентификация (explicit authentication):** Аутентификация, при которой требуется, чтобы проходящая ее сторона выполнила соответствующую процедуру (для подтверждения своей заявленной идентичности).

**3.2.4 домашний шлюз (home gateway) (HGW):** Шлюз между сетью в помещении пользователя (CPN) и сетью доступа.

ПРИМЕЧАНИЕ. – Простейшей разновидностью домашнего шлюза является модем, подключенный через мост или маршрутизатор, а более сложным его вариантом – интегрированное устройство доступа.

**3.2.5 неявная аутентификация (implicit authentication):** Аутентификация на основе доверительных отношений, уже установленных между двумя сторонами, либо на основе одного или нескольких элементов данных, полученных на выходе уже проведенной между двумя сторонами процедуры аутентификации.

**3.2.6 идентификация линии (line identification):** Процесс установления идентификатора линии на основе доверенной конфигурации.

## 4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы.

AAA	Authentication, Authorization and Accounting	Аутентификация, авторизация и учет
ABG-FE	Access Border Gateway Functional Entity	Функциональный объект пограничного шлюза доступа
ACL	Access Control List	Список управления доступом
AM-FE	Access Management Functional Entity	Функциональный объект управления доступом
AN	Access Network	Сеть доступа
AN-FE	Access Node Functional Entity	Функциональный объект узла доступа
API	Application Programming Interface	Интерфейс прикладного программирования
AR-FE	Access Relay Functional Entity	Функциональный объект ретрансляции для обеспечения доступа

ATM	Asynchronous Transfer Mode	АПП	Асинхронный режим передачи
CoS	Class of Service		Класс обслуживания
CPE	Customer Premises Equipment		Оборудование в помещении пользователя
CPN	Customer Premises Network		Сеть в помещении пользователя
DHCP	Dynamic Host Configuration Protocol		Протокол динамической конфигурации хост-компьютера
DNS	Domain Name Server		Сервер наименований доменов
EAP	Extensible Authentication Protocol		Расширяемый протокол аутентификации
EN-FE	Edge Node Functional Entity		Функциональный объект периферийного узла
FQDN	Fully Qualified Domain Name		Полное наименование домена
FTP	File Transfer Protocol		Протокол передачи файлов
GTP	GPRS Tunnelling Protocol		Протокол туннелирования GPRS
HDC-FE	Handover Decision and Control Functional Entity		Функциональный объект решения об эстафетной передаче и управления ею
HGW	Home Gateway		Домашний шлюз
HGWC-FE	Home Gateway Configuration Functional Entity		Функциональный объект конфигурации домашнего шлюза
HTTP	Hyper Text Transfer Protocol		Протокол передачи гипертекста
ID	Identifier		Идентификатор
IMS	IP Multimedia Subsystem		Мультимедийная IP-подсистема
IP	Internet Protocol		Протокол Интернет
IPTV	Internet Protocol Television		Телевидение на основе протокола Интернет
MAC	Media Access Control		Управление доступом к среде
MIP	Mobile Internet Protocol		Мобильный протокол Интернет
MLM-FE	Mobile Location Management Functional Entity		Функциональный объект управления на основе местоположения мобильного устройства
MLM-FE(P)	An instance of the MLM-FE performing the proxy mobile location management role		Экземпляр MLM-FE, выступающий в роли прокси-сервера управления на основе местоположения мобильного устройства
MMCF	Mobility Management and Control Functions		Функции управления мобильностью и контроля мобильности
MPLS	Multi-Protocol Label Switching		Многопротокольная коммутация с использованием меток
NACF	Network Attachment Control Functions		Функции контроля подсоединения к сети
NAC-FE	Network Access Configuration Functional Entity		Функциональный объект конфигурации доступа к сети
NGN	Next Generation Network	СПП	Сеть последующих поколений

NID-FE	Network Information Distribution Functional Entity		Функциональный объект распределения сетевой информации
PAA	PANA Authentication Agent		Агент аутентификации PANA
PaC	PANA Client		Клиент PANA
PANA	Protocol for Carrying Authentication for Network Access		Протокол для переноса аутентификации в целях доступа к сети
P-CSCF	Proxy-Call Session Control Function		Прокси-функция управления сеансом вызова
PD-FE	Policy Decision Functional Entity		Функциональный объект принятия решения в соответствии с политикой
PE-FE	Policy Enforcement Functional Entity		Функциональный объект обеспечения выполнения политики
PIA	Persistent IP Address		Постоянный IP-адрес
PPP	Point-to-Point Protocol		Протокол передачи из пункта в пункт
QoS	Quality of Service		Качество обслуживания
RACF	Resource and Admission Control Functions		Функции управления ресурсами и допуском
SADS	Service and Application Discovery and Selection		Обнаружение и выбор услуг и приложений
SCF	Service Control Functions		Функции управления обслуживанием
SLA	Service Level Agreement		Соглашение об уровне обслуживания
SUP-FE	Service User Profile Functional Entity		Функциональный объект профиля пользователя услуги
TAA-FE	Transport Authentication and Authorization Functional Entity		Функциональный объект аутентификации и авторизации транспортирования
TE	Terminal Equipment		Оконечное оборудование
TFTP	Trivial File Transfer Protocol		Простой протокол передачи файлов
TIA	Temporary IP Address		Временный IP-адрес
TLM-FE	Transport Location Management Functional Entity		Функциональный объект управления местоположением транспортирования
TUP-FE	Transport User Profile Functional Entity		Функциональный объект профиля пользователя транспортирования
VC	Virtual Channel		Виртуальный канал
VCI	Virtual Channel Identifier		Идентификатор виртуального канала
VPI	Virtual Path Identifier		Идентификатор виртуального пути
VPN	Virtual Private Network	ВЧС	Виртуальная частная сеть
WLAN	Wireless Local Area Network		Беспроводная локальная сеть

## 5 Соглашения по терминологии

В настоящей Рекомендации какие-либо специальные соглашения по терминологии не используются.

## 6 Общее описание

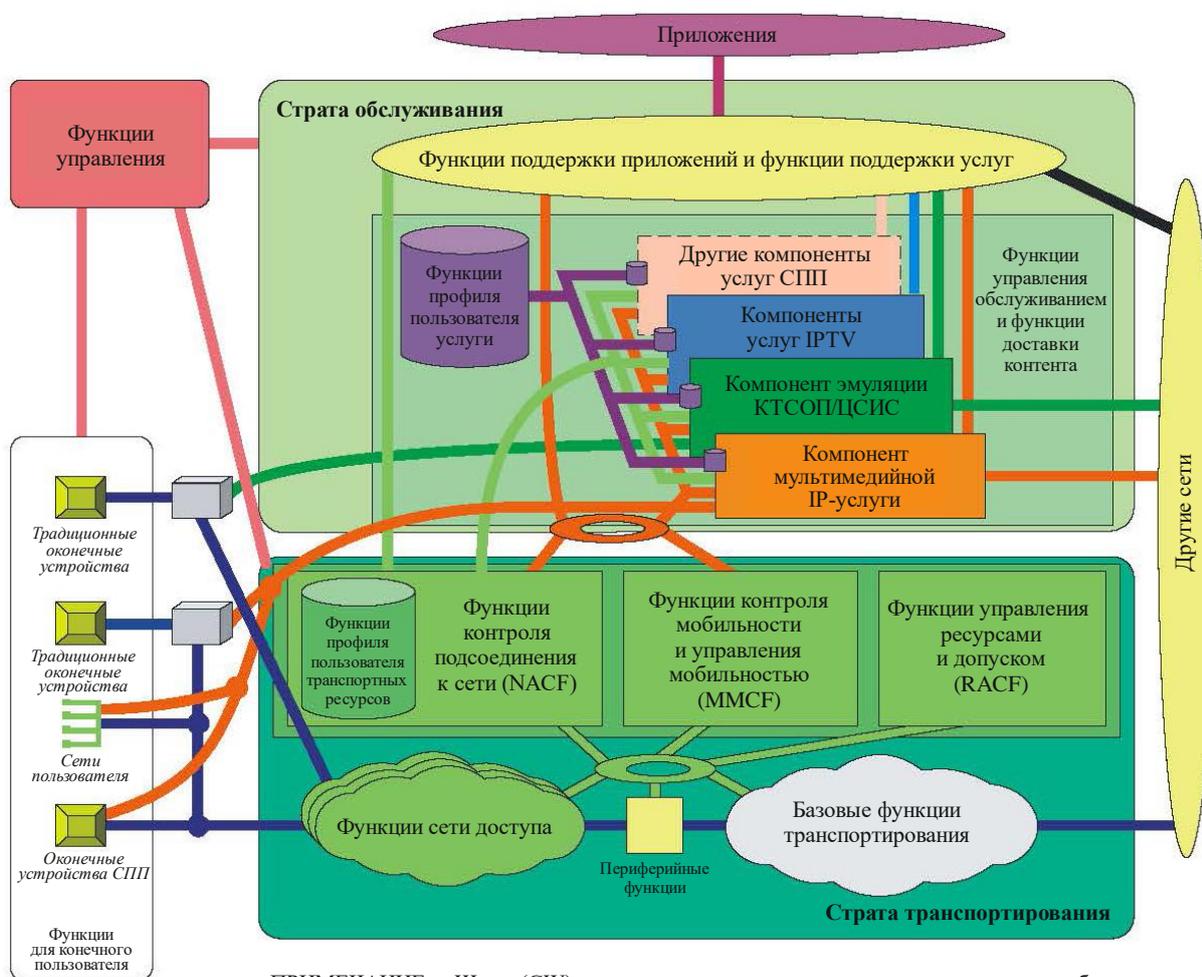
### 6.1 Высокоуровневый обзор функций

NACF предоставляет следующие функциональные возможности:

- динамическую подготовку IP-адресов и других параметров конфигурации CPE;
- с одобрения пользователя – автоматическое обнаружение возможностей CPE и других параметров;
- аутентификацию конечного пользователя и сети на уровне IP (и, возможно, на других уровнях). Осуществляется взаимная аутентификация конечного пользователя и подсоединения к сети;
- авторизацию доступа к сети на основании профилей пользователей;
- настройку сети доступа на основании профилей пользователей;
- управление на основе местоположения на уровне IP.

Упомянутые выше профили пользователей связаны только с подпиской на транспортную сеть доступа и в остальной части настоящей Рекомендации называются "профили абонирования транспортирования".

Место компонента NACF в общей архитектуре СПП описано в [ITU-T Y.2012] и показано здесь на рисунке 1, приведенном для информации.



ПРИМЕЧАНИЕ. – Шлюз (GW) может существовать в страте транспортирования либо в составе функций для конечного пользователя.

Y.2014(10)\_F01

Рисунок 1 – Компоненты СПП, включая NACF

## **6.2 Высокоуровневые концепции NACF**

NACF обеспечивает регистрацию на уровне доступа и инициализацию CPE для доступа к услугам СПП. Кроме того, NACF обеспечивает идентификацию и аутентификацию на уровне сети, управляет пространством IP-адресов сети доступа и аутентифицирует сеансы доступа. NACF также доводит до сведения CPE точки контакта компонентов страны обслуживания СПП.

Подсоединение к сети через NACF основано на учетных данных явной или неявной идентификации и аутентификации пользователя, хранимых в NACF.

## **6.3 Мобильность, кочевничество**

В настоящей Рекомендации функции управления мобильностью, обеспечиваемые NACF, ограничены возможностями перемещения оконечного устройства в различные пункты (точки) и сети доступа (владеть которыми могут разные операторы сетей) и возможностями пользователя применять различное оконечное оборудование, пункты доступа и сети доступа для получения услуг СПП (даже от другого оператора сети).

Под мобильностью в настоящей Рекомендации понимается поддержка эстафетной передачи и непрерывности сеанса между сетями доступа, а также кочевничества; при этом допускается использование возможностей мобильности, предоставляемых в самих сетях доступа.

Архитектура NACF не предполагает каких-либо определенных бизнес-ролей. Однако в целях удовлетворения требований кочевничества, роуминга и мобильности архитектура NACF может быть отображена на различные функциональные сетевые роли, присутствующие в среде фиксированного широкополосного доступа. Влияние требований кочевничества, роуминга и мобильности описывается в Дополнении I.

## **6.4 Регистрация на уровне сети доступа**

Регистрация NACF включает процедуры идентификации, аутентификации и авторизации между CPE и NACF для управления доступом к NACF. Для NACF определено два типа аутентификации – неявная (например, на основе аутентификации линии) и явная (например, на основе EAP [b-IETF RFC 3748]). Чтобы любое решение по аутентификации было возможным, NACF должна быть известна взаимосвязь между идентификаторами и учетными данными, используемыми для аутентификации.

Явная аутентификация осуществляется между CPE и NACF. Для этого требуется, чтобы между ними была выполнена процедура сигнализации. Неявная аутентификация может выполняться NACF на основе идентификации линии связи с CPE. Выбор той или другой формы аутентификации определяется политикой оператора.

Явная и неявная аутентификация могут использоваться как независимые механизмы аутентификации NACF.

### **6.4.1 Неявная аутентификация**

В зависимости от конфигурации сети доступа, особенно в случае сетей проводного широкополосного доступа, возможно, что неявная аутентификация доступа будет опираться только на неявную аутентификацию посредством физической или логической идентификации транспорта уровня 2 (L2). CPE может получать доступ к сети напрямую, без выполнения процедуры явной аутентификации.

Выбор метода неявной аутентификации зависит от политики оператора.

#### **6.4.1.1 Аутентификация линии**

Аутентификация линии – это один из видов неявной аутентификации. Такая аутентификация обеспечивает, чтобы линия доступа была аутентифицирована и к ней был возможен доступ с домашнего шлюза (HGW). Аутентификация линии основана на активации соединения L2 между HGW и сетью доступа.

Аутентификация линии гарантирует, что линия доступа прошла проверку подлинности и к ней возможен доступ с домашнего HGW. Для аутентификации линии используется идентификатор линии. Возможность применения этого вида аутентификации зависит от политики оператора.

## **6.4.2 Явная аутентификация**

Если в роли NGW выступает модем-маршрутизатор, а сеть в помещении пользователя (CPN) представляет собой область частных IP-адресов, аутентификация инициируется NGW. Если NGW представляет собой мост, аутентификацию с NACF выполняет каждое TE, так как область IP-адресов CPN известна сети доступа (AN).

Чтобы любое решение по явной аутентификации было возможным, NACF должна быть известна взаимосвязь между идентификаторами и учетными данными, используемыми для аутентификации. Идентификаторы, используемые для явной аутентификации, могут зависеть от применяемого механизма аутентификации и от сети доступа, к которой подключено CPE. Вот два примера таких идентификаторов:

- идентификатор и учетные данные пользователя;
- идентификатор CPE.

Тип применяемых механизмов явной аутентификации зависит от конфигурации сети доступа и политики оператора.

## **6.4.3 Настройка удаленной сети NGW**

Эта процедура необходима для инициализации доступа NGW к компонентам страты обслуживания СПП.

## **6.4.4 Обнаружение компонентов страты обслуживания СПП**

В процессе регистрации в сети NACF должна иметь возможность довести до сведения CPE контактную информацию компонентов страты обслуживания СПП. Если компонентом страты обслуживания СПП является компонент услуг IMS [ITU-T Y.2021], то контактная информация, которую предоставляет NACF, служит для идентификации P-CSCF. Если же это компонент услуг IPTV [ITU-T Y.1910], то контактная информация, которую предоставляет NACF, служит для идентификации функционального блока обнаружения и выбора услуг и приложений (SADS).

Рекомендуется, чтобы NACF предоставляла контактную информацию в виде либо IP-адреса точки контакта, либо полного наименования домена (FQDN) точки контакта; в последнем случае NACF также предоставляет IP-адрес DNS-сервера, способного преобразовать это FQDN в IP-адрес точки контакта.

Как вариант, точки контакта компонентов страты обслуживания СПП могут быть заданы статически в CPE, например, в виде полных наименований доменов, преобразуемых в IP-адреса точек контакта с помощью DNS-сервера. Этот вариант применяется в отсутствие роуминга.

# **7 Функциональная архитектура**

## **7.1 Обзор**

На рисунке 2 показана функциональная архитектура NACF с функциональными объектами и соответствующими эталонными точками. Эталонные точки функций начисления платы не представлены.

В Дополнении II описываются потоки информации, связанные с подсоединением к сети, а в Дополнении III – возможные физические конфигурации, в которых может применяться функциональная архитектура NACF.

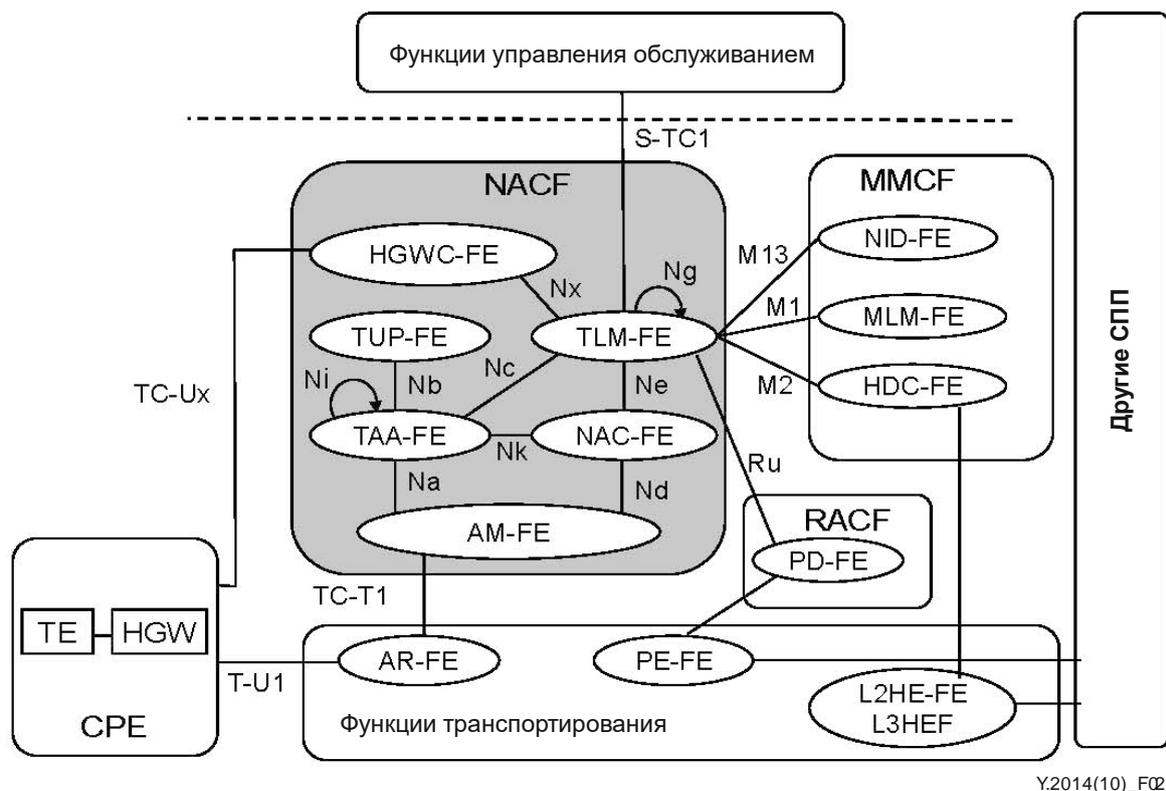


Рисунок 2 – Функциональная архитектура NACF

NACF включает следующие функциональные объекты:

- функциональный объект конфигурации доступа к сети (NAC-FE);
- функциональный объект управления доступом (AM-FE);
- функциональный объект управления местоположением транспортирования (TLM-FE);
- функциональный объект аутентификации и авторизации транспортирования (TAA-FE);
- функциональный объект профиля пользователя транспортирования (TUP-FE);
- функциональный объект конфигурации домашнего шлюза (HGWC-FE).

NACF взаимодействует со следующими компонентами и объектами СПП:

- функциями управления обслуживанием (SCF) (например, SCF компонента услуг IMS [ITU-T Y.2021]) в эталонной точке S-TC1 для экспорта информации о сеансах доступа;
- функциями управления ресурсами и допуском (RACF) [ITU-T Y.2111] в эталонной точке Ru для экспорта информации о профиле абонирования транспортирования;
- функциями управления мобильностью и контроля мобильности (MMCF) [ITU-T Y.2018] в эталонных точках M1, M2 и M13 для экспорта нескольких типов информации об управлении мобильностью;
- функциями транспортирования (например, функциональным объектом ретрансляции для обеспечения доступа (AR-FE) [ITU-T Y.2012]), обеспечивающими ретрансляцию для CPE входящей и исходящей информации, предназначенной для распределения, аутентификации и авторизации адреса (эталонные точки TC-T1 и T-U1);
- оборудованием в помещении пользователя (CPE) в эталонной точке TC-Ux для целей настройки.

Один или несколько функциональных объектов могут быть отображены в одном физическом объекте. Если один функциональный объект реализован двумя физическими объектами, то интерфейс между этими физическими объектами не стандартизирован.

На рисунке 2 не показаны административные домены. Функциональные объекты NACF могут быть распределены по двум административным доменам. Информацию о том, как кочевничество и роуминг отражаются на распределении NACF между доменами сети доступа гостевой и домашней СПП, см. в Дополнении I. Следует отметить, что эталонная точка Ru между NACF и RACF [ITU-T Y.2111] и эталонные точки M1, M2 и M13 между NACF и MMSF [ITU-T Y.2018] являются внутримодечными.

Архитектура СПП не требует, чтобы один экземпляр NACF поддерживал несколько сетей доступа. Это не мешает операторам развертывать функции NACF, общие для нескольких сетей доступа (например, общая база данных профилей пользователей для разных сетей доступа).

## **7.2 Функциональные объекты**

### **7.2.1 Функциональный объект конфигурации доступа к сети (NAC-FE)**

NAC-FE отвечает за распределение IP-адресов CPE. Он также может распределять другие параметры конфигурации сети, такие как адреса DNS-серверов, адреса прокси-серверов сигнализации для конкретных компонентов страты обслуживания (например, адреса P-CSCF и SADS при доступе к компоненту услуг IMS [ITU-T Y.2021] и компоненту IPTV соответственно [ITU-T Y.1910]).

NAC-FE должен быть в состоянии предоставить информацию об используемой CPE сети доступа. Эта информация однозначно идентифицирует сеть доступа, к которой подсоединено CPE. CPE может передать эту информацию функциям управления обслуживанием (SCF) в качестве подсказки для определения местоположения TLM-FE.

SCF определяют местоположение TLM-FE по IP-адресу CPE и/или по информации о сети доступа, из которой они получили IP-пакет (например, у P-CSC-FE может быть несколько логических/физических интерфейсов к различным сетям доступа). SCF передают "запрос информации о местоположении" в TLM-FE через эталонную точку S-TC1. Ключом для запроса служит IP-адрес, используемый CPE.

NAC-FE может обеспечивать выделение TE двух видов IP-адресов – постоянных (PIA) и временных (TIA) – для поддержки мобильности. Выданный TE постоянный IP-адрес не меняется при перемещении TE. Однако следует иметь в виду, что в некоторых случаях, например после перезагрузки TE, тому же TE может быть назначен другой постоянный IP-адрес. Примером постоянного IP-адреса может служить домашний адрес MIP [b-IETF RFC 3220]. При этом всякий раз, когда TE перемещается в новую подсеть, ему выдается новый временный IP-адрес. Адрес для передачи в MIP является примером временного IP-адреса. NAC-FE может выделять IP-адреса со связанным TAA-FE, если выделение адреса должно происходить в ходе аутентификации.

ПРИМЕЧАНИЕ 1. – Транспортирование идентификатора сети доступа к CPE зависит от расширений существующих протоколов (например, новый DHCP или использование DHCP Option 120 [b-IETF RFC 2131]).

ПРИМЕЧАНИЕ 2. – Типичными реализациями NAC-FE являются серверы DHCP или RADIUS.

### **7.2.2 Функциональный объект управления доступом (AM-FE)**

AM-FE прерывает соединение на уровне 2 между CPE и NACF для регистрации и инициализации CPE. Соединение на уровне 2 может использоваться для обнаружения подсоединения к сети на сетевом уровне. В данном случае соединение на уровне 2 между CPE и NACF может служить единой платформой для объектов более высокого уровня в неоднородной сетевой среде, упрощающей обнаружение и выбор из множества типов сетей доступа, которые присутствуют в некоторой географической области. Важно отметить, что ни одно отношение связи между CPE и AM-FE не подразумевает какого-то конкретного механизма транспортирования.

Через это соединение AM-FE может собирать информацию о сети доступа, в том числе об идентификаторе линии, параметрах линии, местоположении TE, параметрах конфигурации хоста и т. д. Информация о конфигурации хоста может также включать ранее назначенные аутентифицированные данные и управление на основе местоположения с информацией о профиле абонирования транспортирования, выданной в предыдущей сети доступа. Если рассматривать укрупненно, информация о сети доступа призвана помочь функциям управления мобильностью более высокого уровня в получении глобального представления об имеющихся неоднородных сетях для реализации кочевничества между ними.

AM-FE транслирует выдаваемые CPE запросы на доступ к сети в формат, воспринимаемый NACF. Он перенаправляет запросы на выделение IP-адреса и, возможно, дополнительных параметров конфигурации сети в адрес TAA-FE и NAC-FE и обратно в зависимости от типа запроса. AM-FE перенаправляет запросы в адрес TAA-FE в целях аутентификации пользователя, авторизации доступа к сети или отказа в нем и получения параметров конфигурации для конкретного пользователя. Кроме того, AM-FE может добавлять в перенаправляемые запросы параметры канального уровня и конфигурации хоста.

Информация о сети доступа помогает NAC-FE и TAA-FE в обнаружении сети и регистрации в ней. Как CPE, так и AM-FE могут принимать решения о возможности установления соединений для управления мобильностью, а также повторно использовать данные регистрации/аутентификации в сети для быстрого восстановления, не выполняя заново процедуры регистрации/аутентификации/настройки целиком. Информация о сети может далее использоваться CPE для выполнения собственной процедуры управления мобильностью.

ПРИМЕЧАНИЕ 1. – Если применяется PPP [b-IETF RFC 1661], AM-FE прерывает соединение PPP и обеспечивает взаимодействие с эталонной точкой NACF, используя, например, протокол AAA (RADIUS [b-IETF RFC 2865] или Diameter [b-IETF RFC 3588]). AM-FE действует в качестве клиента RADIUS, если TAA-FE реализован на сервере RADIUS (AM-FE прерывает соединение PPP и транслирует его в сигнальную информацию в эталонной точке Na).

ПРИМЕЧАНИЕ 2. – Если применяется IEEE 802.1X [b-IEEE 802.1X]/PANA [b-IETF RFC 4058], может осуществляться неявная аутентификация линии. Возможно, что неявная аутентификация будет опираться только на аутентификацию линии доступа к CPE посредством физической или логической идентификации транспорта на уровне 2.

ПРИМЕЧАНИЕ 3. – Если установлено соединение с сетью подвижного доступа (например, 3GPP [b-3GPP TS 23.401], [b-3GPP TS 23.402]), аутентификация может осуществляться после трансляции запросов на доступ к сети в AM-FE. Детали этого вопроса находятся в стадии изучения.

### **7.2.3 Функциональный объект управления местоположением транспортирования (TLM-FE)**

TLM-FE регистрирует связь между IP-адресом, выделенным CPE, и соответствующей информацией о местоположении в сети, которую предоставляет NAC-FE, например характеристиками транспортного оборудования сети доступа, идентификатором логического соединения, идентификационными данными периферийного устройства PE-FE и т. д. TLM-FE регистрирует связь между информацией о местоположении транспортирования, полученной от NAC-FE, и информацией о географическом местоположении. TLM-FE может также хранить идентификатор (идентификаторы) пользователя/CPE, которому был выделен IP-адрес (информацию, полученную от TAA-FE), а также информацию о профиле абонирования транспортирования и о предпочтениях, касающихся конфиденциальности информации о местоположении. Если TLM-FE не хранит идентификатор/профиль пользователя/CPE, требуется, чтобы TLM-FE был способен получать эту информацию от TAA-FE. Подробную информационную модель TLM-FE см. в пункте 7.2.3.1.

Для поддержки иерархической структуры запроса о местоположении TLM-FE может выступать в нескольких ролях, например в домашней, локальной или той и другой вместе. В домашней роли TLM-FE хранит указатель на экземпляр TLM-FE, который выступает в локальной роли с точки зрения подсоединения к сети. Информация о текущем местоположении пользователя/CPE в домене доступа хранится в локальном TLM-FE и привязана к нему. Поэтому при перемещении пользователя/CPE в пределах того же домена доступа достаточно обновить только информацию о привязке местоположения локального TLM-FE, обновлять соответствующую информацию домашнего TLM-FE не требуется.

TLM-FE отвечает на запросы о местоположении, поступающие от функций управления обслуживанием. Когда у одной из таких функций (например, P-CSCF) возникнет необходимость запросить информацию о местоположении оконечного оборудования, она сначала направит запрос в домашний TLM-FE. После этого домашний TLM-FE запросит у локального TLM-FE подробную информацию о местоположении оконечного оборудования в сети, к которой он подсоединен, на основании индекса локального TLM-FE, к которому относится это оконечное оборудование. Фактическая информация, поступающая от TLM-FE, может принимать различные формы (например, местоположение в сети, географические координаты, почтовый адрес и т. д.) в зависимости от соглашений с запрашивающим объектом и предпочтений пользователя, касающихся конфиденциальности информации о местоположении.

С другой стороны, для поддержки кочевничества/роуминга SCF домашней сети обращаются к TLM-FE в гостевой сети за информацией о местоположении через прокси TLM-FE в домашней сети, как показано на рисунке I.5.

Кроме того, для поддержки мобильности взаимодействие между локальными TLM-FE происходит через эталонную точку Ng.

**ПРИМЕЧАНИЕ 1.** – Способ, посредством которого TLM-FE получает географическую информацию из соответствующих характеристик местоположения пользователя в сети, выходит за рамки настоящей Рекомендации.

**ПРИМЕЧАНИЕ 2.** – Географическая информация может принимать различные формы в зависимости от типа доступа и приложения.

TLM-FE определяет текущее местоположение ТЕ в сети и следит за его изменением. Когда меняется точка подсоединения ТЕ в сети, TLM-FE обновляет связь между IP-адресом, выделенным ТЕ, и соответствующей информацией о местоположении в сети. Одновременно он обновляет связь между информацией о местоположении в сети и информацией о географическом местоположении.

Когда ТЕ подсоединяется к новой сети доступа и выделяется новый временный IP-адрес, а информация о местоположении сохраняется в новом TLM-FE, старый TLM-FE может передать соответствующую контекстную информацию (профиль QoS, предпочтения пользователя и т. д.) новому TLM-FE. В этот момент новый TLM-FE может уведомить функцию управления обслуживанием об обновлении информации о привязке.

TLM-FE может быть проинформирован о списках управления доступом (ACL), которые создаются функциями управления и/или объектами управления на основании профиля пользователя в TUP-FE. Примером профиля пользователя может служить факт наличия или отсутствия подписки на определенную группу многоадресной передачи. ACL могут состоять из адреса источника пакетов, адреса назначения пакетов или протокола верхнего уровня и номера порта. TLM-FE уведомляет PD-FE об ACL, подлежащих загрузке в AN-FE, EN-FE и ABG-FE.

AN-FE, EN-FE или ABG-FE принимают решение о пересылке или блокировке каждого пакета на основании ACL, полученных от PD-FE. Если от пользователя поступает запрос на присоединение к группе многоадресной передачи, AN-FE, EN-FE или ABG-FE пересылают и/или обрабатывают этот запрос. В противном случае запрос отбрасывается и в конечном счете завершается неудачей.

### 7.2.3.1 Информационная модель

TLM-FE ведет ряд записей об активных сеансах доступа. Они содержат информацию, полученную от NAC-FE и TAA-FE, информацию, содержащуюся в списке SCF, подписавшихся на конкретные события, а также дополнительные статически сконфигурированные данные. В таблице 1 указывается, какие элементы информации хранятся для каждого из этих сеансов доступа.

**ПРИМЕЧАНИЕ.** – Если используется PPP [b-IETF RFC 1661], TAA-FE может передавать TLM-FE идентификатор физического соединения.

**Таблица 1 – Информационная модель TLM-FE**

Описание сеанса доступа	
Компонент информации, полученной от NAC-FE	
Информация об уникальном в глобальном масштабе IP-адресе	Набор сведений об IP-адресе, используемых для определения местоположения сети доступа, к которой подключено (подсоединено) CPE
– Уникальный IP-адрес	IP-адрес для идентификации подключенного CPE
– Область адреса	Домен адресации IP-адреса (например, префикс подсети или идентификатор VPN)
Идентификатор физического соединения (факультативно)	Локальный идентификатор для физического соединения транспортной сети доступа, к которой подключено CPE (например, IP-адрес устройства PE-FE, MAC-адрес или идентификатор линии и физический порт)

**Таблица 1 – Информационная модель TLM-FE**

<b>Описание сеанса доступа</b>	
Идентификатор логического соединения	Локальный идентификатор для логического соединения транспортной сети доступа, к которой подключено CPE (например, ATM VPI/VCI, PPP, метка MPLS, туннель GTP и логический порт). Он может использоваться для определения местоположения соединения на уровне 2 и соответствующих сетевых устройств для какого-либо конкретного подключенного CPE
Тип CPE	Тип CPE, которому был распределен IP-адрес
<b>Информация, полученная от TAA-FE/TUP-FE</b>	
Идентификатор абонента транспортирования	Уникальный в глобальном масштабе идентификатор подключенного CPE. Он может использоваться для определения местоположения информации об абонировании транспортирования для CPE
Идентификатор логического соединения	Локальный идентификатор для логического соединения транспортной сети доступа, к которой подключено CPE (например, VPI/VCI APN, PPP, метка MPLS, туннель GTP и логический порт)
Параметры услуг мобильности (факультативно) (Примечание 8)	
– Адрес MLM-FE(C) (Примечание 9)	Адрес экземпляра MLM-FE, в котором хранится информация о привязке мобильного адреса
– Адрес MLM-FE(P) (Примечание 9)	Адрес экземпляра MLM-FE, который передает информацию о регистрации местоположения
– Материал ключа (Примечание 9)	Материал, используемый для установления ассоциации безопасности между UE и MMCF
– Тип протокола мобильности	Тип протокола мобильности, который могут поддерживать TE или CPE, например мобильность на базе хост-узла или мобильность на базе сети
– Адрес опорной точки (факультативно)	Адрес верхней конечной точки туннеля с точки зрения UE
– Адрес конечной точки туннеля (факультативно) (Примечание 10)	Адрес конечной точки туннеля для узла сети, который работает в качестве прокси-сервера для UE (нижней конечной точки туннеля)
Идентификатор конфиденциальности (Примечание 1)	Указывает на возможность экспорта услугам и приложениям информации о местоположении
Абонирование транспортного ресурса (Примечания 2 и 3)	
– Идентификатор профиля абонирования транспортирования (Примечание 4)	Идентификатор набора сведений о профиле абонирования транспортирования
– Описание профиля абонирования транспортирования (Примечание 4)	
– Класс обслуживания сети	Представляет класс обслуживания сети, абонированный CPE (например, высший, золотой, серебряный, обычный и т. д.). Может включать класс показателей QoS (например, класс, определенный в [ITU-T Y.1541])
– Абонированная ширина полосы в восходящем направлении	Максимальная пропускная способность, абонированная CPE для соединений в восходящем направлении

**Таблица 1 – Информационная модель TLM-FE**

<b>Описание сеанса доступа</b>	
– Абонированная ширина полосы в нисходящем направлении	Максимальная пропускная способность, абонированная CPE для соединений в нисходящем направлении
– Уровень приоритета	Максимальный уровень приоритета, допустимый для любого запроса на резервирование
– Наименование запросчика	Определяет запросчика (запросчиков), разрешенного (разрешенных) в соответствии с абонированием транспортного ресурса
Конфигурация по умолчанию (факультативно)	
– Идентификатор конфигурации по умолчанию (Примечание 5)	Идентификатор конфигурации по умолчанию
– Описание конфигурации по умолчанию (Примечание 5)	
– Список управления доступом по умолчанию: список допускаемых пунктов назначения	Список IP-адресов, портов, префиксов и диапазонов портов назначения, доступ к которым предоставляется по умолчанию. (Примечание 6)
– Список управления доступом по умолчанию: список блокируемых пунктов назначения и многоадресных потоков	Список IP-адресов, портов, префиксов и диапазонов портов назначения, трафик к которым по умолчанию отклоняется. В случае многоадресных потоков – список адресов при многоадресной групповой передаче по IP и/или список пар (IP-адрес источника, IP-адрес многоадресной передачи), трафик от которых к подсоединенному оборудованию пользователя должен отклоняться. В списке поддерживаются диапазоны адресов. (Примечание 6)
– Пропускная способность для восходящих соединений по умолчанию	Максимальная ширина полосы, которую можно использовать для соединений в восходящем направлении по умолчанию
– Пропускная способность для нисходящих соединений по умолчанию	Максимальная пропускная способность, которую можно использовать для соединений в нисходящем направлении по умолчанию
Статическая информация, полученная от идентификатора физического соединения	
Информация о местоположении	
Идентификатор абонента транспортирования по умолчанию	
Статическая информация, полученная от идентификатора логического соединения	
Точка контакта RACF	Адрес элемента RACF, по которому следует передать профиль абонирования транспортирования
Тип сети доступа	Тип сети доступа, с которой соединено CPE
Наименование подсоединенного домена доступа	Наименование домена доступа, к которому подсоединено CPE, или соответствующего оператора
Информация об управлении событиями	
Информация об управлении событиями (Примечание 7)	
– Событие	Тип события, подлежащего контролю
– Идентичности SCF	Список функций SCF, которые должны быть уведомлены при возникновении события

**Таблица 1 – Информационная модель TLM-FE**

<b>Описание сеанса доступа</b>
<p>ПРИМЕЧАНИЕ 1. – Указание о наличии у приложений возможности доступа к информации о местоположении в зависимости от уровня их безопасности.</p> <p>ПРИМЕЧАНИЕ 2. – Сеанс доступа может содержать описание нескольких абонирований транспортных ресурсов.</p> <p>ПРИМЕЧАНИЕ 3. – Фактически доступная пропускная способность неизвестна RACF. Эта информация может быть определена RACF по идентификатору логического соединения.</p> <p>ПРИМЕЧАНИЕ 4. – Может присутствовать либо идентификатор профиля абонирования транспортирования, либо описание профиля абонирования транспортирования, но не то и другое одновременно.</p> <p>ПРИМЕЧАНИЕ 5. – Может присутствовать либо идентификатор конфигурации по умолчанию, либо описание конфигурации по умолчанию, но не то и другое одновременно.</p> <p>ПРИМЕЧАНИЕ 6. – Если пункт назначения не фигурирует ни в одном из этих двух списков, принятием решений о пропуске или блокировании трафика в эти адреса управляет RACF.</p> <p>ПРИМЕЧАНИЕ 7. – Могут храниться несколько событий и связанных с ними идентичностей SCF.</p> <p>ПРИМЕЧАНИЕ 8. – Доступно только в случае использования услуги мобильности.</p> <p>ПРИМЕЧАНИЕ 9. – Доступно только в случае использования услуги мобильности на базе хост-узла.</p> <p>ПРИМЕЧАНИЕ 10. – Эта информация необязательна, если адрес конечной точки туннеля задается статически или если MLM-FE может получить его, задействуя собственные механизмы. Она доступна только в случае использования услуги мобильности на базе сети.</p>

Возможна ситуация, когда одновременно несколько записей будут содержать один и тот же идентификатор физического соединения, идентификатор логического соединения и/или идентификатор абонента транспортирования, поскольку абонент может установить более одного сеанса IP-доступа в рамках одного или разных логических соединений доступа (например, по виртуальному каналу API) с использованием одного или разных физических соединений доступа. Нет необходимости, чтобы TLM-FE устанавливал какую-либо связь между этими записями, хотя он может это делать для оптимизации емкости хранения.

### 7.2.3.2 Модель состояний TLM-FE

Поведение TLM-FE при управлении записями о доступе может быть представлено приводимой в настоящем пункте моделью состояний. Данная модель не предполагает наложения каких-либо ограничений на реализацию TLM-FE. В конкретных реализациях допускается использовать другую модель при условии, что они демонстрируют то же самое внешнее поведение.

В данной модели состояний определяется конечный автомат сеанса (SSM), имеющий пять состояний.

- *Null* – представляет несуществующую запись о доступе.
- *Wait\_For\_Bind\_Indication\_and\_Profile* – переход в это состояние происходит, когда в ответ на поступивший запрос о подписке на то или иное событие (например, событие входа) создается запись о доступе, и при этом отсутствует запись о сеансе с соответствующим идентификатором абонента транспортирования или информацией об уникальном в глобальном масштабе IP-адресе. Создается частичная запись, и TLM-FE ожидает наступления события *Bind\_Indication*.
- *Wait\_For\_Bind\_Indication* – переход в это состояние происходит, когда в ответ на поступившую информацию о профиле абонирования транспортирования создается запись о доступе, и при этом отсутствует запись о сеансе с соответствующим идентификатором абонента транспортирования или информацией об уникальном в глобальном масштабе IP-адресе. Создается частичная запись, и TLM-FE ожидает наступления события *Bind\_Indication*.
- *Wait\_For\_Profile\_Information* представляет частичную запись о сеансе, в которой отсутствует информация о профиле абонирования транспортирования.
- *Active\_Session* представляет запись о сеансе, содержащую полное описание сеанса доступа.

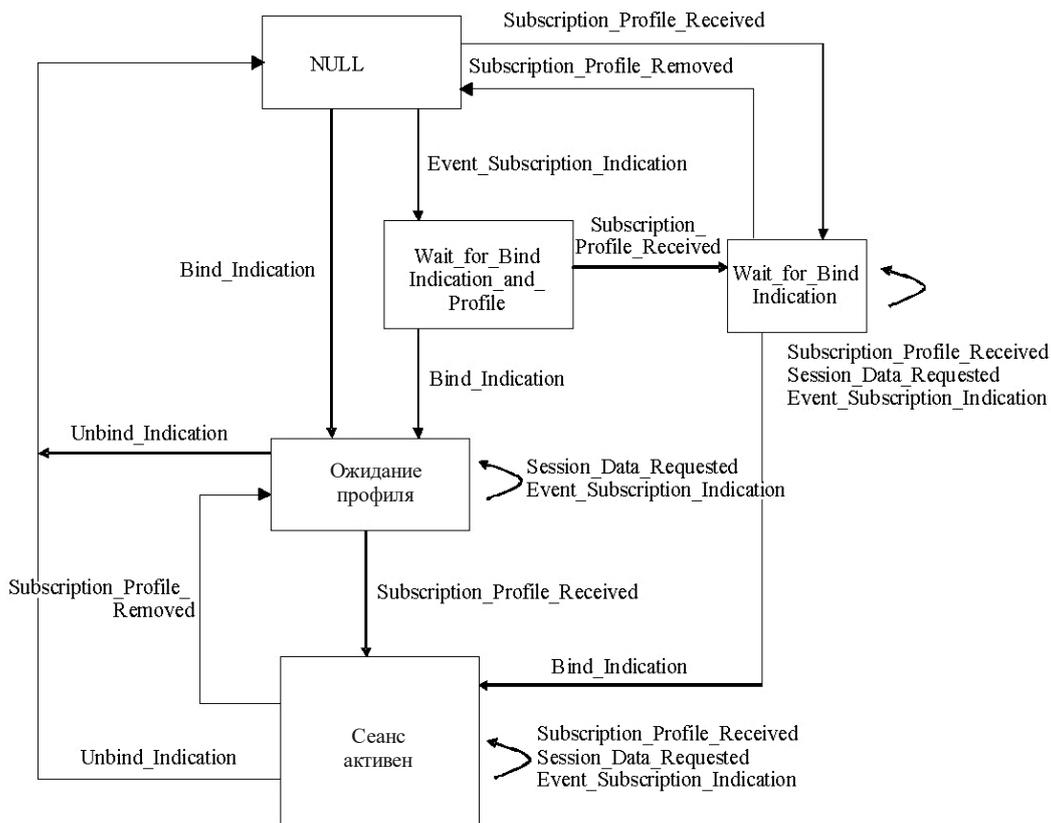
TLM-FE передает и принимает информационные потоки в эталонных точках S-TC1, Ru, Ne и Nc. Входящие информационные потоки направляются в конечные автоматы сеансов (SSM) на основании указанных в них идентификатора абонента транспортирования или информации об уникальном в глобальном масштабе IP-адресе.

При возникновении события *Bind\_Indication* или *Event\_Subscription\_Indication*, сигнализирующего о неизвестном идентификаторе абонента транспортирования или неизвестной информации об уникальном в глобальном масштабе IP-адресе, создается экземпляр SSM.

Конечный автомат сеанса TLM-FE обрабатывает следующие события, вызывающие переход между состояниями.

- *Event\_Subscription\_Indication* возникает, когда от SCF поступает информационный поток запроса регистрации события (см. пункт 8.3.1).  
ПРИМЕЧАНИЕ. – При фактическом наступлении события TLM-FE информационный поток запроса события уведомления возвращается в AF. Это не приводит к смене состояний.
- *Bind\_Indication* возникает, когда в эталонной точке Ne принимается информационный поток сообщения о связывании (см. пункт 8.1.2).
- *Unbind\_Indication* возникает, когда в эталонной точке Ne принимается информационный поток сообщения об отвязывании или неподтверждение запроса информации о связывании (см. пункт 8.1.2).
- *Subscription\_Profile\_Received* возникает, когда в эталонной точке Nc асинхронно или в ответ на переданный ранее информационный поток запроса информации о транспортном ресурсе принимается информационный поток сообщения информации о транспортном ресурсе либо когда из внутренних данных конфигурации следует, что применим профиль абонента транспортирования по умолчанию.
- *Subscription\_Profile\_Removed* возникает, когда в эталонной точке Nc принимается информационный поток уведомления об освобождении транспортного ресурса.
- *Session\_Data\_Requested* возникает, когда в эталонной точке Ru принимается информационный поток запроса информации о транспортном ресурсе или в эталонной точке S-TC1 принимается информационный поток запроса информации. При наступлении этого события через эталонную точку S-TC1 или Ru передается соответственно информационный поток ответа на запрос информации или информационный поток сообщения информации о транспортном ресурсе.

Обзор вызываемых этими событиями переходов между состояниями приведен на рисунке 3.



Y.2014(10)\_F08

**Рисунок 3 – Модель состояний TLM-FE при управлении записями о доступе**

#### 7.2.4 Функциональный объект аутентификации и авторизации транспортирования (ТАА-FE)

ТАА-FE выполняет аутентификацию пользователей и проверку авторизации для доступа к сети на основании профилей абонирования транспортирования. ТАА-FE получает данные аутентификации и информацию об авторизации доступа для каждого пользователя из информации о профиле абонирования транспортирования, хранящейся в TUP-FE. ТАА-FE может также осуществлять сбор данных учета по каждому пользователю, аутентифицированному NACF.

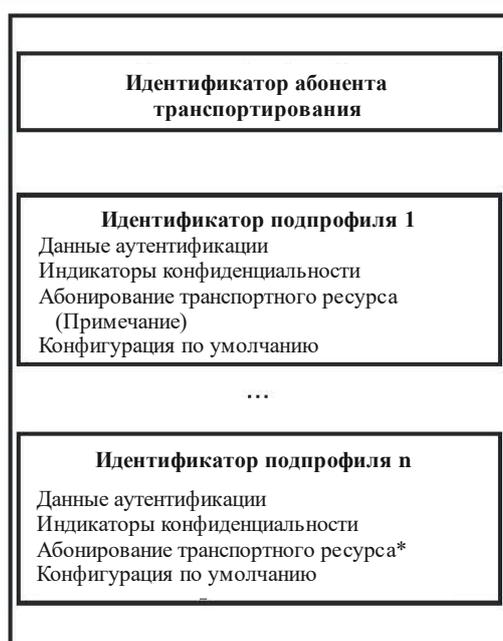
ТАА может поддерживать выделение оконечному оборудованию (ТЕ) IP-адреса или IP-префикса. Выделение IP-адреса и IP-префикса может требоваться в процессе аутентификации в рамках архитектуры мобильности на основе хост-узла или мобильности на основе сети соответственно. В архитектуре мобильности на основе хост-узла ТАА-FE может направить NAC-FE запрос на выделение IP-адреса. Кроме того, в архитектурах мобильности обоих типов ТАА может просто использовать IP-адрес или IP-префикс, хранящийся в TUP-FE в качестве информации профиля пользователя. Для динамического выделения IP-адреса ТАА-FE может направить запрос на выделение IP-адреса в NAC-FE. В этом случае выделенный IP-адрес может меняться при каждом новом таком запросе, даже если он поступил от того же ТЕ. Для статического выделения IP-адреса или IP-префикса ТАА-FE может использовать IP-адрес или IP-префикс, хранящийся в TUP-FE в качестве информации профиля пользователя.

ТАА-FE может также выступать в качестве прокси-сервера. В этом случае ТАА-FE может находить ТАА-FE, действующий в качестве сервера с данными аутентификации абонирования TUP-FE, и взаимодействовать с ним. Выступающий в качестве прокси-сервера ТАА-FE может перенаправлять запросы на доступ и авторизацию, а также учетные сообщения, принятые от AM-FE, в ТАА-FE, действующий в качестве сервера. Ответы, полученные от ТАА-FE, действующего в качестве сервера, возвращаются AM-FE через ТАА-FE, выступающего в качестве прокси-сервера. Взаимодействие выступающего в качестве прокси-сервера ТАА-FE и ТАА-FE, действующего в качестве сервера, происходит через эталонную точку Ni.

ПРИМЕЧАНИЕ. – Если применяется PPP [b-IETF RFC 1661], AM-FE прерывает соединение PPP и преобразует его в сигнальную информацию в эталонной точке Na. Предполагается, что TAA-FE имеет возможность связаться с NAC-FE через внутреннюю эталонную точку для получения IP-адреса (TAA-FE и NAC-FE являются внутренними функциями в случае применения PPP). Сигнализация DHCP [b-IETF RFC 2131] через эталонную точку Nd не передается – вместо этого для передачи AM-FE сведений о конфигурации протокола IP используется эталонная точка Na.

### 7.2.5 Функциональный объект профиля пользователя транспортирования (TUP-FE)

TUP-FE – это функциональный объект, содержащий данные аутентификации абонирования (идентификатор абонента транспортирования, список поддерживаемых методов аутентификации, материал ключа и т. д.) и информацию о требуемой конфигурации доступа к сети. Эти данные в совокупности называются "профиль абонирования транспортирования". Профиль абонирования транспортирования может включать информацию о конфигурации сети для TE, такую как IP-адрес или IP-префикс. Храня IP-адрес или IP-префикс в TUP-FE, можно выделить их TE на постоянной основе, вместо того чтобы запрашивать их динамическое выделение у NAC-FE. Профиль абонирования транспортирования можно разделить на подпрофили (см. рисунок 4), каждый из которых связан с одним или несколькими идентификаторами логических соединений. Поддержка идентификаторов логических соединений носит факультативный (то есть необязательный) характер.



ПРИМЕЧАНИЕ. – В каждом подпрофиле может быть более одного абонирования транспортного ресурса.

Y.2014(10)\_F04

**Рисунок 4 – Профиль абонирования транспортирования в TUP-FE**

TUP-FE отвечает на поступающие от TAA-FE запросы полного профиля или конкретного подпрофиля. В последнем случае обязанность определить идентификатор подпрофиля по идентификатору логического соединения возлагается на TAA-FE (или TAA-FE, выступающий в качестве прокси-сервера).

TUP-FE может размещаться вместе с SUP-FE (как описано в [ITU-T Y.2012]).

### 7.2.6 Функциональный объект конфигурации домашнего шлюза (HGWC-FE)

HGWC-FE используется при инициализации и обновлении HGW. Он также предоставляет HGW дополнительную информацию о конфигурации (например, о настройках внутреннего брандмауэра HGW, QoS-маркировке IP-пакетов и т. д.). Эти данные отличаются от данных конфигурации сети, которые предоставляет NAC-FE.

Кроме того, HGWC-FE выполняет еще ряд функций.

- HGWC-FE управляет текущей конфигурацией HGW и отслеживает ее.
- В HGWC-FE хранятся различные данные конфигурации, на основании которых он решает, какие параметры конфигурации или профили устанавливать или загружать на HGW. HGWC-FE осведомлен о связи между HGW и профилем конфигурации на основании информации об абоненте и/или классах приложений.
- В HGWC-FE имеются механизмы записи (SET) параметров конфигурации в HGW и их чтения (GET).

Рекомендуется обеспечить наличие у HGWC-FE механизма, облегчающего загрузку профилей для различных целей, таких как обновление микропрограммы или настройка конфигурации под конкретного поставщика.

HGWC-FE может также обрабатывать уведомления о доступности TE от HGW. Он может предоставлять TE информацию о конфигурации косвенно, через HGW, или напрямую. HGWC-FE может запускать тесты при техническом обслуживании и обрабатывать результаты тестов, переданные с HGW или TE.

HGWC-FE может быть также сопряжен с TLM-FE для получения информации о HGW и о сети доступа, к которой он подключен. В таких случаях HGWC-FE использует процедуры, описанные в пункте 8.1.7. Информация, полученная от TLM-FE (например, идентификатор физического соединения и/или идентификатор абонента транспортирования) может служить входным параметром для выбора данных конфигурации, подлежащих доставке на HGW.

#### **7.2.6.1 Оптимизированная аутентификация в NACF**

В ходе процедуры подсоединения к сети HGW направляет NACF запрос на доступ, а TAA-FE выполняет аутентификацию и авторизацию на уровне сети. В случае их успешного выполнения между TAA-FE и HGW может быть по согласованию установлена ассоциация безопасности (SA), используемая для защиты соединения между HGW и HGWC-FE.

TAA-FE принудительно доставляет установленную SA на TLM-FE через эталонную точку Nc, после чего TLM-FE уведомляет HGWC-FE о SA через эталонную точку Nx.

Обмен управляющей информацией между HGW и HGWC-FE аутентифицируется в обоих направлениях посредством SA.

Следует отметить, что эта процедура носит факультативный (необязательный) характер.

#### **7.2.7 Функциональный объект ретрансляции для обеспечения доступа (AR-FE)**

AR-FE выступает в качестве ретранслятора между CPE и NACF. Он получает запросы на доступ к сети от CPE и перенаправляет их в NACF. Прежде чем перенаправить запрос, AR-FE может также добавить информацию о локальной конфигурации. Функциональность AR-FE описана в [ITU-T Y.2012].

ПРИМЕЧАНИЕ. – При использовании PPP [b-IETF RFC 1661] AR-FE может действовать в качестве ретранслятора PPPoE. При использовании DHCP [b-IETF RFC 2131] AR-FE действует в качестве агента-ретранслятора DHCP.

## **8 Эталонные точки**

### **8.1 Внутренние эталонные точки NACF**

#### **8.1.1 Эталонная точка AM-FE – NAC-FE (Nd)**

Эталонная точка Nd позволяет AM-FE передавать NAC-FE запрос о выделении IP-адреса и других параметров конфигурации сети для CPE.

#### **8.1.2 Эталонная точка NAC-FE – TLM-FE (Ne)**

Эталонная точка Ne позволяет NAC-FE регистрировать в TLM-FE связь между выделенным IP-адресом и CPE, а также другой информацией, относящейся к транспортированию, например адресами логических/физических портов.

Через эталонную точку TLM-FE – NAC-FE проходят следующие информационные потоки:

- сообщение о связывании;
- подтверждение связывания;
- сообщение об отвязывании;
- запрос информации о связывании;
- подтверждение запроса информации о связывании.

### 8.1.2.1 Сообщение о связывании

В таблице 2 описаны элементы информационного потока сообщения о связывании.

**Таблица 2 – Сообщение о связывании (NAC-FE → TLM-FE)**

Информация об уникальном в глобальном масштабе IP-адресе	Набор сведений об IP-адресе, используемых для определения местоположения сети доступа, к которой подключено CPE
– Уникальный IP-адрес	IP-адрес, выделенный подключенному CPE
– Область адреса	Домен адресации, в котором IP-адрес имеет значение
Идентификатор физического соединения (факультативно)	Локальный идентификатор для физического соединения транспортной сети доступа, к которой подключено CPE (например, IP-адрес устройства PE-FE, MAC-адрес или идентификатор линии и идентификатор физического порта)
– Идентификатор логического соединения (Примечание 1)	Локальный идентификатор для логического соединения транспортной сети доступа, к которой подключено CPE (например, VPI/VCI API, PPP, метка MPLS, туннель GTP или логический порт)
Тип CPE (факультативно) (Примечание 2)	Тип CPE
<p>ПРИМЕЧАНИЕ 1. – Если NAC-FE реализован как сервер DHCP, этот параметр отображается на опции 82 DHCP (подопции 1 и 2 [b-IETF RFC 2131]).</p> <p>ПРИМЕЧАНИЕ 2. – Если NAC-FE реализован как сервер DHCP, этот параметр отображается на опции 77 DHCP [b-IETF RFC 2131].</p>	

### 8.1.2.2 Подтверждение связывания

В информационном потоке подтверждения связывания передается информация, которая может быть передана обратно в CPE. Информацию, возвращаемую в ответ на сообщение о связывании, TLM-FE принимает от TAA-FE или получает от TUP-FE через TAA-FE.

В таблице 3 описаны элементы информационного потока подтверждения связывания.

**Таблица 3 – Подтверждение связывания (TLM-FE → NAC-FE)**

Адрес HGWC-FE (факультативно)	Адрес объекта HGWC-FE, от которого CPE может получать данные конфигурации
Информация о географическом местоположении (факультативно)	Сведения о географическом местоположении
Идентичность P-CSCF (факультативно)	Идентификатор P-CSCF для доступа к услугам IMS [ITU-T Y.2021]
Идентичность SADS (факультативно)	Идентификатор SADS для доступа к услугам IPTV [ITU-T Y.1910]

### 8.1.2.3 Сообщение об отвязывании

NAC-FE передает информационный поток сообщения об отвязывании, когда истекает срок действия связи между IP-адресом и CPE или когда освобождается соответствующее соединение PPP либо соединение на уровне 2.

В таблице 4 описаны элементы информационного потока сообщения об отвязывании.

**Таблица 4 – Сообщение об отвязывании (NAC-FE → TLM-FE)**

Информация об уникальном в глобальном масштабе IP-адресе	Набор сведений об IP-адресе, используемых для определения местоположения сети доступа, к которой подключено CPE
– Уникальный IP-адрес	IP-адрес для идентификации подключенного CPE
– Область адреса	Домен адресации IP-адреса (например, префикс подсети или идентификатор VPN)

#### 8.1.2.4 Запрос информации о связывании

Посредством этого запроса TLM-FE запрашивает информацию о связывании (например, в контексте процедур восстановления) у NAC-FE.

В таблице 5 описаны элементы информационного потока запроса информации о связывании.

**Таблица 5 – Запрос информации о связывании (TLM-FE → NAC-FE)**

Информация об уникальном в глобальном масштабе IP-адресе	Набор сведений об IP-адресе, используемых для определения местоположения сети доступа, к которой подключено CPE
– Уникальный IP-адрес	IP-адрес для идентификации подключенного CPE
– Область адреса	Домен адресации IP-адреса (например, префикс подсети или идентификатор VPN)

#### 8.1.2.5 Подтверждение запроса информации о связывании

Информационный поток подтверждения запроса информации о связывании используется NAC-FE для уведомления TLM-FE о результатах запроса информации о связывании. Если запрос является успешным, в информационном потоке подтверждения передается информация, описанная в таблице 6.

**Таблица 6 – Подтверждение запроса информации о связывании (NAC-FE → TLM-FE)**

Идентификатор физического соединения (факультативно)	Локальный идентификатор для физического соединения транспортной сети доступа, к которой подключено CPE (например, IP-адрес устройства PE-FE и MAC-адрес или идентификатор линии и идентификатор физического порта)
– Идентификатор логического соединения (Примечание 1)	Локальный идентификатор для логического соединения транспортной сети доступа, к которой подключено CPE (например, VPI/VCI API, PPP, метка MPLS, туннель GTP или логический порт)
Тип CPE (факультативно) (Примечание 2)	Тип CPE
<p>ПРИМЕЧАНИЕ 1. – Если NAC-FE реализован как сервер DHCP, этот параметр отображается на опции 82 DHCP (подопции 1 и 2 [b-IETF RFC 2131]).</p> <p>ПРИМЕЧАНИЕ 2. – Если NAC-FE реализован как сервер DHCP, этот параметр отображается на опции 77 DHCP [b-IETF RFC 2131].</p>	

#### 8.1.2.6 Сообщение параметров услуг мобильности

Информационный поток сообщения параметров услуг мобильности используется для принудительной доставки информации об услугах мобильности от TLM-FE в NAC-FE после успешной аутентификации пользователя.

В таблице 7 описаны элементы информационного потока сообщения параметров услуг мобильности.

**Таблица 7 – Сообщение параметров услуг мобильности (TLM-FE → NAC-FE)**

Идентификатор абонента транспортирования	Уникальный в глобальном масштабе идентификатор подключенного CPE. Он может использоваться для определения местоположения информации об абонировании транспортирования для CPE
Информация об уникальном в глобальном масштабе IP-адресе (Примечание 1)	Набор сведений об IP-адресе, используемых для определения местоположения сети доступа, к которой подключено CPE
– Уникальный IP-адрес	IP-адрес для идентификации подключенного CPE
– Область адреса	Домен адресации IP-адреса (например, префикс подсети или идентификатор VPN)
Параметры услуг мобильности (факультативно) (Примечание 2)	
– Адрес MLM-FE(C) (Примечание 3)	Адрес экземпляра MLM-FE, в котором хранится информация о привязке мобильного адреса
– Адрес MLM-FE(P) (Примечание 3)	Адрес экземпляра MLM-FE, который передает информацию о регистрации местоположения
– Материал ключа (Примечание 3)	Материал, используемый для установления ассоциации безопасности между UE и MMCF
– Тип протокола мобильности	Тип протокола мобильности, который могут поддерживать TE или CPE, например мобильность на базе хост-узла или мобильность на базе сети
– Адрес опорной точки (факультативно)	Адрес верхней конечной точки туннеля с точки зрения UE
– Адрес конечной точки туннеля (факультативно) (Примечание 4)	Адрес конечной точки туннеля для узла сети, который работает в качестве прокси-сервера для UE (нижней конечной точки туннеля)
<p>ПРИМЕЧАНИЕ 1. – Информация об уникальном в глобальном масштабе IP-адресе включается сюда в том случае, если ее запрашивает TAA-FE. Она идентична постоянному IP-адресу с точки зрения MMCF.</p> <p>ПРИМЕЧАНИЕ 2. – Доступен только в случае использования услуги мобильности.</p> <p>ПРИМЕЧАНИЕ 3. – Доступен только в случае использования услуги мобильности на базе хост-узла.</p> <p>ПРИМЕЧАНИЕ 4. – Эта информация необязательна, если адрес конечной точки туннеля задается статически или если MLM-FE может получить его, задействуя собственные механизмы. Она доступна только в случае использования услуги мобильности на базе сети.</p>	

### 8.1.3 Эталонная точка AM-FE – TAA-FE (Na)

Эталонная точка Na позволяет AM-FE запрашивать у TAA-FE проверку аутентификации пользователя и информации об абонировании транспортирования.

### 8.1.4 Эталонная точка TAA-FE – TLM-FE (Nc)

Эталонная точка Nc позволяет TLM-FE зарегистрировать связь между абонентом и соответствующими предпочтениями, касающимися конфиденциальности информации о местоположении, которую предоставляет TAA-FE. Кроме того, эталонная точка Nc используется для регистрации информации об абонировании транспортного ресурса. TLM-FE может получать информацию об абонировании транспортного ресурса от TAA-FE.

Связь TAA-FE – TLM-FE может вестись в режиме принудительной доставки (push) или в опросном режиме (pull). Режим принудительной доставки используется, когда TAA-FE участвует в обработке запросов на доступ к сети для авторизации доступа или отказа в доступе (например, когда применяется явная аутентификация). Опросный режим используется, когда применяется неявная аутентификация или для поддержки процедур восстановления TLM-FE.

Через эталонную точку Nc проходят следующие информационные потоки:

- сообщение информации о транспортном ресурсе;
- запрос информации о транспортном ресурсе;
- ответ на запрос информации о транспортном ресурсе;

– уведомление об освобождении транспортного ресурса.

#### 8.1.4.1 Сообщение информации о транспортном ресурсе

Информационный поток сообщения информации о транспортном ресурсе используется для принудительной доставки информации об абонировании транспортирования от TAA-FE в TLM-FE после успешной аутентификации пользователя. TAA-FE может принять решение о том, чтобы передать в одном и том же информационном потоке сообщения информации о транспортном ресурсе одни профили абонирования транспортирования в виде идентификатора профиля (поскольку предполагается, что фактическая информация о профиле абонирования транспортирования доступна в TLM-FE), а другие – в виде полного описания профиля. Эту информацию TAA-FE получает от TUP-FE.

В таблице 8 описаны элементы информационного потока сообщения информации о транспортном ресурсе.

ПРИМЕЧАНИЕ. – Если используется PPP [b-IETF RFC 1661], TAA-FE может передавать TLM-FE идентификатор физического соединения.

**Таблица 8 – Сообщение информации о транспортном ресурсе (TAA-FE → TLM-FE)**

Идентификатор абонента транспортирования	Уникальный в глобальном масштабе идентификатор подключенного CPE. Он может использоваться для определения местоположения информации об абонировании транспортирования для CPE
Информация об уникальном в глобальном масштабе IP-адресе (Примечание 1)	Набор сведений об IP-адресе, используемых для определения местоположения сети доступа, к которой подключено CPE
– Уникальный IP-адрес	IP-адрес для идентификации подключенного CPE
– Область адреса	Домен адресации IP-адреса (например, префикс подсети или идентификатор VPN)
Идентификатор логического соединения	Локальный идентификатор для логического соединения транспортной сети доступа, к которой подключено CPE (например, VPI/VCI API, PPP, метка MPLS, туннель GTP и логический порт)
Параметры услуг мобильности (факультативно) (Примечание 7)	
– Адрес MLM-FE(C) (Примечание 8)	Адрес экземпляра MLM-FE, в котором хранится информация о привязке мобильного адреса
– Адрес MLM-FE(P) (Примечание 8)	Адрес экземпляра MLM-FE, который передает информацию о регистрации местоположения
– Материал ключа (Примечание 8)	Материал, используемый для установления ассоциации безопасности между UE и MMCF
– Тип протокола мобильности	Тип протокола мобильности, который могут поддерживать TE или CPE, например мобильность на базе хост-узла или мобильность на базе сети
– Адрес опорной точки (факультативно)	Адрес верхней конечной точки туннеля с точки зрения UE
– Адрес конечной точки туннеля (факультативно) (Примечание 9)	Адрес конечной точки туннеля для узла сети, который работает в качестве прокси-сервера для UE (нижней конечной точки туннеля)
Точка контакта домашнего TLM-FE	FQDN или IP-адрес домашнего TLM-FE
Точка контакта локального TLM-FE	FQDN или IP-адрес локального TLM-FE
Идентификатор конфиденциальности	Указывает на возможность экспорта услугам и приложениям информации о местоположении
Ассоциация безопасности (факультативно)	Ассоциация безопасности, установленная по согласованию между HGW и TAA-FE в ходе процедуры аутентификации и авторизации доступа к сети.
Абонирование транспортного ресурса (факультативно) (Примечание 2)	

**Таблица 8 – Сообщение информации о транспортном ресурсе (TAA-FE → TLM-FE)**

– Идентификатор профиля абонирования транспортирования (Примечание 3)	Идентификатор набора сведений о профиле абонирования транспортирования
– Описание профиля абонирования транспортирования (Примечание 3)	
– Класс обслуживания сети	Представляет класс обслуживания сети, абонированный СРЕ (например, высший, золотой, серебряный, обычный и т. д.). Может включать класс показателей QoS (например, класс, определенный в [ITU-T Y.1541])
– Абонированная ширина полосы в восходящем направлении	Максимальная пропускная способность, абонированная СРЕ для соединений в восходящем направлении
– Абонированная ширина полосы в нисходящем направлении	Максимальная пропускная способность, абонированная СРЕ для соединений в нисходящем направлении
– Уровень приоритета	Максимальный уровень приоритета, допустимый для любого запроса на резервирование
– Наименование запросчика	Определяет запросчика (запросчиков), разрешенного (разрешенных) в соответствии с абонированием транспортного ресурса
Конфигурация по умолчанию (факультативно) Примечание 4)	
– Идентификатор конфигурации по умолчанию (Примечание 5)	Идентификатор конфигурации по умолчанию
– Описание конфигурации по умолчанию (Примечание 5)	
– Список управления доступом по умолчанию: список допускаемых пунктов назначения и многоадресных потоков	Список IP-адресов, портов, префиксов и/или диапазонов портов назначения, трафик к которым по умолчанию пропускается. В случае многоадресных потоков – список адресов при многоадресной групповой передаче по IP-протоколу и/или список пар (IP-адрес источника, IP-адрес многоадресной передачи), трафик от которых может получать подсоединенное оборудование пользователя. В списке поддерживаются диапазоны адресов. (Примечание 6)
– Список управления доступом по умолчанию: список блокируемых пунктов назначения и многоадресных потоков	Список IP-адресов, портов, префиксов и диапазонов портов назначения, трафик к которым по умолчанию отклоняется. В случае многоадресных потоков – список адресов при многоадресной групповой передаче по IP-протоколу и/или список пар (IP-адрес источника, IP-адрес многоадресной передачи), трафик от которых к подсоединенному оборудованию пользователя должен отклоняться. В списке поддерживаются диапазоны адресов. (Примечание 6)
– Пропускная способность для восходящих соединений по умолчанию	Максимальная ширина полосы, которую можно использовать для соединений в восходящем направлении по умолчанию
– Пропускная способность для нисходящих соединений по умолчанию	Максимальная пропускная способность, которую можно использовать для соединений в нисходящем направлении по умолчанию

**Таблица 8 – Сообщение информации о транспортном ресурсе (TAA-FE → TLM-FE)**

<p>ПРИМЕЧАНИЕ 1. – Если используется PPP [b-IETF RFC 1661], TAA-FE обязан передать TLM-FE информацию об уникальном в глобальном масштабе IP-адресе. При использовании DHCP [b-IETF RFC 2131] этот параметр является факультативным.</p> <p>ПРИМЕЧАНИЕ 2. – Абонирование транспортного ресурса может содержать несколько профилей абонирования транспортирования.</p> <p>ПРИМЕЧАНИЕ 3. – Может присутствовать либо идентификатор профиля абонирования транспортирования, либо описание профиля абонирования транспортирования, но не то и другое одновременно.</p> <p>ПРИМЕЧАНИЕ 4. – Эту информацию использует RACF для настройки транспортных функций перед приемом запросов на резервирование ресурсов от услуг/приложений.</p> <p>ПРИМЕЧАНИЕ 5. – Может присутствовать либо идентификатор конфигурации по умолчанию, либо описание конфигурации по умолчанию, но не то и другое одновременно.</p> <p>ПРИМЕЧАНИЕ 6. – Если пункт назначения не фигурирует ни в одном из этих двух списков, принятием решений о пропуске или блокировании трафика в эти адреса управляет RACF.</p> <p>ПРИМЕЧАНИЕ 7. – Доступен только в случае использования услуги мобильности.</p> <p>ПРИМЕЧАНИЕ 8. – Доступен только в случае использования услуги мобильности на базе хост-узла.</p> <p>ПРИМЕЧАНИЕ 9. – Эта информация необязательна, если адрес конечной точки туннеля задается статически или если MLM-FE может получить его, задействуя собственные механизмы. Она доступна только в случае использования услуги мобильности на базе сети.</p>
--

#### 8.1.4.2 Запрос информации о транспортном ресурсе

TLM-FE использует информационный поток запроса информации о транспортном ресурсе, чтобы запросить информацию о профиле абонирования транспортирования у TAA-FE. Этот информационный поток используется, когда связь между TLM-FE и TAA-FE ведется в опросном режиме или в контексте процедур восстановления TLM-FE.

В таблице 9 описаны элементы информационного потока запроса информации о транспортном ресурсе.

**Таблица 9 – Запрос информации о транспортном ресурсе (TLM-FE → TAA-FE)**

Информация об уникальном в глобальном масштабе IP-адресе (Примечание 1)	Набор сведений об IP-адресе, используемых для определения местоположения сети доступа, к которой подключено CPE
– Уникальный IP-адрес	IP-адрес для идентификации подключенного CPE
– Область адреса	Домен адресации IP-адреса (например, префикс подсети или идентификатор VPN)
Идентификатор логического соединения	Локальный идентификатор для логического соединения транспортной сети доступа, к которой подключено CPE (например, VPI/VCI АП, PPP, метка MPLS, туннель GTP и логический порт)
Идентификатор абонента транспортирования (Примечание 2)	Уникальный в глобальном масштабе идентификатор подсоединенного CPE. Может использоваться для определения местоположения информации об абонировании транспортирования для CPE
<p>ПРИМЕЧАНИЕ 1. – Если этот информационный поток используется для поддержки процедур восстановления, а эталонная точка работает в режиме принудительной доставки, то требуется указывать информацию об уникальном в глобальном масштабе IP-адресе.</p> <p>ПРИМЕЧАНИЕ 2. – Если эталонная точка работает в опросном режиме, то требуется указывать идентификатор абонента транспортирования.</p>	

#### 8.1.4.3 Ответ на запрос информации о транспортном ресурсе

Информационный поток ответа на запрос информации о транспортном ресурсе используется для передачи информации об абонировании транспортирования от TAA-FE в TLM-FE в ответ на запрос информации о транспортном ресурсе.

В таблице 10 описаны элементы информационного потока ответа на запрос информации о транспортном ресурсе.

ПРИМЕЧАНИЕ. – Если используется PPP [b-IETF RFC 1661], TAA-FE может передавать TLM-FE идентификатор физического соединения.

**Таблица 10 – Ответ на запрос информации о транспортном ресурсе (TAA-FE → TLM-FE)**

Идентификатор абонента транспортирования	Уникальный в глобальном масштабе идентификатор подключенного CPE. Он может использоваться для определения местоположения информации об абонировании транспортирования для CPE
Информация об уникальном в глобальном масштабе IP-адресе (Примечание 1)	Набор сведений об IP-адресе, используемых для определения местоположения сети доступа, к которой подключено CPE
– Уникальный IP-адрес	IP-адрес для идентификации подключенного CPE
– Область адреса	Домен адресации IP-адреса (например, префикс подсети или идентификатор VPN)
Идентификатор логического соединения	Локальный идентификатор для логического соединения транспортной сети доступа, к которой подключено CPE (например, VPI/VCI APN, PPP, метка MPLS, туннель GTP и логический порт)
Параметры услуг мобильности (факультативно) (Примечание 7)	
– Адрес MLM-FE(C) (Примечание 8)	Адрес экземпляра MLM-FE, в котором хранится информация о привязке мобильного адреса
– Адрес MLM-FE(P) (Примечание 8)	Адрес экземпляра MLM-FE, который передает информацию о регистрации местоположения
– Материал ключа (Примечание 8)	Материал, используемый для установления ассоциации безопасности между UE и MMCF
– Тип протокола мобильности	Тип протокола мобильности, который могут поддерживать TE или CPE, например мобильность на базе хост-узла или мобильность на базе сети
– Адрес опорной точки (факультативно)	Адрес верхней конечной точки туннеля с точки зрения UE
– Адрес конечной точки туннеля (факультативно) (Примечание 9)	Адрес конечной точки туннеля для узла сети, который работает в качестве прокси-сервера для UE (нижней конечной точки туннеля)
Идентификатор конфиденциальности	Указывает на возможность экспорта услугам и приложениям информации о местоположении
Ассоциация безопасности (факультативно)	Ассоциация безопасности, установленная по согласованию между NGW и TAA-FE в ходе процедуры аутентификации и авторизации доступа к сети

**Таблица 10 – Ответ на запрос информации о транспортном ресурсе (TAA-FE → TLM-FE)**

Абонирование транспортного ресурса (факультативно) (Примечание 2)	
– Идентификатор профиля абонирования транспортирования (Примечание 3)	Идентификатор набора сведений о профиле абонирования транспортирования
– Описание профиля абонирования транспортирования (Примечание 3)	
– Класс обслуживания сети	Представляет класс обслуживания сети, абонируемый СРЕ (например, высший, золотой, серебряный, обычный и т. д.). Может включать класс показателей QoS (например, класс, определенный в [ITU-T Y.1541])
– Абонируемая ширина полосы в восходящем направлении	Максимальная пропускная способность, абонируемая СРЕ для соединений в восходящем направлении
– Абонируемая ширина полосы в нисходящем направлении	Максимальная пропускная способность, абонируемая СРЕ для соединений в нисходящем направлении
– Уровень приоритета	Максимальный уровень приоритета, допустимый для любого запроса на резервирование
– Наименование запросчика	Определяет запросчика (запросчиков), разрешенного (разрешенных) в соответствии с абонированием транспортного ресурса
Конфигурация по умолчанию (факультативно) (Примечание 4)	
– Идентификатор конфигурации по умолчанию (Примечание 5)	Идентификатор конфигурации по умолчанию
– Описание конфигурации по умолчанию (Примечание 5)	
– Список управления доступом по умолчанию: список допускаемых пунктов назначения и многоадресных потоков	Список IP-адресов, портов, префиксов и/или диапазонов портов назначения, трафик к которым по умолчанию пропускается. В случае многоадресных потоков – список адресов при многоадресной групповой передаче по IP-протоколу и/или список пар (IP-адрес источника, IP-адрес многоадресной передачи), трафик от которых может получать подсоединенное оборудование пользователя. В списке поддерживаются диапазоны адресов. (Примечание 6)
– Список управления доступом по умолчанию: список блокируемых пунктов назначения и многоадресных потоков	Список IP-адресов, портов, префиксов и диапазонов портов назначения, трафик к которым по умолчанию отклоняется. В случае многоадресных потоков – список адресов при многоадресной групповой передаче по IP-протоколу и/или список пар (IP-адрес источника, IP-адрес многоадресной передачи), трафик от которых к подсоединенному оборудованию пользователя должен отклоняться. В списке поддерживаются диапазоны адресов. (Примечание 6)
– Пропускная способность для восходящих соединений по умолчанию	Максимальная ширина полосы, которую можно использовать для соединений в восходящем направлении по умолчанию
– Пропускная способность для нисходящих соединений по умолчанию	Максимальная пропускная способность, которую можно использовать для соединений в нисходящем направлении по умолчанию

**Таблица 10 – Ответ на запрос информации о транспортном ресурсе (TAA-FE → TLM-FE)**

<p>ПРИМЕЧАНИЕ 1. – Если используется PPP [b-IETF RFC 1661], TAA-FE обязан передать TLM-FE информацию об уникальном в глобальном масштабе IP-адресе. При использовании DHCP [b-IETF RFC 2131] этот параметр является факультативным.</p> <p>ПРИМЕЧАНИЕ 2. – Абонирование транспортного ресурса может содержать несколько профилей абонирования транспортирования.</p> <p>ПРИМЕЧАНИЕ 3. – Может присутствовать либо идентификатор профиля абонирования транспортирования, либо описание профиля абонирования транспортирования, но не то и другое одновременно.</p> <p>ПРИМЕЧАНИЕ 4. – Эту информацию использует RACF для настройки транспортных функций перед приемом запросов на резервирование ресурсов от услуг/приложений.</p> <p>ПРИМЕЧАНИЕ 5. – Может присутствовать либо идентификатор конфигурации по умолчанию, либо описание конфигурации по умолчанию, но не то и другое одновременно.</p> <p>ПРИМЕЧАНИЕ 6. – Если пункт назначения не фигурирует ни в одном из этих двух списков, принятием решений о пропуске или блокировании трафика в эти адреса управляет RACF.</p> <p>ПРИМЕЧАНИЕ 7. – Доступен только в случае использования услуги мобильности.</p> <p>ПРИМЕЧАНИЕ 8. – Доступен только в случае использования услуги мобильности на базе хост-узла.</p> <p>ПРИМЕЧАНИЕ 9. – Эта информация необязательна, если адрес конечной точки туннеля задается статически или если TLM-FE может получить его, задействуя собственные механизмы. Она доступна только в случае использования услуги мобильности на базе сети.</p>
--

#### 8.1.4.4 Уведомление об освобождении транспортного ресурса

TAA-FE использует информационный поток уведомления об освобождении транспортного ресурса, чтобы запросить у TLM-FE удаление хранящейся в нем информации о CPE. Это событие возникает в результате действий по управлению сетью.

В таблице 11 описаны элементы информационного потока уведомления об освобождении транспортного ресурса.

**Таблица 11 – Уведомление об освобождении транспортного ресурса (TAA-FE → TLM-FE)**

Информация об уникальном в глобальном масштабе IP-адресе (Примечание)	Набор сведений об IP-адресе, используемых для определения местоположения сети доступа, к которой подключено CPE
– Уникальный IP-адрес	IP-адрес для идентификации подключенного CPE
– Область адреса	Домен адресации IP-адреса (например, префикс подсети или идентификатор VPN)
Идентификатор логического соединения (факультативно)	Локальный идентификатор для логического соединения транспортной сети доступа, к которой подключено CPE (например, VPI/VCI АПД, PPP, метка MPLS, туннель GTP и логический порт)
Идентификатор абонента транспортирования (Примечание)	Уникальный в глобальном масштабе идентификатор подключенного CPE. Он может использоваться для определения местоположения информации об абонировании транспортирования для CPE
ПРИМЕЧАНИЕ. – Указывается либо информация об уникальном в глобальном масштабе IP-адресе, либо идентификатор абонента транспортирования.	

#### 8.1.5 Эталонная точка NAC-FE – TAA-FE (Nk)

В настоящей Рекомендации эталонная точка Nk не определяется.

#### 8.1.6 Эталонная точка TAA-FE – TAA-FE (Ni)

Эта эталонная точка предназначена для использования между прокси-сервером TAA-FE и сервером TAA-FE, которые могут находиться в различных административных доменах. Через нее прокси-сервер TAA-FE может передавать серверу TAA-FE запросы на аутентификацию и авторизацию пользователя на основании профилей абонирования транспортирования. Через нее прокси-сервер TAA-FE может также пересылать серверу TAA-FE данные учета по конкретному пользовательскому сеансу или перенаправлять запросы, принятые от TLM-FE.

Прокси-сервер ТАА-FE будет перенаправлять серверу ТАА-FE через эталонную точку Ni запросы на доступ и авторизацию, а также учетные сообщения, принятые от АМ-FE через эталонную точку Na. Ответы, полученные от сервера ТАА-FE через эталонную точку Ni, будут пересылаться в АМ-FE через эталонную точку Na. Для организации этого обмена между прокси-сервером ТАА-FE и сервером ТАА-FE должны быть установлены двусторонние отношения доверия.

Эта эталонная точка поддерживает обмен сообщениями AAA между прокси-сервером ТАА-FE и сервером ТАА-FE.

ПРИМЕЧАНИЕ. – Возможные протоколы для обмена через эту эталонную точку – RADIUS [b-IETF RFC 2865] и Diameter [b-IETF RFC 3588].

### 8.1.6.1 Информация, обмен которой осуществляется через эталонную точку Ni

В таблице 12 указаны информационные компоненты, обмен которыми осуществляется через эталонную точку Ni.

Таблица 12 – Эталонная точка Ni

Информационный компонент	Описание
Идентификатор абонента транспортирования	Уникальный в глобальном масштабе идентификатор CPE, запрашивающего IP-соединение. Он может использоваться для определения местоположения информации об абонировании транспортирования для CPE
Идентификатор конфиденциальности	Указывает на возможность экспорта услугам и приложениям информации о местоположении
Информация об уникальном в глобальном масштабе IP-адресе	Набор сведений об IP-адресе, используемых для определения местоположения сети доступа, к которой подключено CPE
– Уникальный IP-адрес	IP-адрес для идентификации подключенного CPE
– Область адреса	Домен адресации IP-адреса (например, префикс подсети или идентификатор VPN)
Параметры услуг мобильности (факультативно) (Примечание 6)	
– Адрес MLM-FE(C) (Примечание 7)	Адрес экземпляра MLM-FE, в котором хранится информация о привязке мобильного адреса
– Адрес MLM-FE(P) (Примечание 7)	Адрес экземпляра MLM-FE, который передает информацию о регистрации местоположения
– Материал ключа (Примечание 7)	Материал, используемый для установления ассоциации безопасности между UE и MMCF
– Тип протокола мобильности	Тип протокола мобильности, который могут поддерживать TE или CPE, например мобильность на базе хост-узла или мобильность на базе сети
– Адрес опорной точки (факультативно)	Адрес верхней конечной точки туннеля с точки зрения UE
– Адрес конечной точки туннеля (факультативно) (Примечание 8)	Адрес конечной точки туннеля для узла сети, который работает в качестве прокси-сервера для UE (нижней конечной точки туннеля)
Точка контакта домашнего TLM-FE	FQDN или IP-адрес домашнего TLM-FE
Информация о взаимодействии (факультативно)	Набор информации о взаимодействии, используемый для идентификации информации о подсоединении к сети и услуге в случае, когда CPE подключено к гостевой сети (например, протокол управления услугой IPTV, идентичность SADS и т. д.)
Абонирование транспортного ресурса (факультативно) (Примечание 1)	
– Идентификатор профиля абонирования транспортирования (Примечание 2)	Идентификатор набора сведений о профиле абонирования транспортирования

**Таблица 12 – Эталонная точка Ni**

<b>Информационный компонент</b>	<b>Описание</b>
– Описание профиля абонирования транспортирования (Примечание 2)	
– Класс обслуживания сети	Представляет класс обслуживания сети, абонированный подключенным СРЕ (например, высший, золотой, серебряный, обычный и т. д.). Может включать класс показателей QoS (например, класс, определенный в [ITU-T Y.1541])
– Абонированная ширина полосы в восходящем направлении	Максимальная пропускная способность, абонированная СРЕ для соединений в восходящем направлении
– Абонированная ширина полосы в нисходящем направлении	Максимальная пропускная способность, абонированная СРЕ для соединений в нисходящем направлении
– Уровень приоритета	Максимальный уровень приоритета, допустимый для любого запроса на резервирование
– Наименование запросчика	Определяет запросчика (запросчиков), разрешенного (разрешенных) в соответствии с абонированием транспортного ресурса
Конфигурация по умолчанию (факультативно) (Примечание 3)	
– Идентификатор конфигурации по умолчанию (Примечание 4)	Идентификатор конфигурации по умолчанию
– Описание конфигурации по умолчанию (Примечание 4)	
– Список управления доступом по умолчанию: список допускаемых пунктов назначения и многоадресных потоков	Список IP-адресов, портов, префиксов и диапазонов портов назначения, допуск к которым предоставляется по умолчанию. В случае многоадресных потоков – список адресов при многоадресной групповой передаче по IP-протоколу и/или список пар (IP-адрес источника, IP-адрес многоадресной передачи), трафик от которых может получать подсоединенное оборудование пользователя. В списке поддерживаются диапазоны адресов. (Примечание 5)
– Список управления доступом по умолчанию: список блокируемых пунктов назначения и многоадресных потоков	Список IP-адресов, портов, префиксов и диапазонов портов назначения, трафик к которым по умолчанию блокируется. В случае многоадресных потоков – список адресов при многоадресной групповой передаче по IP-протоколу и/или список пар (IP-адрес источника, IP-адрес многоадресной передачи), трафик от которых к подсоединенному оборудованию пользователя должен отклоняться. В списке поддерживаются диапазоны адресов. (Примечание 5)
– Пропускная способность для восходящих соединений по умолчанию	Максимальная ширина полосы, которую можно использовать для соединений в восходящем направлении по умолчанию
– Пропускная способность для нисходящих соединений по умолчанию	Максимальная пропускная способность, которую можно использовать для соединений в нисходящем направлении по умолчанию
<p>ПРИМЕЧАНИЕ 1. – Абонирование транспортного ресурса может содержать несколько профилей.</p> <p>ПРИМЕЧАНИЕ 2. – Может присутствовать либо идентификатор профиля абонирования транспортирования, либо описание профиля абонирования транспортирования, но не то и другое одновременно.</p> <p>ПРИМЕЧАНИЕ 3. – Эту информацию использует RACF для настройки транспортных функций перед приемом запросов на резервирование ресурсов от услуг/приложений.</p> <p>ПРИМЕЧАНИЕ 4. – Может присутствовать либо идентификатор конфигурации по умолчанию, либо описание конфигурации по умолчанию, но не то и другое одновременно.</p>	

**Таблица 12 – Эталонная точка Ni**

Информационный компонент	Описание
ПРИМЕЧАНИЕ 5. – Если пункт назначения не фигурирует ни в одном из этих двух списков, принятием решений о пропуске или блокировании трафика в эти адреса управляет RACF. ПРИМЕЧАНИЕ 6. – Доступен только в случае использования услуги мобильности. ПРИМЕЧАНИЕ 7. – Доступен только в случае использования услуги мобильности на базе хост-узла. ПРИМЕЧАНИЕ 8. – Эта информация необязательна, если адрес конечной точки туннеля задается статически или если MLM-FE может получить его, задействуя собственные механизмы. Она доступна только в случае использования услуги мобильности на базе сети.	

**8.1.7 Эталонная точка HGWC-FE – TLM-FE (Nx)**

Эталонная точка Nx позволяет HGWC-FE получать информацию от TLM-FE. Следует иметь в виду, что эталонная точка Nx по своему характеру аналогична эталонной точке S-TC1 (см. пункт 8.3.1), а HGWC-FE ведет себя в этом случае как особый тип функции управления обслуживанием.

**8.1.7.1 Запрос информации**

В таблице 13 описаны элементы информационного потока запроса информации.

**Таблица 13 – Запрос информации (HGWC-FE → TLM-FE)**

Информация об уникальном в глобальном масштабе IP-адресе	Набор сведений об IP-адресе, используемых для определения местоположения сети доступа, к которой подключено CPE
– Уникальный IP-адрес	IP-адрес для идентификации CPE
– Область адреса	Домен адресации IP-адреса (например, префикс подсети или идентификатор VPN)
– Идентичность SCF	Указывает приложение для настройки домашнего шлюза

**8.1.7.2 Ответ на запрос информации**

В таблице 14 описаны элементы информационного потока ответа на запрос информации.

**Таблица 14 – Ответ на запрос информации (TLM-FE → HGWC-FE)**

Идентификатор абонента транспортирования	Уникальный в глобальном масштабе идентификатор подключенного CPE. Он может использоваться для определения местоположения информации об абонировании транспортирования для CPE
Идентификатор физического соединения	Локальный идентификатор для физического соединения транспортной сети доступа, к которой подключено CPE (например, IP-адрес устройства PE-FE, MAC-адрес или идентификатор линии и идентификатор физического порта)
Идентификатор логического соединения	Локальный идентификатор для логического соединения транспортной сети доступа, к которой подключено CPE (например, VPI/VCI API, PPP, метка MPLS, туннель GTP и логический порт)

**8.1.8 Эталонная точка TLM-FE – TLM-FE (Ng)**

Эталонная точка Ng обеспечивает связь между локальным и домашним объектами TLM-FE.

Возможны пять операций: в направлении от локального TLM-FE к домашнему – регистрация местоположения, запрос местоположения и удаление информации о местоположении; в направлении от домашнего TLM-FE к локальному – запрос местоположения; в направлении от локального TLM-FE к локальному – сообщение контекста местоположения.

### 8.1.8.1 Регистрация местоположения

В таблице 15 описаны элементы информационного потока регистрации местоположения.

**Таблица 15 – Регистрация местоположения (локальный TLM-FE → домашний TLM-FE)**

Информация об уникальном в глобальном масштабе IP-адресе	Набор сведений об IP-адресе, используемых для определения местоположения сети доступа, к которой подключено CPE
– Уникальный IP-адрес	IP-адрес для идентификации подключенного CPE
– Область адреса	Домен адресации IP-адреса (например, префикс подсети или идентификатор VPN)
Идентификатор абонента транспортирования	Уникальный в глобальном масштабе идентификатор CPE, запрашивающего IP-соединение
Наименование подсоединенного домена доступа	Наименование домена доступа, к которому подсоединено CPE, или соответствующего оператора
Точка контакта локального TLM-FE	FQDN или IP-адрес локального TLM-FE

### 8.1.8.2 Запрос местоположения

В таблице 16 описаны элементы информационного потока запроса местоположения.

**Таблица 16 – Запрос местоположения (домашний TLM-FE → локальный TLM-FE)**

Информация об уникальном в глобальном масштабе IP-адресе	Набор сведений об IP-адресе, используемых для определения местоположения сети доступа, к которой подключено CPE
– Уникальный IP-адрес	IP-адрес для идентификации подключенного CPE
– Область адреса	Домен адресации IP-адреса (например, префикс подсети или идентификатор VPN)
Идентификатор абонента транспортирования	Уникальный в глобальном масштабе идентификатор подключенного CPE
Наименование подсоединенного домена доступа	Наименование домена доступа, к которому подсоединено CPE, или соответствующего оператора
Точка контакта локального TLM-FE	FQDN или IP-адрес локального TLM-FE

### 8.1.8.3 Ответ на запрос местоположения

Информационный поток ответа на запрос местоположения идентичен информационному потоку ответа на запрос информации через эталонную точку S-TC1 (см. пункт 8.3.1.2).

### 8.1.8.4 Удаление информации о местоположении

В таблице 17 описано содержимое информационного потока удаления информации о местоположении.

**Таблица 17 – Удаление информации о местоположении (локальный TLM-FE → домашний TLM-FE)**

Информация об уникальном в глобальном масштабе IP-адресе	Уникальный в глобальном масштабе IP-адрес, соответствующий UNI, который связан с подсоединенным к сети пользователем
– Уникальный IP-адрес	IP-адрес для идентификации CPE
– Область адреса	Домен адресации IP-адреса (например, префикс подсети или идентификатор VPN)
Идентификатор абонента транспортирования	Уникальный в глобальном масштабе идентификатор CPE, запрашивающего транспортный ресурс. Может использоваться для определения местоположения информации об абонировании транспортирования для CPE

### 8.1.8.5 Сообщение контекста местоположения

В таблице 18 описаны элементы информационного потока сообщения контекста местоположения.

**Таблица 18 – Сообщение контекста местоположения  
(локальный TLM-FE → локальный TLM-FE)**

Информация об уникальном в глобальном масштабе IP-адресе	Набор сведений об IP-адресе, используемых для определения местоположения сети доступа, к которой подключено CPE
– Уникальный IP-адрес	IP-адрес для идентификации подключенного CPE
– Область адреса	Домен адресации IP-адреса (например, префикс подсети или идентификатор VPN)
Идентификатор абонента транспортирования	Уникальный в глобальном масштабе идентификатор подключенного CPE
Наименование подсоединенного домена доступа	Наименование домена доступа или оператора гостевой сети
Точка контакта локального TLM-FE	FQDN или IP-адрес локального TLM-FE
Идентификатор конфиденциальности (Примечание 1)	Указывает на возможность экспорта услугам и приложениям информации о местоположении
Абонирование транспортного ресурса (Примечания 2 и 3)	
– Идентификатор профиля абонирования транспортирования (Примечание 4)	Идентификатор набора сведений о профиле абонирования транспортирования
– Описание профиля абонирования транспортирования (Примечание 4)	
– Класс обслуживания сети	Представляет класс обслуживания сети, абонированный CPE (например, высший, золотой, серебряный, обычный и т. д.). Может включать класс показателей QoS (например, класс, определенный в [ITU-T Y.1541])
– Абонированная ширина полосы в восходящем направлении	Максимальная пропускная способность, абонированная CPE для соединений в восходящем направлении
– Абонированная ширина полосы в нисходящем направлении	Максимальная пропускная способность, абонированная CPE для соединений в нисходящем направлении
– Уровень приоритета	Максимальный уровень приоритета, допустимый для любого запроса на резервирование
– Наименование запросчика	Определяет запросчика (запросчиков), разрешенного (разрешенных) в соответствии с абонированием транспортного ресурса
Конфигурация по умолчанию (факультативно)	
– Идентификатор конфигурации по умолчанию (Примечание 5)	Идентификатор конфигурации по умолчанию
– Описание конфигурации по умолчанию (Примечание 5)	
– Список управления доступом по умолчанию: список допускаемых пунктов назначения и многоадресных потоков	Список IP-адресов, портов, префиксов и диапазонов портов назначения, доступ к которым предоставляется по умолчанию. В случае многоадресных потоков – список адресов при многоадресной групповой передаче по IP-протоколу и/или список пар (IP-адрес источника, IP-адрес многоадресной передачи), трафик от которых может получать подсоединенное оборудование пользователя. В списке поддерживаются диапазоны адресов. (Примечание 6)

**Таблица 18 – Сообщение контекста местоположения  
(локальный TLM-FE → локальный TLM-FE)**

<ul style="list-style-type: none"> <li>– Список управления доступом по умолчанию: список пунктов назначения и многоадресных потоков, в доступе к которым отказано</li> </ul>	<p>Список IP-адресов, портов, префиксов и диапазонов портов назначения, трафик к которым предоставляется по умолчанию. В случае многоадресных потоков – список адресов при многоадресной групповой передаче по IP-протоколу и/или список пар (IP-адрес источника, IP-адрес многоадресной передачи), трафик от которых к подсоединенному оборудованию пользователя должен отклоняться. В списке поддерживаются диапазоны адресов. (Примечание 6)</p>
<ul style="list-style-type: none"> <li>– Пропускная способность для восходящих соединений по умолчанию</li> </ul>	<p>Максимальная ширина полосы, которую можно использовать для соединений в восходящем направлении по умолчанию</p>
<ul style="list-style-type: none"> <li>– Пропускная способность для нисходящих соединений по умолчанию</li> </ul>	<p>Максимальная пропускная способность, которую можно использовать для соединений в нисходящем направлении по умолчанию</p>
<p>ПРИМЕЧАНИЕ 1. – Указание о наличии у приложений возможности доступа к информации о местоположении в зависимости от уровня их безопасности.</p> <p>ПРИМЕЧАНИЕ 2. – Абонирование транспортного ресурса может содержать несколько профилей абонирования транспортирования.</p> <p>ПРИМЕЧАНИЕ 3. – Может присутствовать либо идентификатор профиля абонирования транспортирования, либо описание профиля абонирования транспортирования, но не то и другое одновременно.</p> <p>ПРИМЕЧАНИЕ 4. – Эту информацию использует RACF для настройки транспортных функций перед приемом запросов на резервирование ресурсов от услуг/приложений.</p> <p>ПРИМЕЧАНИЕ 5. – Может присутствовать либо идентификатор конфигурации по умолчанию, либо описание конфигурации по умолчанию, но не то и другое одновременно.</p> <p>ПРИМЕЧАНИЕ 6. – Если пункт назначения не фигурирует ни в одном из этих двух списков, принятием решений о пропуске или блокировании трафика в эти адреса управляет RACF.</p>	

### 8.1.9 Эталонная точка TUP-FE – TAA-FE (Nb)

Настоящая Рекомендация не устанавливает требований к эталонной точке Nb, то есть TAA-FE и TUP-FE размещаются совместно или соединяются через нестандартизированный интерфейс.

## 8.2 Эталонная точка между NACF и функциями управления ресурсами и допуском (RACF)

### 8.2.1 Эталонная точка между TLM-FE и RACF (Ru)

Эталонная точка Ru позволяет PD-FE взаимодействовать с NACF для проверки информации о профиле абонирования транспортирования CPE и информации о связывании адреса логического/физического порта с присвоенным IP-адресом.

Эталонная точка Ru является внутридоменной эталонной точкой.

Эталонная точка Ru позволяет следующий обмен информацией:

- NACF принудительно доставляет в PD-FE информацию о профиле абонирования транспортирования;
- PD-FE получает в опросном режиме из NACF информацию о профиле абонирования транспортирования.

Дополнительную информацию см. в пункте 8.4 [ITU-T Y.2111].

### 8.3 Эталонная точка между NACF и функциями управления обслуживанием

#### 8.3.1 Эталонная точка между TLM-FE и функциями управления обслуживанием (S-TC1)

Эталонная точка S-TC1 позволяет функциям управления обслуживанием (SCF) получать от TLM-FE информацию о характеристиках сеанса связи по протоколу IP, используемого для доступа к таким функциям (например, информацию о местоположении в сети). Вид, в котором TLM-FE предоставляет информацию о местоположении, зависит от запрашивающего объекта (запросчика).

Через эталонную точку S-TC1 проходят следующие информационные потоки:

- запрос информации;
- ответ на запрос информации;
- запрос регистрации события;
- ответ на запрос регистрации события;
- запрос события уведомления;
- ответ на запрос события уведомления.

##### 8.3.1.1 Запрос информации

В таблице 19 описаны элементы информационного потока запроса информации.

**Таблица 19 – Запрос информации (SCF → TLM-FE)**

Информация об уникальном в глобальном масштабе IP-адресе (Примечание 1)	Набор сведений об IP-адресе, используемых для определения местоположения сети доступа, к которой подключено CPE
– Уникальный IP-адрес	IP-адрес для идентификации подключенного CPE
– Область адреса	Домен адресации IP-адреса (например, префикс подсети или идентификатор VPN). (Примечание 2)
Идентификатор абонента транспортирования (Примечание 1)	Уникальный в глобальном масштабе идентификатор подключенного CPE
– Идентичность SCF	Идентификатор функции управления обслуживанием, совершающей запрос
ПРИМЕЧАНИЕ 1. – Указывается либо информация об уникальном в глобальном масштабе IP-адресе, либо идентификатор абонента транспортирования. ПРИМЕЧАНИЕ 2. – Домен адресации известен SCF либо из данных конфигурации (в этом случае все оконечное оборудование, которое обслуживается SCF, принадлежит к одному домену адресации), либо на основании физического или логического интерфейса, через который был получен запрос на обслуживание, повлекший запрос местоположения.	

##### 8.3.1.2 Ответ на запрос информации

В таблице 20 описаны элементы информационного потока ответа на запрос информации.

**Таблица 20 – Ответ на запрос информации (TLM-FE → SCF)**

Идентификатор абонента транспортирования (факультативно)	Уникальный в глобальном масштабе идентификатор подключенного CPE. (Примечание 1)
Информация о местоположении (факультативно) (Примечание 2)	Информация о местоположении (или указатель на такую информацию) в виде, подходящем для функции управления обслуживанием, от которой поступил запрос
Точка контакта RACF (факультативно)	FQDN или IP-адрес объекта RACF, которому направлен запрос на ресурс (например, адрес PD-FE)
Тип CPE (факультативно)	Тип CPE
Тип сети доступа (факультативно)	Тип сети доступа, к которой подключено CPE

**Таблица 20 – Ответ на запрос информации (TLM-FE → SCF)**

Идентификатор физического соединения (факультативно)	Локальный идентификатор для физического соединения транспортной сети доступа, к которой подключено CPE (например, IP-адрес устройства PE-FE, MAC-адрес или идентификатор линии и физический порт)
Идентификатор логического соединения (факультативно)	Локальный идентификатор для логического соединения транспортной сети доступа, к которой подключено CPE (например, VPI/VCI APII, PPP, метка MPLS, туннель GTP и логический порт)
<p>ПРИМЕЧАНИЕ 1. – Этот идентификатор может использоваться SCF при взаимодействии с RACF.</p> <p>ПРИМЕЧАНИЕ 2. – Раскрытие информации о местоположении зависит от запрашивающего приложения и установленных для данного абонента ограничений конфиденциальности. Ограничения конфиденциальности задаются в индикаторе конфиденциальности, который хранится в TLM-FE.</p>	

### 8.3.1.3 Запрос регистрации события

В таблице 21 описаны элементы информационного потока запроса регистрации события. Этот информационный поток неприменим, если в качестве SCF выступает P-CSCF [ITU-T Y.2021].

**Таблица 21 – Запрос регистрации события (SCF → TLM-FE)**

Длительность абонирования	Длительность запрашиваемой подписки на конкретное событие
Идентификатор абонента транспортирования (Примечание 1)	Уникальный в глобальном масштабе идентификатор подключенного CPE
Событие	Тип события (например, событие входа пользователя) и формат описания ретрансляции события/уведомления о событии
Информация об уникальном в глобальном масштабе IP-адресе (факультативно) (Примечание 1)	Набор сведений об IP-адресе, используемых для определения местоположения сети доступа, к которой подключено CPE
– Уникальный IP-адрес	IP-адрес для идентификации подключенного CPE
– Область адреса	Домен адресации IP-адреса (например, префикс подсети или идентификатор VPN). (Примечание 2)
Идентичность SCF (факультативно)	Идентификатор функции управления обслуживанием, совершающей запрос
<p>ПРИМЕЧАНИЕ 1. – Должен быть представлен по крайней мере один из двух идентификаторов (идентификатор абонента транспортирования или информация об уникальном в глобальном масштабе IP-адресе).</p> <p>ПРИМЕЧАНИЕ 2. – Домен адресации известен SCF либо из данных конфигурации (в этом случае все оборудование пользователя, которое обслуживается SCF, принадлежит к одному домену адресации), либо на основании физического или логического интерфейса, через который был получен соответствующий запрос на обслуживание.</p>	

### 8.3.1.4 Ответ на запрос регистрации события

В таблице 22 описаны элементы информационного потока ответа на запрос регистрации события. Этот информационный поток неприменим, если в качестве SCF выступает P-CSCF [ITU-T Y.2021].

**Таблица 22 – Ответ на запрос регистрации события (TLM-FE → SCF)**

Действие обновления	Административное действие/информация по данному событию, например ACTIVATED (запрос регистрации события успешно принят, и уведомление о данном событии включено)
Идентификатор абонента транспортирования (Примечание)	Уникальный в глобальном масштабе идентификатор подключенного CPE
Событие	Тип события (например, вход пользователя)
Информация об уникальном в глобальном масштабе IP-адресе (Примечание)	Набор сведений об IP-адресе, используемых для определения местоположения сети доступа, к которой подключено CPE
– Уникальный IP-адрес	IP-адрес для идентификации подключенного CPE
– Область адреса	Домен адресации IP-адреса (например, префикс подсети или идентификатор VPN)
ПРИМЕЧАНИЕ. – Должен быть представлен по крайней мере один из двух идентификаторов (идентификатор абонента транспортирования или информация об уникальном в глобальном масштабе IP-адресе).	

### 8.3.1.5 Запрос события уведомления

В таблице 23 описаны элементы информационного потока запроса события уведомления. Этот информационный поток неприменим, если в качестве SCF выступает P-CSCF [ITU-T Y.2021].

**Таблица 23 – Запрос события уведомления (TLM-FE → SCF)**

Информация об уникальном в глобальном масштабе IP-адресе	Набор сведений об IP-адресе, используемых для определения местоположения сети доступа, к которой подсоединено CPE
– Уникальный IP-адрес	IP-адрес для идентификации подсоединенного CPE
– Область адреса	Домен адресации IP-адреса (например, префикс подсети или идентификатор VPN)
Идентификатор абонента транспортирования	Уникальный в глобальном масштабе идентификатор подключенного CPE
Событие	Тип события (например, вход пользователя)

### 8.3.1.6 Ответ на запрос события уведомления

В таблице 24 описаны элементы информационного потока ответа на запрос события уведомления. Этот информационный поток неприменим, если в качестве SCF выступает P-CSCF [ITU-T Y.2021].

**Таблица 24 – Ответ на запрос события уведомления (SCF → TLM-FE)**

Информация об уникальном в глобальном масштабе IP-адресе	Набор сведений об IP-адресе, используемых для определения местоположения сети доступа, к которой подсоединено CPE
– Уникальный IP-адрес	IP-адрес для идентификации подсоединенного CPE
– Область адреса	Домен адресации IP-адреса (например, префикс подсети или идентификатор VPN)
Идентификатор абонента транспортирования	Уникальный в глобальном масштабе идентификатор подключенного CPE
Событие	Тип события
Результат	Код результата (например, успех, постоянная ошибка и т. д.)

## 8.4 Эталонные точки между NACF и CPE

### 8.4.1 Эталонные точки для аутентификации и выделения IP-адреса (T-U1 и TC-T1)

Между NACF и CPE нет эталонной точки, непосредственно предназначенной для поддержки аутентификации и выделения IP-адреса. Связь между NACF и CPE осуществляется через функциональный объект ретрансляции для обеспечения доступа (AR-FE) в транспортных функциях с использованием эталонной точки T-U1 между CPE и AR-FE и эталонной точки TC-T1 между AR-FE и NACF.

Окончанием для эталонной точки T-U1 на стороне CPE может служить HGW или TE. Последнее применяется в случае прямого соединения TE с AR-FE.

Эталонная точка T-U1 позволяет CPE инициировать запросы на выделение IP-адреса и, возможно, других параметров конфигурации сети для доступа к сети. AR-FE принимает эти запросы и ретранслирует их в адрес AM-FE в NACF через эталонную точку TC-T1.

Запросы на выделение IP-адреса и параметров конфигурации сети выполняются в виде запроса по протоколу DHCP [b-IETF RFC 2131] или PPP [b-IETF RFC 1661].

Если используется DHCP, в состав транспортных функций входит функциональный объект ретрансляции для обеспечения доступа (AR-FE), действующий в качестве ретранслятора DHCP между DHCP-клиентами в CPE и DHCP-сервером в NACF.

Прежде чем передавать NACF запрос через эталонную точку TC-T1, AR-FE может добавить информацию о местоположении к информации, принятой от CPE через эталонную точку T-U1. Эталонная точка T-U1 позволяет CPE передавать NACF регистрационные данные пользователя (пароль, маркер, сертификат и т. д.) для аутентификации доступа к сети. Кроме того, эталонная точка T-U1 может обеспечивать для NACF возможность передавать CPE параметр аутентификации для осуществления аутентификации сети в случаях, когда требуется процедура взаимной аутентификации. По результатам аутентификации AM-FE авторизует доступ CPE к сети или отказывает в доступе.

ПРИМЕЧАНИЕ. – Когда для выделения IP-адресов и параметров конфигурации CPE между NACF и CPE используется DHCP, возможными протоколами для аутентификации между NACF и CPE является IEEE 802.1X [b-IEEE 802.1X] и PANA [b-IETF RFC 4058].

### 8.4.2 Эталонная точка между HGWC-FE и CPE (TC-Ux)

Эталонная точка TC-Ux позволяет HGWC-FE настраивать HGW, запускать тесты при техническом обслуживании, вести мониторинг производительности и принимать уведомления. Эталонная точка TC-Ux используется при инициализации и обновлении HGW для предоставления ему дополнительной информации о конфигурации сети в случаях, когда эта информация недоступна через эталонную точку T-U1, чтобы обеспечить HGW доступ к функциям управления обслуживанием СПП.

HGWC-FE может также управлять подключенными к HGW устройствами TE (косвенно через HGW или напрямую) для целей настройки, технического обслуживания, мониторинга производительности и рассылки уведомлений.

Эталонная точка TC-Ux поддерживает следующие процедуры:

- идентификацию/аутентификацию HGW со стороны HGWC-FE, например, для передачи соответствующей информации о конфигурации (обновления микропрограммы) от HGWC-FE;
- аутентификацию HGWC-FE со стороны HGW, например перед тем, как HGW примет переданную ему удаленно конфигурацию;
- запуск с HGWC-FE тестов при техническом обслуживании HGW и передачу результатов тестов с HGW;
- настройку HGW;
- уведомление HGWC-FE о доступности TE;
- обеспечение настройки и обновления TE;
- запуск с HGWC-FE тестов при техническом обслуживании TE и передачу результатов тестов с TE.

ПРИМЕЧАНИЕ. – Возможными протоколами для этой эталонной точки является TR-069 [b-DSL Forum TR-069], HTTP [b-IETF RFC 2616], FTP [b-IETF RFC 959] и TFTP [b-IETF RFC 783].

## **8.5 Эталонные точки между NACF и функциями управления мобильностью и контроля мобильности (MMCF)**

### **8.5.1 Эталонная точка между TLM-FE и MLM-FE(P) (M1)**

Эталонная точка M1 позволяет TLM-FE взаимодействовать с MLM-FE(P) для принудительной доставки параметров услуг мобильности, таких как материал ключа, адрес опорной точки и т. д.

Эталонная точка M1 является внутридоменной эталонной точкой.

Эталонная точка M1 позволяет следующий обмен информацией:

- TLM-FE принудительно доставляет в MLM-FE(P) информацию о параметрах услуг мобильности.

Для получения дополнительно информации см. пункт 6.5 [ITU-T Y.2018].

### **8.5.2 Эталонная точка между TLM-FE и HDC-FE (M2)**

Эталонная точка M2 позволяет TLM-FE взаимодействовать с HDC-FE для принудительной доставки параметров услуг мобильности, таких как материал ключа, в целях поддержки установления требуемой ассоциации безопасности между HDC-FE и UE.

Эталонная точка M2 является внутридоменной эталонной точкой.

Эталонная точка M2 позволяет следующий обмен информацией:

- TLM-FE принудительно доставляет в HDC-FE информацию о параметрах услуг мобильности.

Для получения дополнительно информации см. пункт 6.5 [ITU-T Y.2018].

### **8.5.3 Эталонная точка между TLM-FE и NID-FE (M13)**

Эталонная точка M13 позволяет TLM-FE взаимодействовать с NID-FE для принудительной доставки параметров услуг мобильности, таких как материал ключа, в целях поддержки установления требуемой ассоциации безопасности между NID-FE и UE.

Эталонная точка M13 является внутридоменной эталонной точкой.

Эталонная точка M13 позволяет следующий обмен информацией:

- TLM-FE принудительно доставляет в NID-FE информацию о параметрах услуг мобильности.

Для получения дополнительно информации см. пункт 6.5 [ITU-T Y.2018].

## **9 Соображения безопасности**

Требования безопасности в рамках функциональных требований и архитектуры NACF задаются требованиями к безопасности СПП [ITU-T Y.2701], а также требованиями к безопасности авторизации и аутентификации в СПП [ITU-T Y.2702].

## Дополнение I

### Отображение на сетевые роли

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации.)

Архитектура NACF не предполагает каких-либо определенных бизнес-ролей. Однако в целях удовлетворения требований кочевничества и мобильности архитектура NACF может быть отображена на различные функциональные сетевые роли, присутствующие в среде фиксированного широкополосного доступа, как показано на рисунке I.1.



Рисунок I.1 – Функциональные сетевые роли в СПП

Отображение архитектуры NACF показано на рисунках I.2 и I.3. Примером сети доступа на этих рисунках служит сеть доступа xDSL или точка доступа WLAN.

На рисунке I.2 приведен сценарий 1, в котором функции управления обслуживанием (частично) предоставляет гостевая сеть СПП. Рисунок I.3 поясняет сценарий 2, в котором функции управления обслуживанием предоставляет домашняя сеть СПП.

Рисунки I.4 и I.5 иллюстрируют сценарии 3 и 4, в которых посещающее CPE не выполняет аутентификацию доступа. На рисунке I.4 посещающее CPE может получить доступ к своим домашним услугам посредством соглашения о роуминге на уровне функций управления обслуживанием. Однако определение такого сценария выходит за рамки настоящей Рекомендации. На рисунке I.5 приведен сценарий, в котором функции управления обслуживанием домашней сети обращаются к TLM-FE в гостевой сети за информацией о местоположении через прокси-сервер TLM-FE в домашней сети. Эталонная точка Ng используется здесь для связи между двумя объектами TLM-FE.

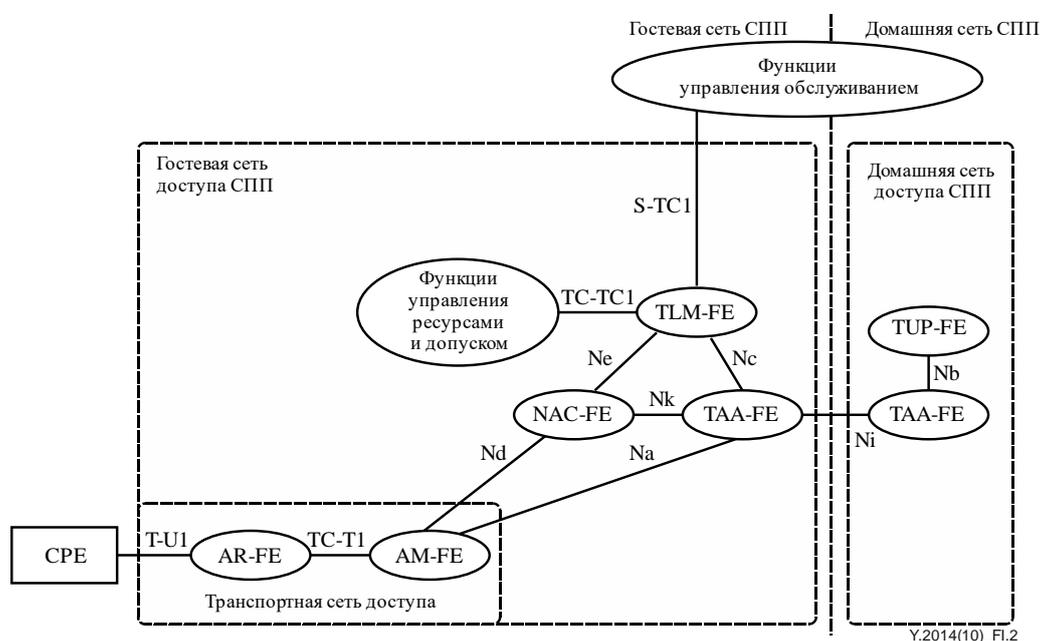
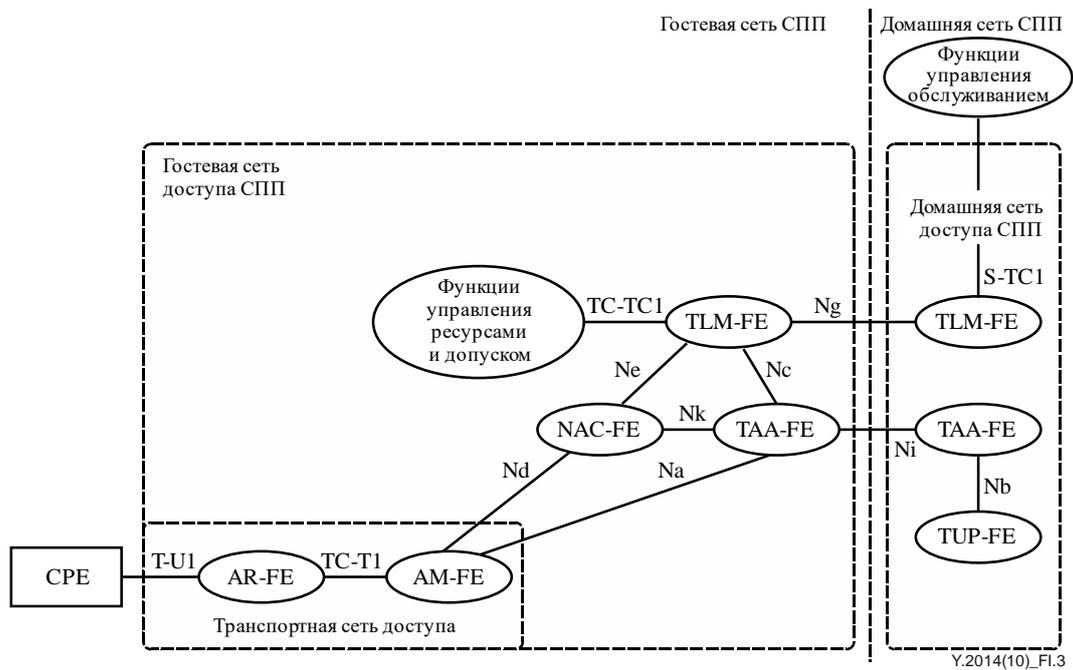
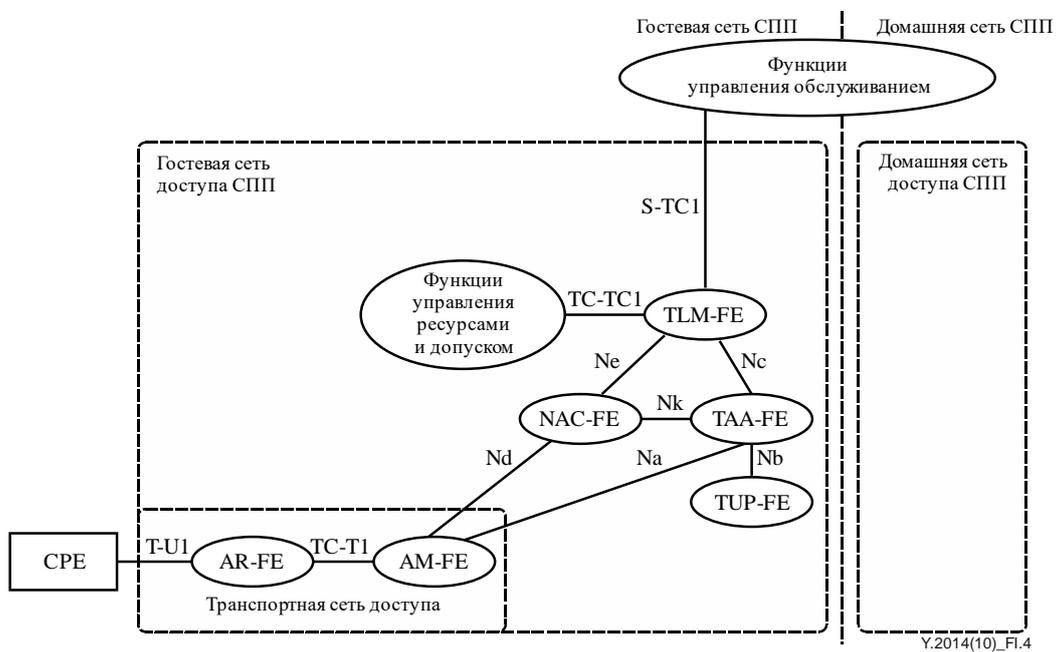


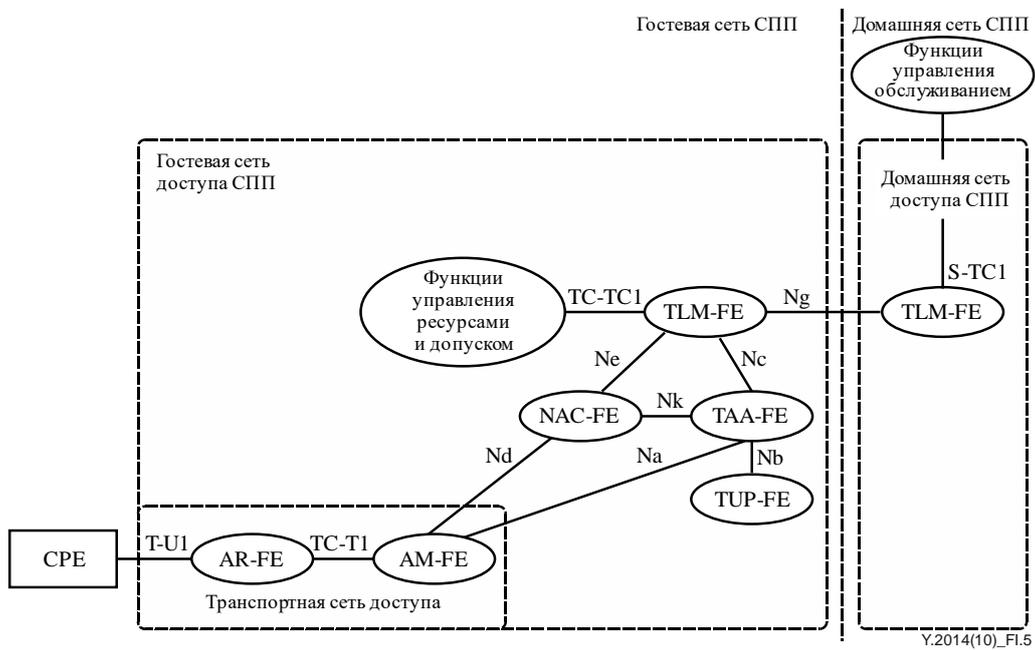
Рисунок I.2 – Отображение NACF на функциональные сетевые роли – сценарий 1



**Рисунок I.3 – Отображение NACF на функциональные сетевые роли – сценарий 2 (услуги СПП из домашней сети)**



**Рисунок I.4 – Отображение NACF на функциональные сетевые роли – сценарий 3**



**Рисунок I.5 – Отображение NACF на функциональные сетевые роли – сценарий 4**

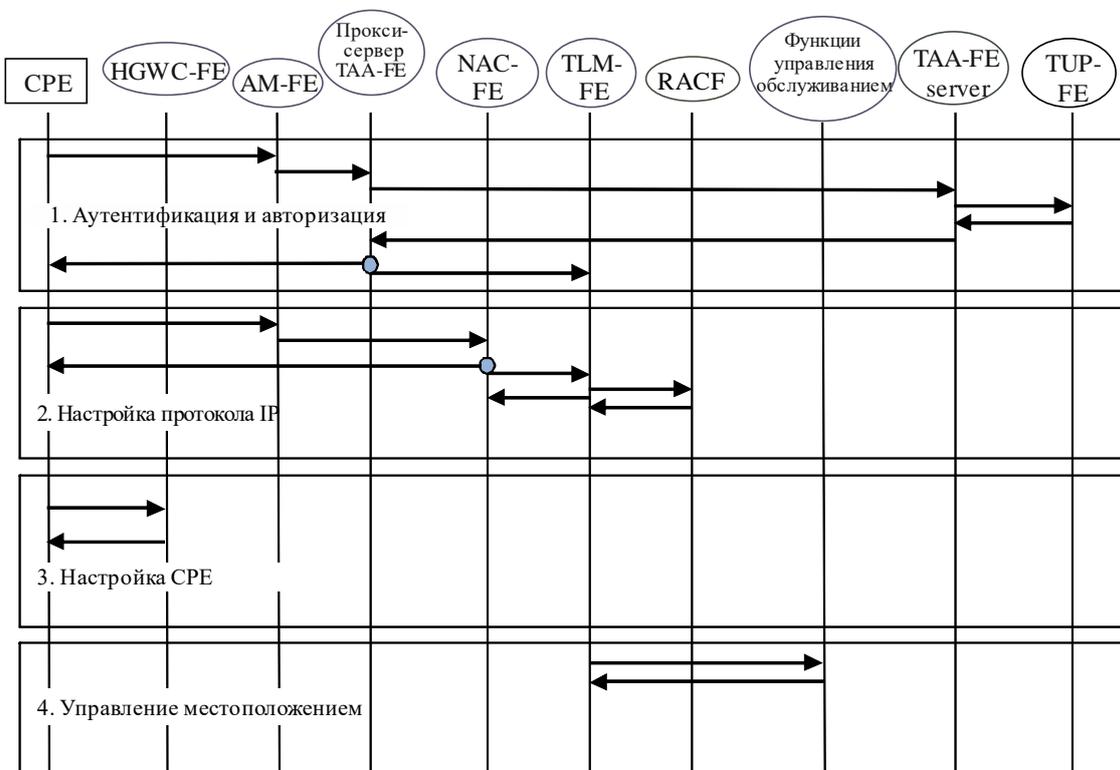
## Дополнение II

### Информационные потоки

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации.)

#### II.1 Высокоуровневые информационные потоки

В данном разделе описываются высокоуровневые информационные потоки, определяющие процесс подключения к сети и передачу информации о профиле абонирования транспортирования внутри NACF и в адрес RACF.



Y.2014(10)\_Fil.1

Рисунок II.1 – Высокоуровневые информационные потоки

NACF участвует в нескольких этапах процесса подключения к сети. На рисунке II.1 показаны высокоуровневые информационные потоки и различные процедуры, выполняемые NACF. В зависимости от используемой технологии (например, [b-IEEE 802.1X], [b-IETF RFC 4058] и т. д.) и конфигурации эти этапы могут следовать в другом, чем на рисунке II.1, порядке.

- 1 На первом этапе процесса подключения к сети выполняется аутентификация и авторизация CPE. Для аутентификации применяются механизмы и идентификационные данные, описанные в разделах 6, 7 и 8. Подразумевается, что используются аутентификация линии и/или аутентификация доступа. Применимые идентификаторы – это идентификатор пользователя и регистрационные данные, предоставленные пользователем, или идентификатор CPE. На этапе 1 также осуществляется авторизация доступа к сети на основании профиля абонирования транспортирования. Из домашней сети СПП в гостевую сеть СПП (с сервера TAA-FE в прокси-сервер TAA-FE) может быть загружен конкретный профиль абонирования транспортирования, связанный, например, с QoS. В случае успешной аутентификации и авторизации CPE для использования ресурсов сети доступа производится настройка сети доступа в соответствии с профилем абонирования транспортирования. Это, в частности, предполагает необходимость передать в TLM-FE через эталонную точку Nc информацию о профиле абонирования транспортирования, относящуюся конкретно к аутентифицированному пользователю. Информация о профиле включает по меньшей мере

идентификатор логического соединения (то есть идентификатор линии), идентификатор абонента транспортирования, информацию об абонировании транспортного ресурса, которая может представлять собой профиль QoS, загруженный из домашней сети СПП, или профиль конфигурации по умолчанию, и идентификатор периферийного устройства PE-FE.

ПРИМЕЧАНИЕ 1. – Этап 1 может проходить перед выполнением или во время выполнения процедуры выделения IP-адреса (этап 2).

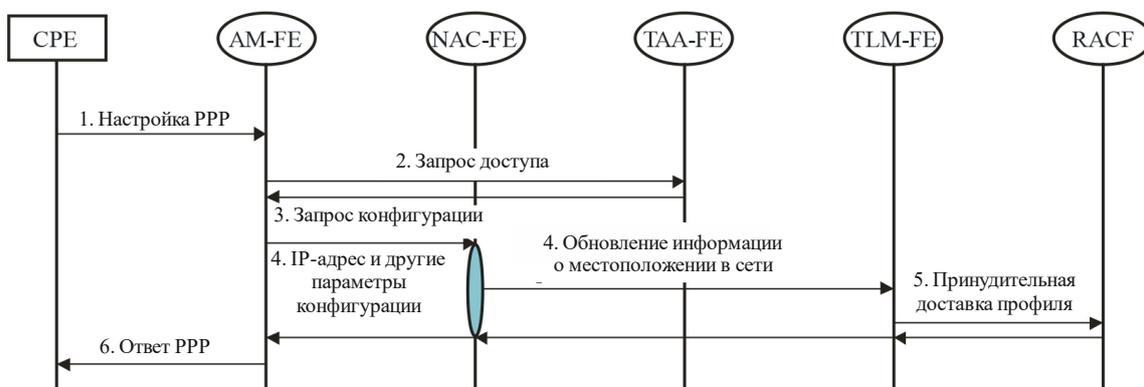
- 2 Динамическое выделение IP-адреса CPE и предоставление ему параметров IP-конфигурации. На этапе 2 NAC-FE назначает параметры IP-конфигурации. NAC-FE получает идентификатор логического соединения (то есть идентификатор линии) посредством сигнализации через эталонную точку TC-T1 и устанавливает соответствие между назначенными параметрами IP-конфигурации и идентификатором логического соединения. Информация об этом соответствии пересылается (через эталонную точку Ne) в TLM-FE, который сопоставляет ее с идентификатором абонента транспортирования и профилем абонирования транспортирования, после чего принудительно доставляет эту информацию в RACF через эталонную точку Ru. RACF настраивает свою функциональность в соответствии с информацией о профиле абонирования транспортирования, полученной от TLM-FE.
- 3 HGWC-FE может настраивать параметры HGW.
- 4 Функции управления обслуживанием СПП получают информацию о местоположении от TLM-FE через эталонную точку S-TC1. Если функциям управления обслуживанием СПП требуется доступ к информации о местоположении в другом домене, сигнализация для получения такой информации должна осуществляться через прокси-сервер TLM-FE, расположенный в той же сети, что и функции управления обслуживанием СПП, которые запрашивают эту информацию. Основные параметры для получения информации о местоположении – это идентификатор абонента транспортирования и/или IP-адрес, выделенный CPE компонентом NACF.

ПРИМЕЧАНИЕ 2. – Для получения дополнительной информации о процедуре подсоединения с обеспечением мобильности см. пункт 7.2 [ITU-T Y.2018].

## II.2 Аутентификация на основе PPP

В данном разделе приведены примеры информационных потоков NACF в случае использования PPP [b-IETF RFC 1661]. Приведенные примеры не рассчитаны на то, чтобы проиллюстрировать всю функциональность NACF в случае аутентификации на основе PPP.

ПРИМЕЧАНИЕ. – Содержащаяся здесь информация дана только в качестве примера.



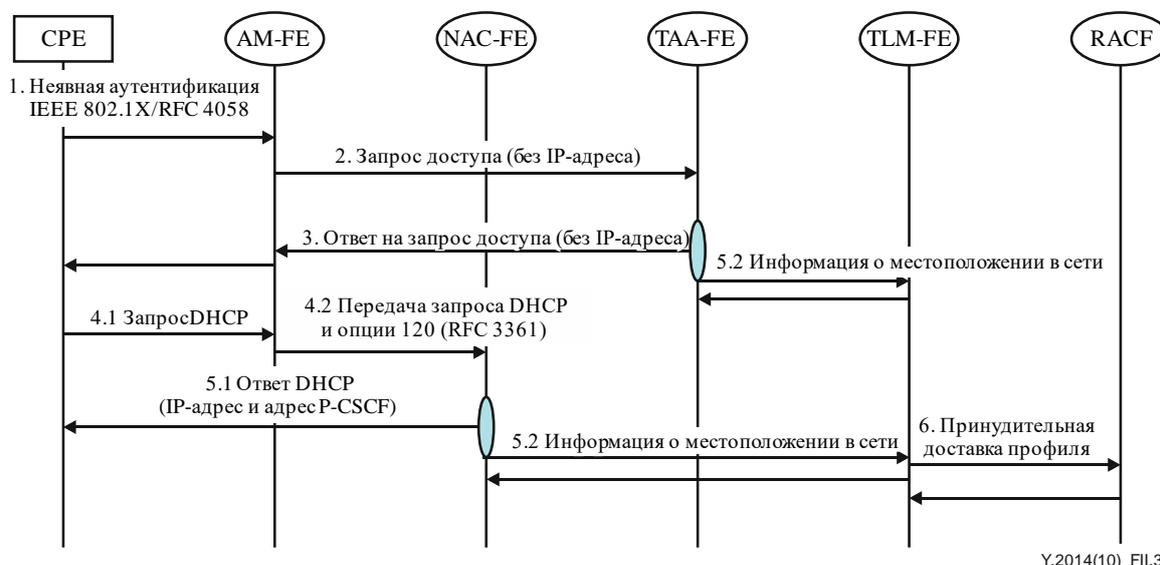
Y.2014(10)\_FII.2

Рисунок II.2 – Подсоединение к сети на основе PPP

- 1 CPE инициирует запрос по протоколу PPP на получение IP-адреса. PPP используется для аутентификации доступа и линии.
- 2 AM-FE ретранслирует запрос PPP в запрос доступа к TAA-FE для аутентификации.
- 3 AM-FE передает NAC-FE запрос конфигурации для получения IP-адреса и других параметров, включая (в данном случае) IP-адрес функции управления обслуживанием СПП (например, P-CSCF).
- 4 NAC-FE выделяет IP-адрес и отвечает AM-FE. Кроме того, NAC-FE передает TLM-FE информацию о связи между выделенным IP-адресом, идентификатором линии и идентификационными данными периферийного устройства PE-FE.
- 5 TLM-FE принудительно доставляет информацию об этой связи в RACF через эталонную точку Ru.
- 6 AM-FE направляет CPE ответ PPP, содержащий выделенный IP-адрес и другие параметры, в том числе IP-адрес функции управления обслуживанием СПП (например, P-CSCF).

### II.3 Режим DHCP

В данном разделе приведены примеры информационных потоков NACF в случае использования DHCP. Приведенные примеры не рассчитаны на то, чтобы проиллюстрировать всю функциональность NACF в режиме DHCP.



**Рисунок II.3 – Подсоединение к сети на основе DHCP с неявной аутентификацией доступа или аутентификацией по протоколам [b-IEEE 802.1X]/[b-IETF RFC 4058]**

- 1 СРЕ инициирует аутентификацию по протоколам [b-IEEE 802.1X]/[b-IETF RFC 4058]. Как вариант, возможна неявная аутентификация линии, если кочевничество не предусмотрено.
- 2 АМ-FE связывается с ТАА-FE для аутентификации.
- 3 После успешной аутентификации ТАА-FE передает ответ с ее результатом. ТАА-FE уведомляет ТЛМ-FE, что СРЕ аутентифицировано.
- 4 СРЕ посредством запроса DHCP запрашивает IP-адрес (согласно потоку 4.1), а также – с использованием опции 120 DHCP – адрес функции управления обслуживанием СПП, например Р-CSCF (согласно потоку 4.2). АМ-FE ретранслирует этот запрос в НАС-FE, который действует в качестве сервера DHCP.
- 5 НАС-FE выделяет IP-адрес и отвечает СРЕ. Кроме того, НАС-FE уведомляет ТЛМ-FE о выделении IP-адреса СРЕ, указанному на шаге 3.
- 6 ТЛМ-FE принудительно доставляет в RACF информацию о связи между выделенным IP-адресом, идентификатором линии и идентификационными данными периферийного устройства РЕ-FE через интерфейс Ru.

НАС-FE предоставляет FQDN или IP-адрес точки контакта функции управления обслуживанием СПП (например, Р-CSC-FE), который АМ-FE ретранслирует в адрес СРЕ.

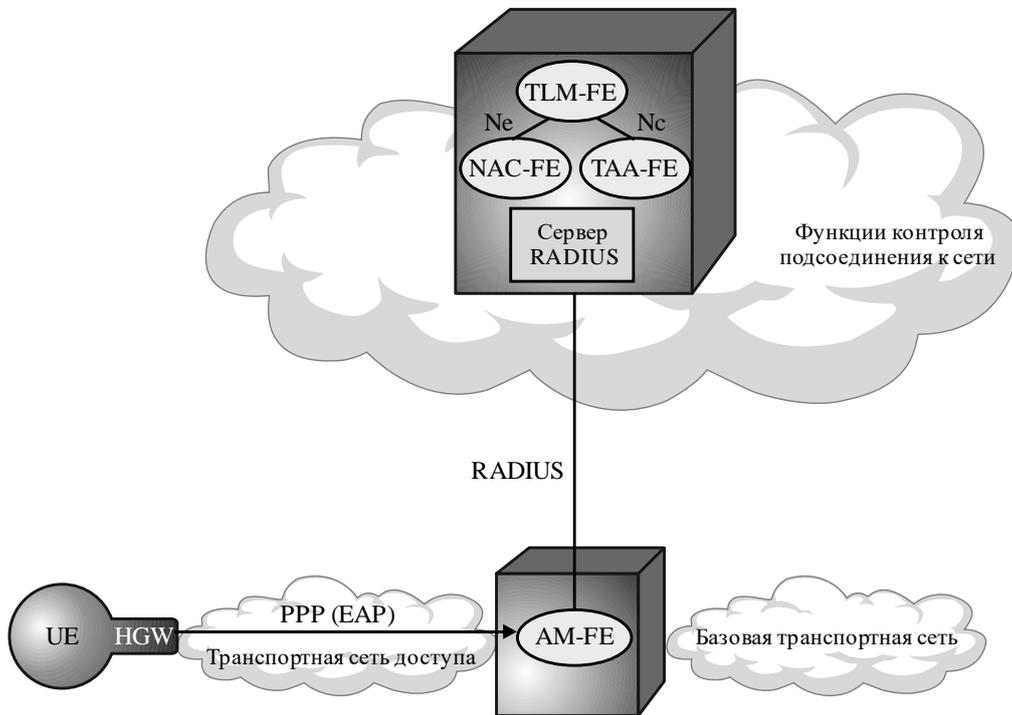
## Дополнение III

### Физические конфигурации

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации.)

В настоящем Дополнении дается ссылка на метод аутентификации EAP [b-IETF RFC 3748]. Вопрос о выборе механизма аутентификации для NACF подлежит дальнейшему изучению.

#### III.1 Случай PPP

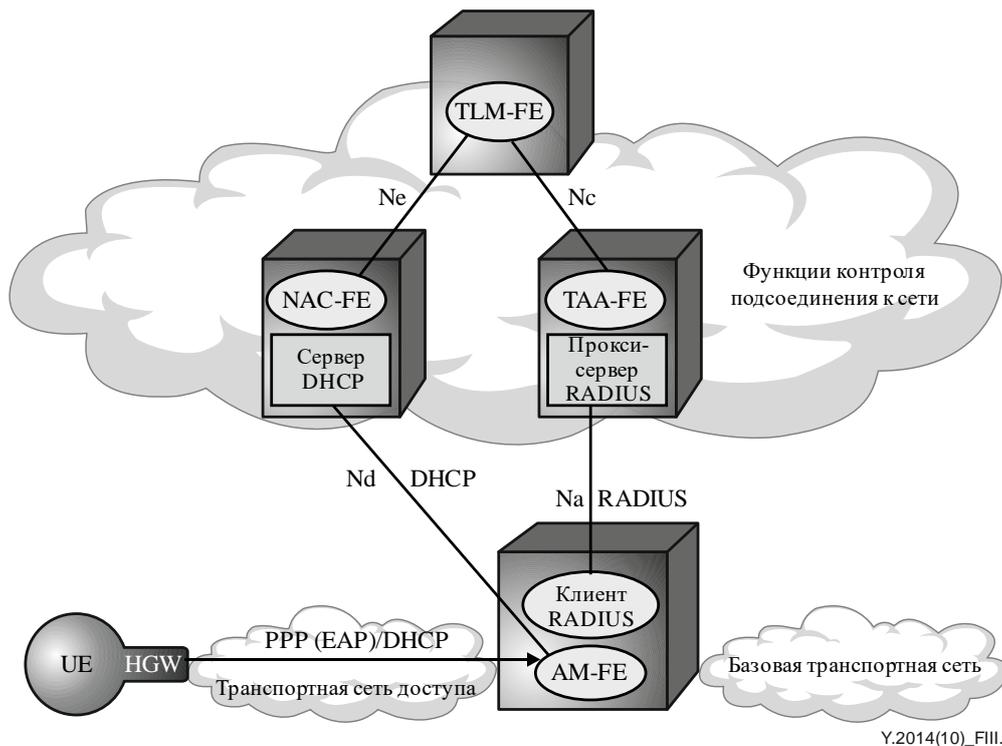


ПРИМЕЧАНИЕ. – Для простоты интерфейсы к RACF не показаны.

Y.2014(10)\_FIII.

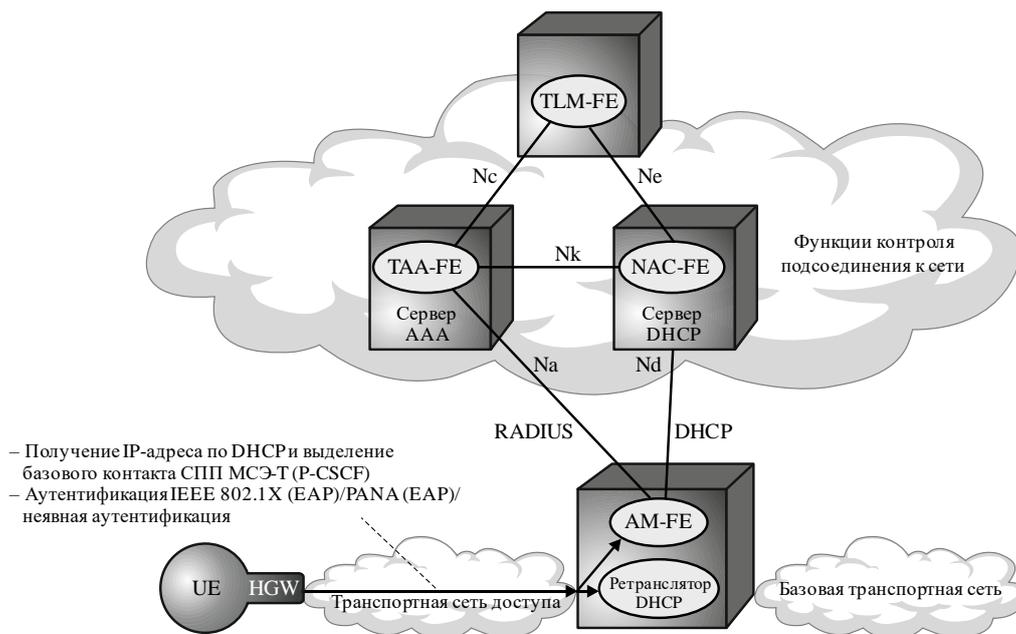
Рисунок III.1 – Конфигурация на основе PPP

### III.2 Конфигурация PPP с DHCP



**Рисунок III.2 – Конфигурация на основе PPP с IP-конфигурацией на основе DHCP (выделение точки контакта функций управления обслуживанием СПП домашнему шлюзу)**

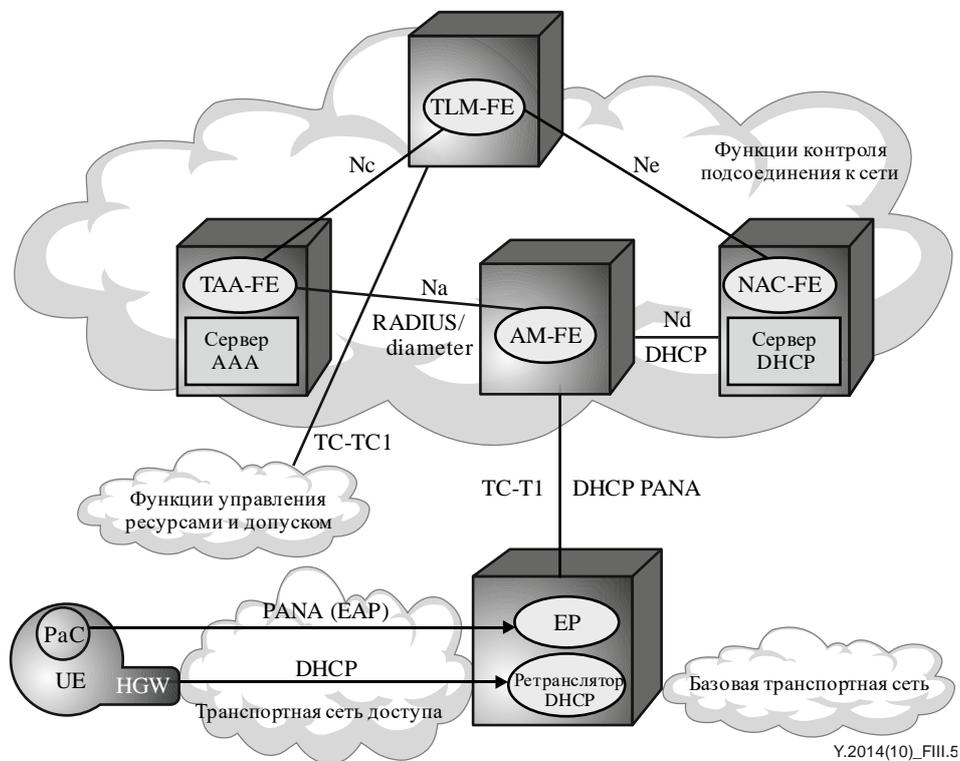
### III.3 DHCP (вариант 1)



ПРИМЕЧАНИЕ.– Для простоты интерфейсы к RACF не показаны.

**Рисунок III.3 – Конфигурация на основе DHCP (вариант 1)**





**Рисунок III.5 – Конфигурация на основе PANA**

## Дополнение IV

### Общее соответствие между Рекомендацией МСЭ-Т Y.2014 и стандартом ETSI ES 282 004 v2.0.0

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации.)

Приведенная ниже таблица описывает высокоуровневое соответствие между компонентом NACF, определенным в настоящей Рекомендации, и подсистемой подключения к сети (NASS), определенной в [b-ETSI ES 282 004].

Таблица IV.1

Стандарт ETSI ES 282 004 v2.0.0	Рекомендация МСЭ-Т Y.2014
<b>Функциональные объекты</b>	
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
<b>Эталонные точки</b>	
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: не определена	TAA-FE/TUP-FE: Nb. Подробности подлежат дальнейшему изучению.
NACF-UAAF: не определена	NAC-FE/TAA-FE: Nk. Подробности подлежат дальнейшему изучению.
ARF-AMF: e1	AR-FE-AM-FE: TC-T1
UE-ARF: e1	CPE/AR-FE: T-U1 [ITU-T Y.2012]
AF (например, P-CSCF)-CLF: e2	Функции управления обслуживанием (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

## Библиография

- [b-3GPP TS 23.401] 3GPP TS 23.401 (действующая версия), *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 (действующая версия), *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).*



## СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

Серия А	Организация работы МСЭ-Т
Серия D	Принципы тарификации и учета и экономические и стратегические вопросы международной электросвязи/ИКТ
Серия E	Общая эксплуатация сети, телефонная служба, функционирование служб и человеческие факторы
Серия F	Нетелефонные службы электросвязи
Серия G	Системы и среда передачи, цифровые системы и сети
Серия H	Аудиовизуальные и мультимедийные системы
Серия I	Цифровая сеть с интеграцией служб
Серия J	Кабельные сети и передача сигналов телевизионных и звуковых программ и других мультимедийных сигналов
Серия K	Защита от помех
Серия L	Окружающая среда и ИКТ, изменение климата, электронные отходы, энергоэффективность; конструкция, прокладка и защита кабелей и других элементов линейно-кабельных сооружений
Серия M	Управление электросвязью, включая СУЭ и техническое обслуживание сетей
Серия N	Техническое обслуживание: международные каналы передачи звуковых и телевизионных программ
Серия O	Требования к измерительной аппаратуре
Серия P	Качество телефонной передачи, телефонные установки, сети местных линий
Серия Q	Коммутация и сигнализация, а также соответствующие измерения и испытания
Серия R	Телеграфная передача
Серия S	Оконечное оборудование для телеграфных служб
Серия T	Оконечное оборудование для телематических служб
Серия U	Телеграфная коммутация
Серия V	Передача данных по телефонной сети
Серия X	Сети передачи данных, взаимосвязь открытых систем и безопасность
<b>Серия Y</b>	<b>Глобальная информационная инфраструктура, аспекты межсетевого протокола, сети последующих поколений, интернет вещей и "умные" города</b>
Серия Z	Языки и общие аспекты программного обеспечения для систем электросвязи