Международный союз электросвязи

МСЭ-Т

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

Y.2059

(07/2012)

СЕРИЯ Y: ГЛОБАЛЬНАЯ ИНФОРМАЦИОННАЯ ИНФРАСТРУКТУРА, АСПЕКТЫ МЕЖСЕТЕВОГО ПРОТОКОЛА, СЕТИ ПОСЛЕДУЮЩИХ ПОКОЛЕНИЙ, ИНТЕРНЕТ ВЕЩЕЙ И "УМНЫЕ" ГОРОДА

Сети последующих поколений – Структура и функциональные модели архитектуры

Функциональные требования для доступа к сетям последующих поколений на базе IPv6

Рекомендация МСЭ-Т Y.2059

ITU-T

ITU Международный союз электросвязи

РЕКОМЕНДАЦИИ МСЭ-Т СЕРИИ Y

ГЛОБАЛЬНАЯ ИНФОРМАЦИОННАЯ ИНФРАСТРУКТУРА, АСПЕКТЫ МЕЖСЕТЕВОГО ПРОТОКОЛА, СЕТИ ПОСЛЕДУЮЩИХ ПОКОЛЕНИЙ, ИНТЕРНЕТ ВЕЩЕЙ И "УМНЫЕ" ГОРОДА

ГЛОБАЛЬНАЯ ИНФОРМАЦИОННАЯ ИНФРАСТРУКТУРА	
Общие сведения	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
АСПЕКТЫ ПРОТОКОЛА ИНТЕРНЕТ	
Общие сведения	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
Ведение расчетов	Y.1800–Y.1899
IPTV по СПП	Y.1900–Y.1999
СЕТИ ПОСЛЕДУЮЩИХ ПОКОЛЕНИЙ	
Структура и функциональные модели архитектуры	**Y.2000–Y.2099**
Качество обслуживания и технические характеристики	Y.2100–Y.2199
Аспекты обслуживания: возможности обслуживания и архитектура обслуживания	Y.2200–Y.2249
Аспекты обслуживания: функциональная совместимость услуг и сетей в СПП	Y.2250–Y.2299
Совершенствование СПП	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
БУДУЩИЕ СЕТИ	Y.3000–Y.3499
ОБЛАЧНЫЕ ВЫЧИСЛЕНИЯ	Y.3500–Y.3999

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

Рекомендация МСЭ-Т Y.2059

Функциональные требования для доступа к сетям последующих поколений на базе IPv6

Резюме

В Рекомендации МСЭ-Т Y.2059 приведено исследование воздействия, анализ сценариев и функциональные требования к сетям, которые соединены с СПП на базе IPv6. В Рекомендации рассматриваются обе части СПП – сеть доступа и базовая сеть.

Весь анализ в основном проводится раздельно по двум аспектам – соединения на базе IPv6 и соединения, совместимые с IPv4. В соединениях на базе IPv6 основное внимание уделяется присоединению к сети, работающей только на базе IPv6, которое включает в себя распределение префиксов и адресов, конфигурацию и т. д. В соединениях, совместимых с IPv4, основное внимание уделяется методам перехода с IPv4 на IPv6, при котором продолжается оказание пользователям услуг на базе IPv4.

Хронологическая справка

Издание	Рекомендация	Утверждение	Исследовательская комиссия	Уникальный идентификатор*
1.0	МСЭ-Т Y.2059	29.07.2012 г.	13-я	11.1002/1000/11698

Ключевые слова

IPv6, доступ к сети IPv6, 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. 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/.

СОДЕРЖАНИЕ

Рекомендация МСЭ-Т Y.2059

Функциональные требования для доступа к сетям последующих поколений на базе IPv6

1 Сфера применения

Цель настоящей Рекомендации заключается в выявлении воздействий на сети, соединенные с СПП на базе IPv6, и в описании соответствующих сценариев и моделей для определения функциональных требований.

Функции страты транспортирования СПП представляют собой серию функций транспортирования и управления транспортированием, поддерживающих функциональные особенности страты обслуживания. Для выполнения доступа к СПП на базе IPv6 некоторые механизмы поддержки функций транспортирования и управления транспортированием уже внедрены в сетях, использующих IPv6. Помимо поддержки IPv6 устройства в сети должны соответствовать определенным функциональным требованиям. В Рекомендации рассматриваются следующие аспекты:

– определение воздействия на сети, соединенные с СПП на базе IPv6;

– сценарии доступа к сети, характерные для СПП, в том числе конфигурации таких параметров, как префикс, адрес и параметры сервера;

– сценарии регистрации уровня сети доступа в СПП на базе IPv6;

– функциональные требования к сетям, которые соединены с СПП на базе IPv6.

2 Справочные документы

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

[ITU-T Y.2001] Рекомендация МСЭ-Т Y.2001 (2004 г.), *Общий обзор СПП.*

[ITU-T Y.2051] Рекомендация МСЭ-Т Y.2051 (2008 г.), *Общий обзор сети последующих поколений на базе IPv6.*

[ITU-T Y.2053] Recommendation ITU-T Y.2053 (2008), *Functional requirements for IPv6 migration in NGN.*

[ITU-T Y.2701] Рекомендация МСЭ-Т Y.2701 (2007 г.), *Требования к безопасности для сетей последующих поколений версии 1.*

3 Определения

3.1 Термины, определенные в других документах

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

3.1.1 СПП на базе IPv6 (IPv6-based NGN) [ITU-T Y.2051]: Данный термин обозначает СПП, которые поддерживают адресацию, протоколы маршрутизации и услуги, связанные с IPv6. В СПП на базе IPv6 должны быть реализованы распознавание и обработка заголовков и опций IPv6 в условиях работы с различными базовыми транспортными технологиями в страте транспортирования.

3.1.2 NAT64 [b-IETF RFC 6146]: Механизм, определяющий переход от IPv4 к IPv6 и сосуществование IPv4 и IPv6. Совместно работающие механизмы NAT64 и DNS64 позволяют клиенту, работающему только с IPv6, инициировать обмен данными с сервером, работающим только с IPv4.

3.1.3 сеть последующих поколений (next generation network) [ITU-T Y.2001]: Сеть с пакетной коммутацией, пригодная для предоставления услуг электросвязи и для использования нескольких широкополосных технологий транспортировки с включенной функцией QoS, в которой связанные с обслуживанием функции не зависят от примененных технологий, обеспечивающих транспортировку. Она обеспечивает свободный доступ пользователей к сетям и конкурирующим поставщикам и/или выбираемым ими услугам. Она поддерживает универсальную подвижность, которая обеспечивает постоянное и повсеместное предоставление услуг пользователям.

3.2 Термины, определенные в настоящей Рекомендации

В настоящей Рекомендации определяются следующие термины.

3.2.1 DNS64 (на основе [b-IETF RFC 6147]): Механизм синтезирования записей DNS IPv6 на основе записей DNS IPv4 [b-IETF RFC 1035]. Механизм DNS64 вместе с механизмом трансляции адресов IPv6 в IPv4 используется для обеспечения соединения между клиентом, работающим только с IPv6, и сервером, работающим только с IPv4, не требуя внесения каких-либо изменений в узел IPv6 или в узел IPv4 для класса приложений, работающих через NAT.

3.2.2 туннельный концентратор (tunnel concentrator): Функция/устройство, которая(ое) прекращает деятельность нескольких туннелей со стороны пользователя, концентрирует трафик, передаваемый по туннелям, и перенаправляет трафик в новый туннель в направлении сети таким образом, что количество туннелей, которые будут обрабатываться сетью, сокращается.

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы.

AAAA	Authentication, Authorization, Accounting and Auditing	Аутентификация, авторизация, учет и проверка
CGA	Cryptographically Generated Address	Криптографически генерируемый адрес
CPE	Customer Premises Equipment	Оборудование в помещении клиента
DHCPv6	Dynamic Host Configuration Protocol version 6	Протокол динамической конфигурации хоста, версия 6
DNS	Domain Name Service	Служба доменных имен
DUID	DHCP Unique Identifier	Уникальный идентификатор DHCP
FE	Functional Entity	Функциональный объект
ID	Identifier	Идентификатор
IPv4	Internet Protocol version 4	Интернет-протокол версии 4
IPv6	Internet Protocol version 6	Интернет-протокол версии 6
ISP	Internet Service Provider	Поставщик услуг интернета
LAN	Local Area Network	Локальная сеть
MAC	Media Access Control	Управление доступом к среде
NACF	Network Attachment Control Function	Функция управления присоединением к сети
NAT	Network Address Translation	Трансляция сетевых адресов
ND	Network Discovery	Обнаружение сети
NGN	Next Generation Network	Сеть последующих поколений
OAM	Operation and Maintenance	Эксплуатация и техническое обслуживание
PD	Prefix Delegation	Делегирование префикса
PPP	Point-to-Point Protocol	Протокол связи пункта с пунктом
RA	Router Advertisement	Объявление маршрутизатора
RACF	Resource and Admission Control Function	Функция управления ресурсами и допуском

RS	Router Solicitation	Запрос маршрутизатора
UE	User Equipment	Оборудование пользователя
VLAN	Virtual Local Area Network	Виртуальная локальная сеть
WAN	Wide Area Network	Территориальная распределенная сеть

5 Условные обозначения

Отсутствуют.

6 Влияние на сетевые функции для доступа к СПП на базе IPv6

IPv6 отличается от IPv4 во многих аспектах. Для доступа к СПП на базе IPv6 необходимо в первую очередь установить соединение по протоколу IPv6, что сводится главным образом к предоставлению и распределению префикса и адреса. Адрес IPv6 состоит из префикса и идентификатора интерфейса. Существующие механизмы используют различные методы конфигурации префиксов и адресов. Помимо соединения по IPv6 сеть также должна поддерживать уже существующих пользователей IPv4, предоставляя им доступ к СПП на базе IPv6. Кроме того, требования к безопасности для IPv6 отличаются от аналогичных требований для IPv4. В настоящем разделе описываются данные механизмы и их влияние на доступ к сети.

6.1 Установление соединений по IPv6

6.1.1 Префикс и адресное пространство

Длина адреса в протоколе IPv6 составляет 128 битов. Наиболее распространенная архитектура адресации – 64 бита с информацией о номере сети (префикс) и 64 бита с информацией о номере хоста (идентификатор интерфейса). Протокол IPv6 обладает более сложной архитектурой адресации, чем протокол IPv4. С учетом значительного объема адресного пространства IPv6 и сложной структуры префикса следует принимать во внимание следующие аспекты, влияющие на доступ к СПП на базе IPv6.

- Доступность и достижимость адреса. Пользователь может иметь один или несколько глобальных уникальных адресов IPv6. Тем самым решается проблема нехватки адресного пространства, характерная для IPv4. Каждый пользователь, желающий получить глобальный уникальный адрес IPv6, должен иметь возможность сделать это оперативно и без технических затруднений. Благодаря полученному адресу IPv6 пользователи становятся доступными на глобальном уровне. Принятие адресов IPv6 влияет на методы трансляции сетевых адресов, потребность в которых при использовании сетей на базе IPv6 может снизиться или даже исчезнуть.

  В IPv6-адресах область действия адреса встроена в элемент адресной структуры. Для индивидуальных адресов определены три области действия, в том числе внутриканальная, уникальная внутриканальная и глобальная. Область действия учитывается при выборе адреса по умолчанию для источника и пункта назначения. Область действия адреса влияет на получение адреса оконечным пользовательским устройством, последовательность начальной загрузки интерфейсов оборудования CPE и т. д.

- Структура префикса. В IPv4 используется адресная маска для разделения адреса на сетевую часть и часть хоста. В IPv6 адресная маска не используется. Вместо нее используется префикс адреса, который отделяет префикс подсети от остальной части адреса. В IPv6 применяется особый способ объявления и делегирования префикса адреса, что позволяет организовать префикс удобным для управления поставщиками услуг или клиентами образом. Оборудование пользователя должно быть способно без затруднений получать префикс адреса.

6.1.2 Механизм распределения префиксов и адресов

IPv6 поддерживает конфигурации адреса с сохранением и без сохранения состояния. Соответствующие механизмы уже стандартизованы в IETF, включая DHCPv6 [b-IETF RCF 3315], протокол обнаружения соседних объектов для IPv6 [b-IETF RFC 4861], автоконфигурацию адреса IPv6 без сохранения состояния [b-IETF RFC 4862], опции префикса IPv6 для DHCPv6 [b-IETF RFC 3633] и

ряд других документов RFC и Рекомендаций. Механизмы распределения префикса и адреса в IPv6 отличаются от аналогичных механизмов в IPv4. Они влияют на следующие аспекты:

- со стороны оборудования CPE – оборудование CPE служит точкой соединения между домашней сетью и сетью доступа/агрегирования. Оно может использовать различные механизмы распределения префикса и адреса, привязанные к интерфейсам LAN и WAN. Доступ пользователя к сети в значительной степени зависит от функций и возможностей, предоставляемых оборудованием CPE;
- со стороны сети – операторы могут применять собственный способ объявления префиксов и конфигурации адресов. В некоторых случаях конфигурации адреса с сохранением и без сохранения состояния могут применяться одновременно. В целях обеспечения и контроля транспортировки данных по IPv6 определенные сетевые узлы должны быть уведомлены о сигнализации, поддерживающей IPv6.

6.1.3 Многоадресные интерфейсы

Одной из важных особенностей IPv6 является его способность присваивать несколько адресов одному интерфейсу. Это находит применение во многих сценариях, например в мобильном протоколе IPv6 и множественной адресации. Кроме того, адреса IPv6 имеют различные области действия, такие как внутриканальная и глобальная. Данные характеристики включены в стандартные протоколы IPv6. Таким образом, для СПП на базе IPv6 характерны узлы, имеющие несколько адресов.

Наличие нескольких адресов с различными областями действия предъявляет новые требования к сети доступа, относящиеся к конфигурации узла.

6.2 Установление соединений, совместимых с IPv4

В отрасли электросвязи существует единое мнение, что переход от IPv4 к IPv6 займет значительное время. В то время как протокол IPv6 внедряется во все больших масштабах, IPv4 должен поддерживаться в течение определенного периода. Исходя из этого следующие аспекты важны для понимания влияния на сеть доступа.

- Двойной стек – для одновременной поддержки протоколов IPv4 и IPv6 может потребоваться модернизация некоторых устройств (таких как хосты, оборудование CPE и граничные маршрутизаторы), зависящая от методики перехода, выбранной поставщиком услуг интернета.
- Туннели – может потребоваться настройка туннелей, например туннеля от IPv6 к IPv4.
- Трансляция адресов/протоколов – взаимодействие протоколов IPv4 и IPv6 должно включать механизмы трансляции адресов/протоколов, такие как NAT64 [b-IETF RFC 6146] и DNS64 [bIETF RFC 6147].

6.3 Безопасность

6.3.1 Регистрация на уровне сети доступа

Регистрация на уровне сети доступа включает в себя процедуры идентификации, аутентификации и авторизации между оборудованием CPE и функцией управления присоединением к сети (NACF) в СПП в целях управления доступом. В основном регистрация предусматривает аутентификацию в явной или неявной форме.

- Аутентификация в неявной форме – узел подключается к сети через физический проводной канал связи и получает информацию только через этот канал (например, телефонное соединение или IP-адреса), поэтому установление канала связи может само по себе рассматриваться как неявная аутентификация.

  IPv6 поддерживает конфигурации адреса с сохранением и без сохранения состояния. Это может влиять на способы получения информации о канале связи и способы обработки информации узлами.
- Аутентификация в явной форме – для аутентификации используются идентификаторы и/или идентификационные данные, заданные в явном виде. В IPv6 для представления идентификаторов и/или регистрационных данных могут использоваться разные методы. Это может влиять на поток аутентификации в явной форме во многих сценариях доступа, например PPP, доступ по IP и т. д.

6.3.2 Валидация и фильтрация адреса источника

Для транспортировки данных пользователя сеть доступа, как правило, должна выполнять валидацию и фильтрацию адреса источника. В сети доступа IPv4 валидация и фильтрация адреса источника в большинстве случаев основывается на информации о взаимной привязке адресов IP, MAC, VLAN и порта. В IPv6 для распределения префикса и адреса применяются разные механизмы, а также имеются разные области действия адресов. Это усложняет валидацию адреса источника и влияет на доступ пользователей.

7 Сценарии и конфигурации параметров для доступа к СПП на базе IPv6

В СПП на базе IPv6 возможны различные сценарии и конфигурации параметров, такие как предоставление префикса и адреса IPv6 без сохранения и с сохранением состояния, делегирование префикса совместно с конфигурацией адреса с сохранением и без сохранения состояния. В данном разделе описаны различные сценарии.

На рисунке 1 показана функциональная архитектура СПП на базе IPv6, определенная в [ITU-T Y.2051].

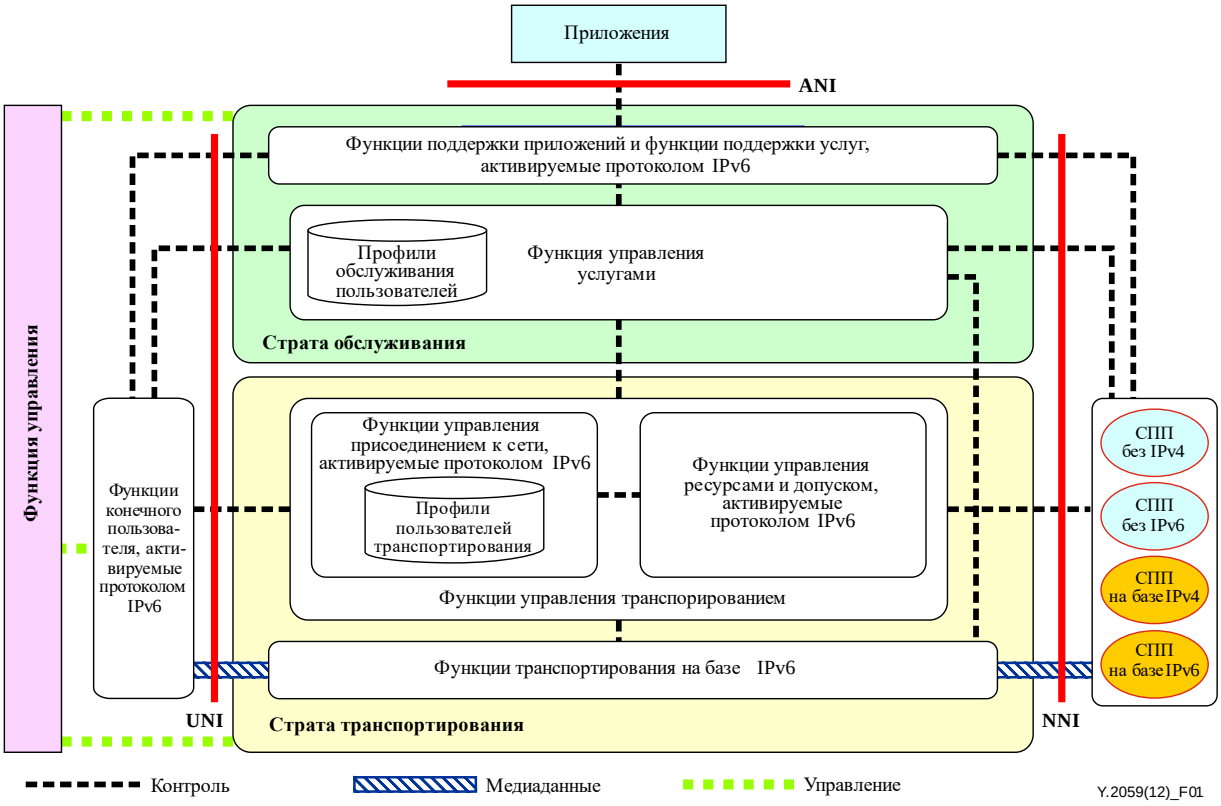

Рисунок 1 – Функциональная архитектура СПП на базе IPv6

Функции транспортирования на базе IPv6 могут быть разделены на следующие совместимые с IPv6 функции: функции сети доступа, граничные функции, функции транспортирования базовой сети, функции шлюза и функции обработки медиаданных. Функции сети доступа и граничные функции особенно важны для пользователей, подключенных к сетям. В то же время в зависимости от сценариев могут быть задействованы и другие функции. С учетом того что функции управления транспортированием взаимодействуют с функциями транспортирования, функции управления присоединением к сети, активируемые протоколом IPv6, должны работать совместно с соответствующими функциями транспортирования. Функции конечного пользователя, активируемые протоколом IPv6, включают в себя серию функций оборудования CPE и оконечных устройств, которые тесно взаимодействуют с функциями транспортирования и управления транспортированием. Страта обслуживания относится к более высокому уровню и напрямую не связана с доступом к сети. На рисунке 2 представлена архитектура доступа к сети, а на рисунке 3 архитектура представлена в логической форме.

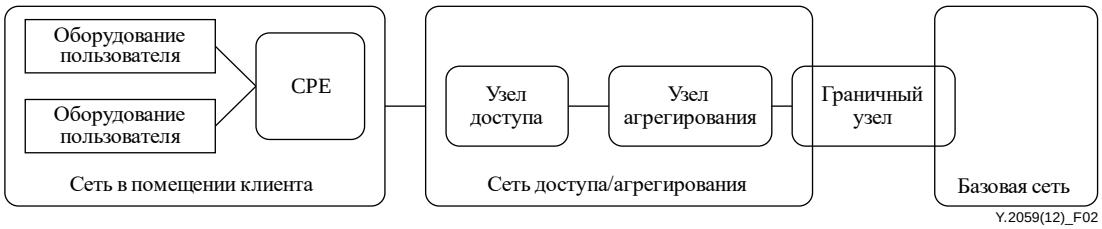

Рисунок 2 – Архитектура доступа к сети

Рисунок 3 – Логическая архитектура доступа к сети

7.1 Установление соединений IPv6

7.1.1 Конфигурация префикса и адреса

Для большинства сетей доступа конфигурация префикса должна быть определена в структурированной форме. Конфигурация может быть статической или динамической. Существует два основных динамических способа объявления префикса – объявление маршрутизатора и делегирование префикса посредством DHCPv6. Как показано на рисунке 4, назначение конфигурации префикса и адреса для доступа к сети заключается в идентифицировании каждого из устройств CPE уникальным образом и присвоении каждому из устройств CPE надлежащего значения префикса. Такой порядок помогает поддерживать профили пользователей IPv6 в структурированной форме и упрощает эксплуатацию, администрирование и техническое обслуживание.

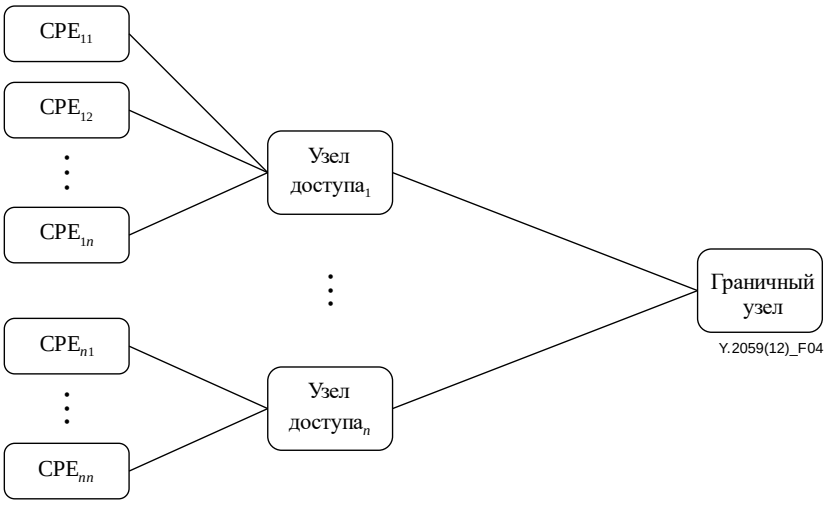

Рисунок 4 – Структура сетевых элементов для доступа к сети

7.1.1.1 Статическое выделение ресурсов

При статическом выделении ресурсов узлы доступа статически сконфигурированы с использованием определенной информации (например, конфигурации делегирования). Это необходимо для последующей конфигурации префикса и адреса. Как правило, для удобства технического обслуживания необходимо, чтобы узлы доступа объявляли конкретный префикс подсети для каждого интерфейса нисходящего канала. Исходя из этого информация о конфигурации должна предоставляться на основе отношений отображения между префиксом, полученным от интерфейса восходящего канала, и префиксом, который должен быть объявлен в каждом интерфейсе нисходящего канала. Узел доступа принимает объявления маршрутизатора с информацией о префиксе от граничного узла, затем на основе представленной информации определяет префикс для объявления в интерфейсе нисходящего канала и в итоге направляет объявления маршрутизатора с объявленным префиксом интерфейсу нисходящего канала.

Существуют различные способы предоставления услуг доступа к сети, в том числе методы эксплуатации, администрирования и технического обслуживания, а также протокол конфигурации узла доступа. В зависимости от метода, используемого для представления информации о конфигурации, могут выполняться разнообразные задачи, такие как предоставление префикса подсети на основе обслуживания или постоянное предоставление оборудованию CPE относительного статического префикса. Статическое выделение ресурсов может соответствовать различным требованиям к обеспечению соединения в разнообразных сценариях. На рисунке 5 представлен один из сценариев статического выделения ресурсов.

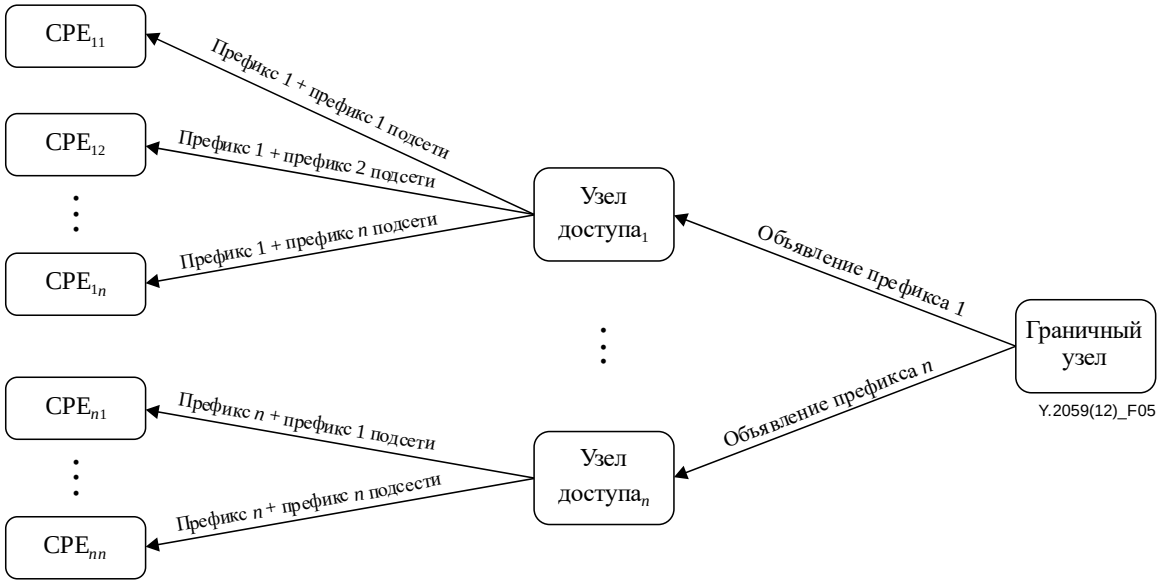

Рисунок 5 – Пример статического выделения ресурсов

7.1.1.2 Динамическое объявление

В некоторых случаях граничный узел может самостоятельно управлять конфигурацией и объявлением префикса и адреса для отдельных устройств CPE вне зависимости от структуры или иерархии сети доступа. В подобных сценариях граничный узел должен объявлять соответствующие префиксы для каждого из устройств CPE. С этой целью, перенаправляя запрос префикса от оборудования CPE граничному узлу, узел доступа должен сообщить граничному узлу идентификационную информацию. Идентификационная информация может включать номер порта узла доступа, расположенного ниже, ID узла доступа и/или другие параметры. Получив запрос префикса с идентификационной информацией оборудования CPE, граничный узел выполняет процедуры аутентификации, авторизации и учета для префикса оборудования CPE, который должен быть объявлен оборудованию CPE.

На рисунке 6 приведен пример сценария динамического объявления. Граничный узел динамически предоставляет информацию о префиксе, основываясь на указаниях узлов доступа.

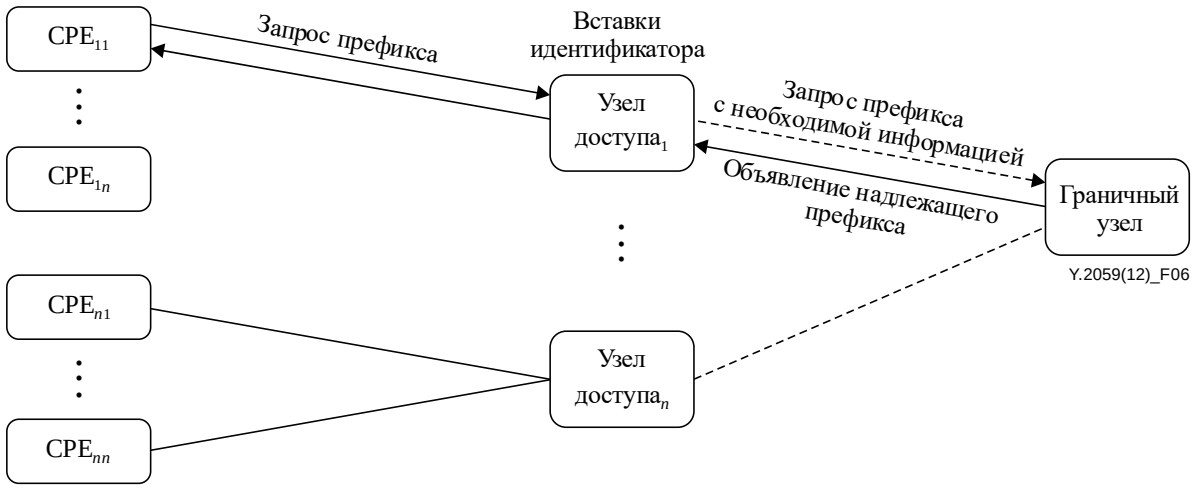

Рисунок 6 – Пример динамического объявления

7.1.1.3 Каскадное делегирование

Ввиду высокой доступности глобального адреса IPv6 очевидно, что будет поддерживаться домашняя сеть, обладающая более сложной структурой. Каскадное делегирование префикса – один из возможных примеров домашней сети, представленный на рисунке 7. Граничный узел или сервер протокола динамической конфигурации хоста версии 6 (DHCPv6), встроенный в граничный узел, отправляют делегированный префикс оборудованию CPE. Благодаря возможности каскадного соединения маршрутизаторов в домашней сети, созданной оборудованием CPE, могут сосуществовать несколько подсетей. Таким образом оборудование CPE должно отправлять каскадный префикс в нисходящем направлении.

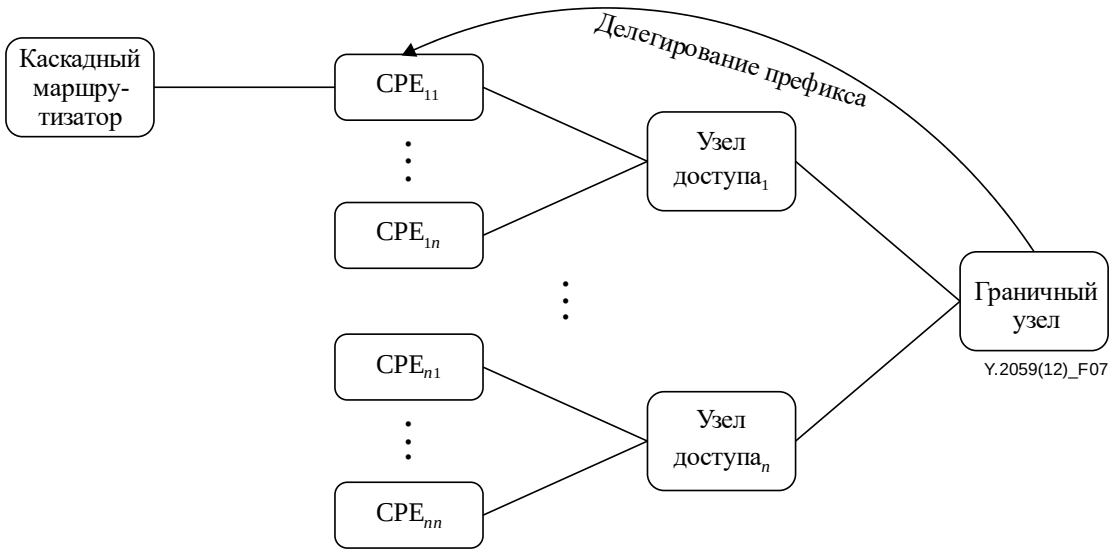

Рисунок 7 – Пример каскадного делегирования префикса

При надлежащем управлении делегированием префикса оборудование CPE получает делегированный префикс и указания по правилу или политике каскадного делегирования в домашней сети. Для каскадного делегирования применяются различные механизмы, в том числе протокол DHCPv6, протокол управления оконечными устройствами и PPP. Указания по правилу или политике направлены на расширение каскадного префикса. Оборудование CPE расширяет префикс, основываясь на значениях расширения каскадного префикса, и делегирует этот префикс каскадному маршрутизатору.

В сценарии каскадного делегирования префиксы могут делегироваться на несколько уровней вниз под управлением операторов.

7.1.1.4 Изменение нумерации префиксов

В некоторых случаях требуется изменение нумерации префиксов по различным причинам, таким как внесение оператором изменения в распределение адресов, изменения внутренней топологии сети или метода авторизации, осуществленные сервером политики. При изменении нумерации оборудование CPE должно обновить как делегированный префикс, так и префикс интерфейса WAN.

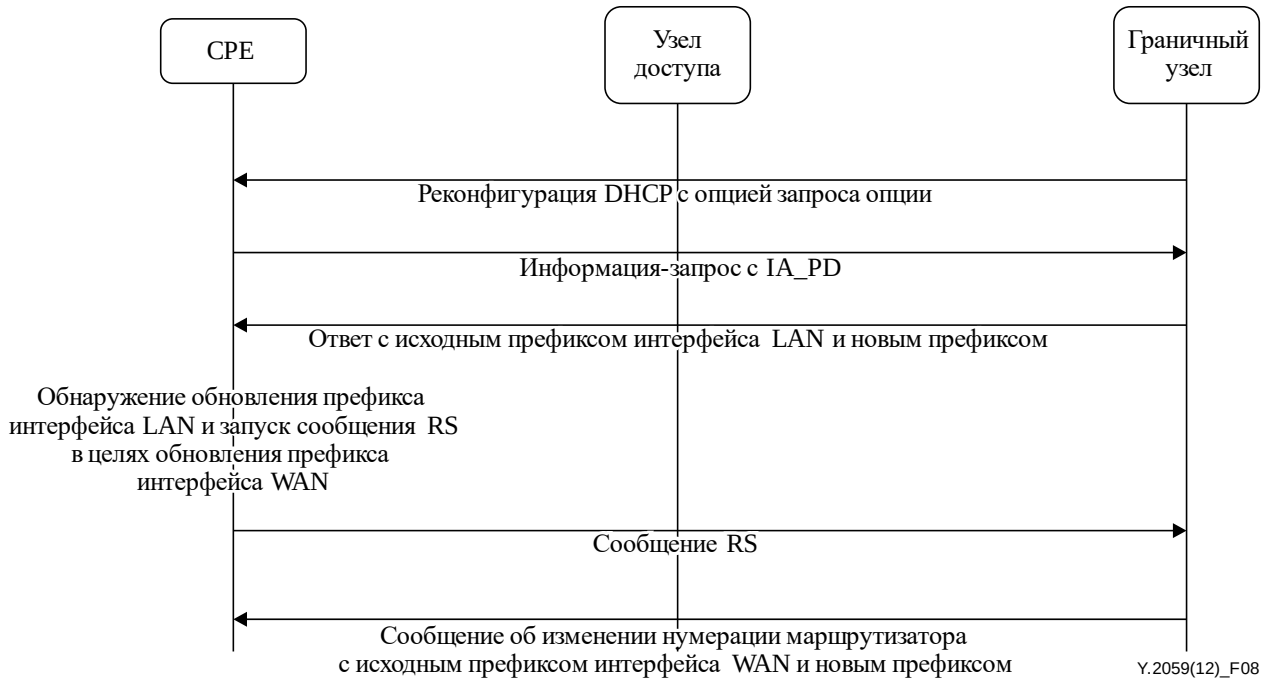

Рисунок 8 – Изменение нумерации префиксов, инициированное DHCPv6

Как показано на рисунке 8, граничный узел инициирует изменение нумерации префиксов, отправляя сообщение о реконфигурации DHCPv6 в целях объявления оборудованию CPE об изменении делегированного префикса. После обеспечения надлежащего делегирования префикса оборудование CPE обновляет делегированный префикс и направляет сообщение RS в целях обновления префикса интерфейса WAN.

Рисунок 9 – Изменение нумерации префиксов, инициированное изменением нумерации маршрутизатора

Как показано на рисунке 9, в некоторых случаях граничный узел способен инициировать изменение нумерации префиксов, отправляя сообщение об изменении нумерации маршрутизатора [b-IETF RFC 2894] интерфейсу WAN оборудования CPE. Затем оборудование CPE обнаруживает обновление префикса в интерфейсе WAN и инициирует реконфигурацию делегирования префикса по протоколу DHCPv6.

На рисунке 8 представлены случаи изменения нумерации, инициируемые протоколом DHCPv6 и ND. Следует отметить, что в ряде случаев DHCPv6 и ND могут применяться одновременно, чтобы инициировать изменение нумерации на одном интерфейсе. Потенциально это может вызывать конфликт политик конфигурации адресов. Например, префиксы в сообщениях DHCPv6 и ND отличаются из-за ошибки сетевого администратора; или хосты, управляемые DHCPv6, получают сообщения с конфигурацией адреса, объявленного маршрутизатором, что может вызвать переход хоста в непредсказуемый режим работы, поскольку ни DHCPv6, ни ND не задали режим работы хоста в такой ситуации. Если в процессе изменения нумерации хосты получают сообщения с конфигурацией адреса (либо через ND, либо через DHCPv6), а также при конфликте с политикой конфигурации адреса, хост должен сообщить сети о возникшем конфликте. В итоге хосты принимают от сети указания с конфигурацией адреса.

7.1.1.5 Динамическое распределение адресов

Протокол DHCPv6 позволяет системе управления сетью динамически распределять адреса IPv6 между оборудованием пользователей и настраивать соответствующие сетевые параметры, как показано на рисунке 10. Оборудование пользователя направляет адреса и запросы конфигурации на сервер DHCPv6, который может быть встроен в узел доступа, граничный узел или запускаться независимо через ретранслятор оборудования CPE. После получения запроса сервер DHCPv6 распределяет адрес IPv6 оборудованию пользователя и передает другие параметры конфигурации оборудованию пользователя в ответных сообщениях DHCPv6.

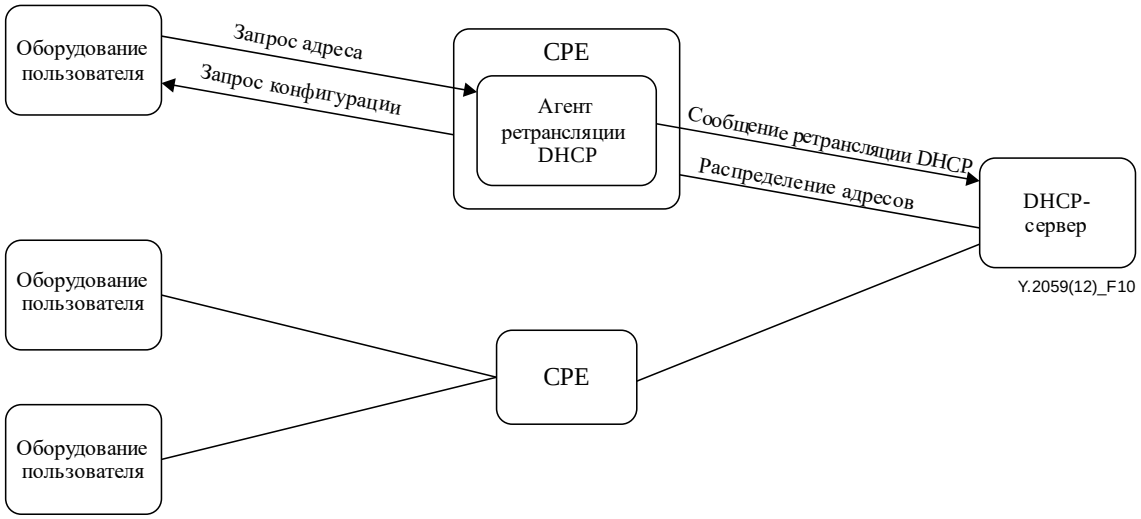

Рисунок 10 – Пример распределения адресов по протоколу DHCPv6

Сервер DHCPv6 также должен управлять адресами IPv6 даже в тех случаях, когда они генерируются оборудованием пользователя. Примером является криптографически генерируемый адрес (CGA) [b-IETF RFC 3971]. Клиент генерирует CGA, отправляет CGA на сервер DHCPv6 и просит сервер DHCPv6 определить, удовлетворяет ли созданный адрес CGA требованиям конфигурации сети (включающей уровень безопасности CGA, установленный сервером DHCPv6). Если CGA не удовлетворяет требованиям конфигурации сети, сервер DHCPv6 направляет узлу надлежащую конфигурацию сети. После этого узел генерирует новый адрес CGA в соответствии с конфигурацией (включающей открытый ключ клиента и уровень безопасности CGA, установленный клиентом), отправленной с сервера DHCPv6, и повторно направляет CGA на сервер DHCPv6 с повторным запросом.

DHCPv6 также может помочь оборудованию пользователя генерировать CGA с правильными параметрами конфигурации сети. Пользовательское устройство отправляет серверу DHCPv6 запрос на генерацию адреса CGA, который удовлетворит требованиям конфигурации сети. Сервер DHCPv6 получает отправленную клиентом информацию о конфигурации клиента (включающую открытый ключ клиента и уровень безопасности CGA, установленный клиентом) и генерирует адрес CGA в соответствии с конфигурацией, обладающей более высоким приоритетом по сравнению с конфигурацией клиента и конфигурацией сети (включающей уровень безопасности CGA, установленный сервером DHCPv6). Затем сервер DHCPv6 направляет адрес CGA клиенту.

7.1.2 Многоадресные интерфейсы

Из числа различных сценариев конфигурации адресов, упомянутых в разделе 6.1.3, множественная адресация [b-ITUT Y.2052] является наиболее конкретным и определенным требованием в СПП на базе IPv6.

На рисунке 11 изображен типовой сценарий множественной адресации для доступа в СПП по IPv6.

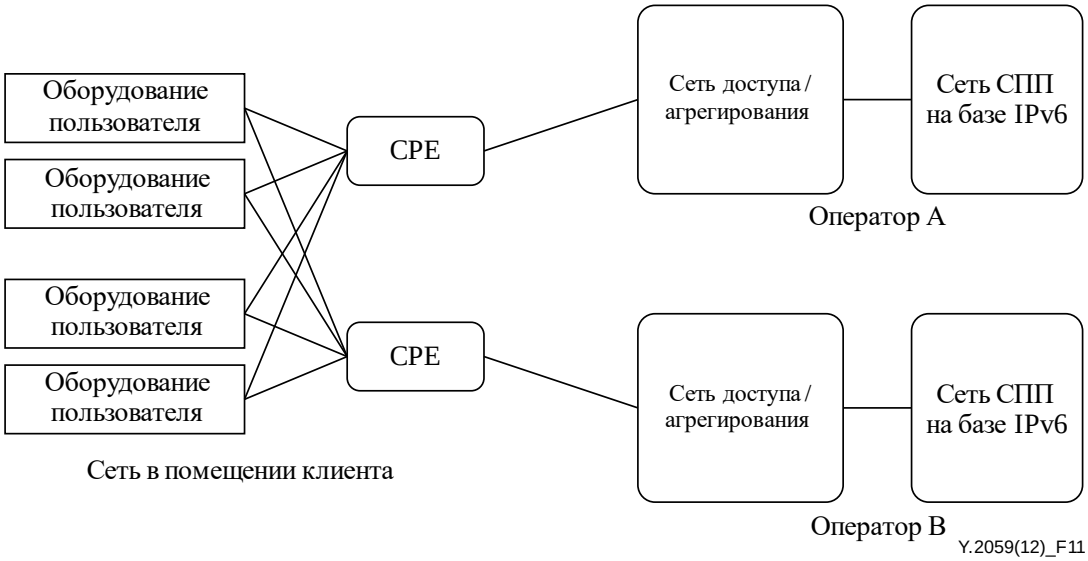

Рисунок 11 – Типовой сценарий множественной адресации для доступа в СПП по IPv6

На рисунке выше представлен сценарий, в котором сети доступа/агрегирования могут разворачивать механизмы перехода к IPv6, включающие разные методы обработки IP-пакетов (например, туннелирование и трансляцию, описанные в разделах 7.2.1 и 7.2.2). Таким образом для определенного типа IP-пакетов (IPv4 или IPv6) эффективность передачи в разных сетях доступа/агрегирования может варьироваться, что представляет собой один из примеров проблемы выбора сети, описанной в [b-IETF RFC 5113]. Для решения проблемы выбора сети требуется метод выбора подходящего маршрута для оборудования пользователя в зоне с множественной адресацией. Оборудование пользователя направляет оборудованию CPE сообщения-запросы с информацией о переходе. Оборудование пользователя коррелирует полученную от оборудования CPE информацию о переходе с адресом IP оборудования CPE. Информация о корреляции записывается в таблицу пользовательского оборудования, которое затем выбирает подходящий маршрут в соответствии с информацией о корреляции. Информация о переходе может быть предварительно сконфигурирована в оборудовании CPE или сгенерирована им в соответствии с принятыми сообщениями сети.

7.2 Установление соединений, совместимых с IPv4

7.2.1 Доступ к узлам IPv4 посредством комбинации механизмов двойного стека и туннелирования

В данном сценарии пользователи выступают в роли узлов IPv4 для доступа к узлам IPv4. В этом случае требуется настройка туннелей IPv4 через IPv6 в СПП на базе IPv6.

Явно выраженное влияние на сеть доступа заключается в том, что пользовательские устройства и оборудование CPE должны поддерживать двойной стек – протоколы IPv4 и IPv6. Оборудование CPE инкапсулирует пакеты IPv4 в пакеты IPv6 и перенаправляет их в туннельный концентратор по сети СПП на базе IPv6. Туннельный концентратор обеспечивает передачу пакетов IPv4 между сетью IPv4 и оборудованием CPE.

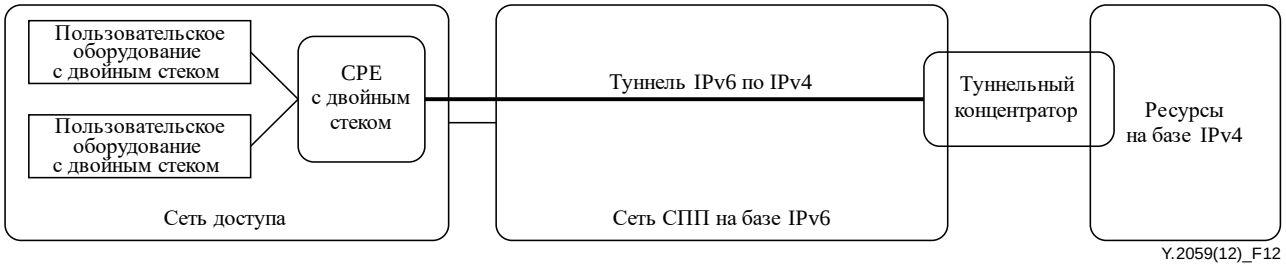

Рисунок 12 – Доступ к узлам IPv4 посредством комбинации механизмов двойного стека и туннелирования

7.2.2 Доступ к узлам IPv4 с помощью транслятора IPv6–IPv4

В данном сценарии пользователи выступают в качестве узлов IPv6 для доступа к узлам IPv4. В этом случае требуется транслятор IPv6–IPv4.

Некоторым механизмам трансляции требуется специальное адресное пространство, которое может влиять на распределение адресов и управление сетью доступа.

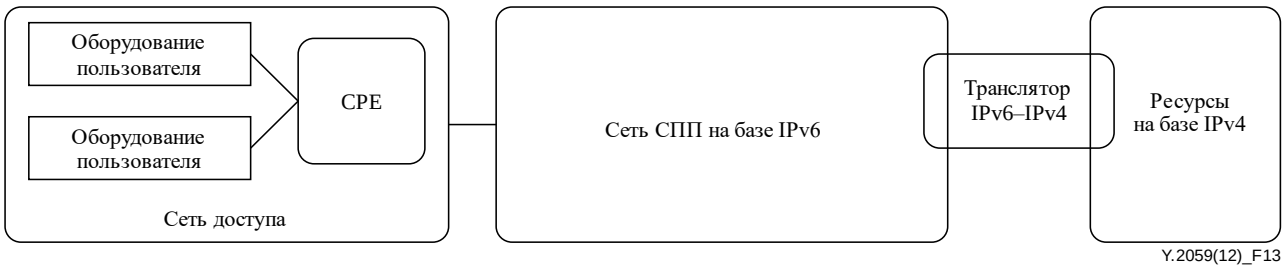

Рисунок 13 – Доступ к узлам IPv4 с помощью транслятора IPv6–IPv4

7.3 Безопасность

7.3.1 Регистрация на уровне сети доступа

7.3.1.1 Регистрация адреса, сконфигурированного без сохранения состояния

В разделе 6.3.1 описывается аутентификация на линии в неявной форме. После того как узел получает от сети адрес IPv6, считается, что он прошел аутентификацию на линии.

IPv6 поддерживает режимы конфигурации адреса с сохранением и без сохранения состояния. В режиме конфигурации без сохранения состояния узел может самостоятельно конфигурировать свой адрес, не уведомляя об этом сеть. Автоконфигурация адреса IPv6 без сохранения состояния является значительным шагом вперед по сравнению с IPv4, однако она на концептуальном уровне конфликтует с адресной архитектурой, управляемой сетью. К примеру, в случае сети с управлением по DHCPv6 или сети со списком управления доступом сеть самостоятельно назначает адреса и управляет ими. В частности, в части аутентификации на линии автоконфигурация означает отсутствие регистрации.

Объявление протокола DHCPv6 и маршрутизатора может быть расширено в целях отправки администратором сети оборудованию пользователя запроса на регистрацию адреса. Сервер DHCPv6 может выступать в качестве сервера регистрации адресов с заново определенными параметрами DHCPv6. На рисунке 14 представлена общая процедура регистрации адреса.

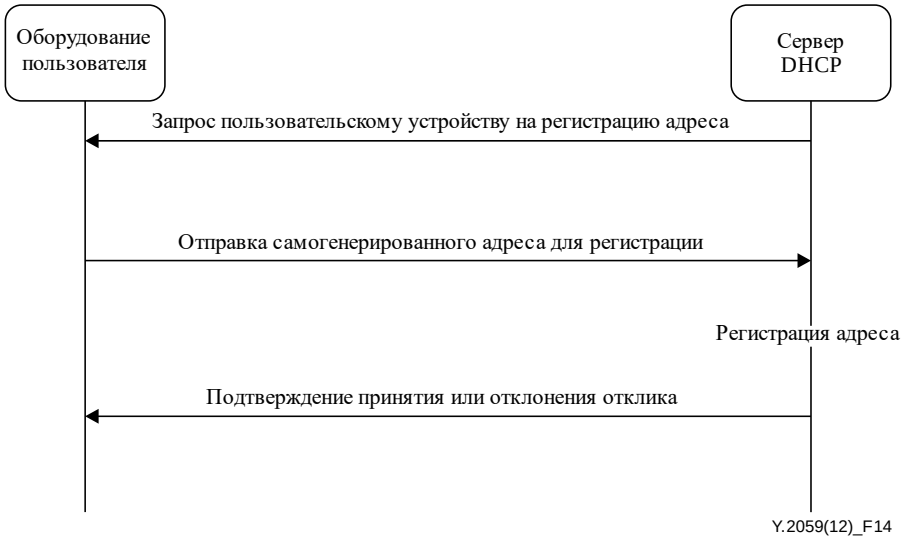

Рисунок 14 – Процедура регистрации адреса

7.3.1.2 Сценарий аутентификации PPP

Протокол PPP широко применяется для доступа к сети и представляет собой набор протоколов уровня канала с функциями аутентификации. Интерфейс PPP для IPv6 определен в [b-IETF RFC 5072] и [b-IETF RFC 5172]. Протокол PPP удобно использовать для аутентификации доступа по IPv6. В соответствии с рабочим режимом оборудования CPE существует два сценария аутентификации PPP.

- Оборудование CPE, работающее в режиме маршрутизации. Оборудование CPE сначала отправляет запрос доступа, который должен быть аутентифицирован оператором. После аутентификации оператор, как правило, через делегирование префикса по DHCPv6 присваивает оборудованию CPE префикс IPv6. Оборудование CPE присваивает пользовательским устройствам адреса по протоколам DHCPv6 или ND. Пользовательские устройства не управляются оператором напрямую.

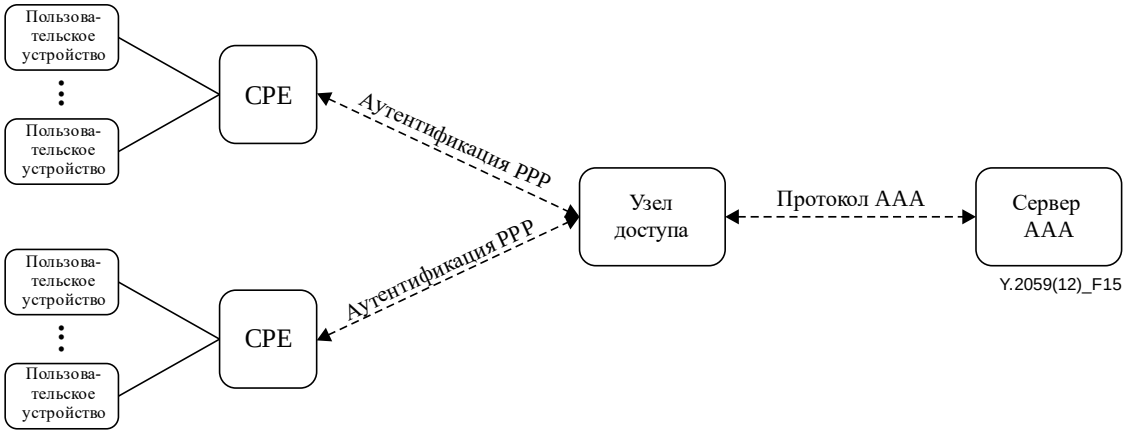

Рисунок 15 – Аутентификация PPP при работе оборудования CPE в режиме маршрутизации

- Оборудование CPE, работающее в режиме моста. При работе оборудования CPE в режиме моста пользовательские устройства взаимодействуют непосредственно с узлом доступа для проведения аутентификации PPP и задания конфигурации адреса. Если пользовательские устройства поддерживают только конфигурацию адреса без сохранения состояния, то узел доступа обычно выступает в качестве прокси-сервера DHCPv6-PD и запрашивает префикс IPv6 с сервера DHCPv6, передавая его пользовательским устройствам по протоколу ND. Если пользовательские устройства поддерживают DHCPv6, то узел доступа обычно выступает в качестве агента ретрансляции DHCPv6, обеспечивая ретрансляцию сообщений между пользовательскими устройствами и сервером DHCPv6.

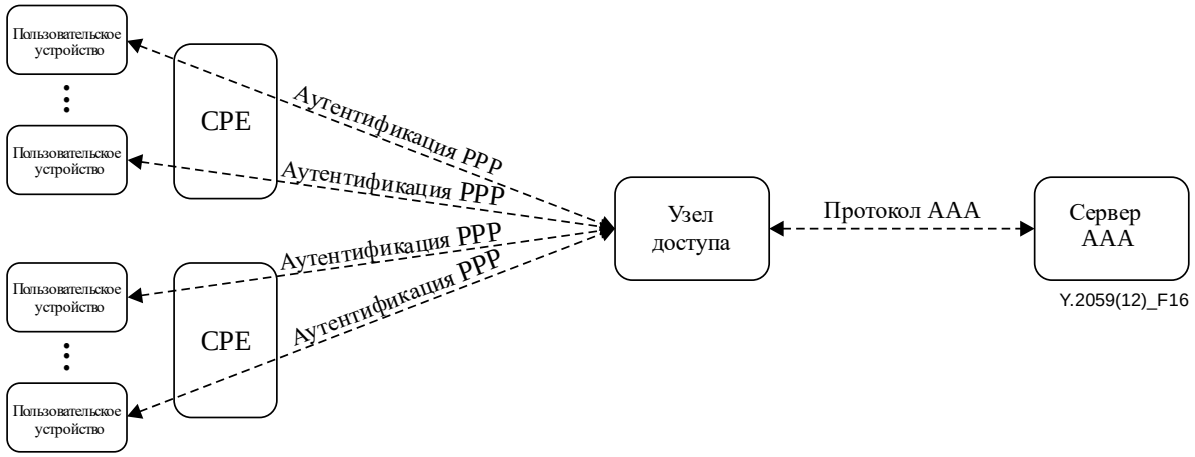

Рисунок 16 – Аутентификация PPP при работе оборудования CPE в режиме моста

7.3.2 Валидация и фильтрация адреса источника

Функция валидации адреса источника имеет большое значение для доступа к сети. Данная функция важна для управления доступом и авторизации, фильтрации трафика с интерфейсов пользователей, реализованных в виде портов моста или маршрутизатора с поддержкой 3-го уровня, общего повышения точности фильтрации в корпоративных сетях и т. д.

Функция валидации адреса источника применяется в различных протоколах, относящихся к доступу к сети.

7.3.2.1 Валидация адреса источника в сценарии DHCPv6

При использовании серверами DHCPv6 и оборудованием пользователя адреса CGA они могут выполнять валидацию адреса источника.

Узел DHCPv6 (сервер, агент ретрансляции или клиент) принимает сообщение DHCPv6, источником которого является CGA, при этом сообщение DHCPv6 содержит подпись отправителя сообщения DHCPv6. Узел DHCPv6 проверяет и CGA, и подпись, после чего обрабатывает полезную информацию сообщения DHCPv6. Параметр CGA, включенный в сообщение DHCPv6, передается в опции параметра CGA, а подпись – в опции подписи. Для проверки CGA получатель – сервер DHCPv6 – может отыскать исходный CGA отправителя в поле адресов одноранговых узлов. В сценариях сервер–ретранслятор–клиент серверу DHCPv6, получившему сообщение DHCPv6 ретрансляция–пересылка, известно, что клиент расположен за ретранслятором. Сервер DHCPv6 отвечает сообщением ретрансляция–ответ, содержащим исходный CGA сервера. Последний содержится в уникальном идентификаторе DHCP-сервера (DUID), который является полезной информацией. Таким образом получатель – клиент DHCPv6 – может получить исходный CGA сервера для проверки адреса источника.

7.3.2.2 Валидация адреса источника в сценарии управления доступом

В сценариях управления доступом общим механизмом валидации адреса источника является взаимная привязка адресов IP и MAC. При выполнении валидации идентификационных данных устройства сеть проверяет не только исходный адрес, но и MAC-адрес Ethernet-интерфейса.

8 Функциональные требования для доступа к СПП на базе IPv6

Для поддержки сценариев, описанных в разделе 7, существующие функции некоторых функциональных объектов (FE) в структуре СПП необходимо расширить. В настоящем разделе описаны соответствующие функциональные требования.

8.1 Функции страты транспортирования

Функции сети доступа и граничные функции в функциях транспортирования тесно связаны с доступом пользователя к сети.

8.1.1 Функции, поддерживающие установление соединения по IPv6

- Рекомендуется, чтобы в сети доступа граничные функции предоставляли оборудованию CPE информацию о префиксе, что помогает оборудованию CPE получить надлежащую конфигурацию префикса и адреса через статические или динамические механизмы.
- Рекомендуется, чтобы граничные функции поддерживали изменение нумерации префиксов в соответствии с изменениями топологии сети или политики авторизации. Изменение нумерации префиксов на интерфейсах LAN и WAN оборудования CPE завершается передачей отдельных сообщений протокола, таких как сообщения реконфигурации DHCPv6 и RS.
- Рекомендуется, чтобы функции сети доступа и граничные функции взаимодействовали с определенной информацией, относящейся к префиксу, в целях завершения распределения префиксов и/или адресов. Функции сети доступа обрабатывают префикс и параметры конфигурации, полученные от граничных функций, и на основе этих параметров распределяют соответствующие префиксы расположенным ниже портам.
- Рекомендуется, чтобы функции сети доступа взаимодействовали с граничными функциями в целях передачи идентификационной информации узла доступа при необходимости, например в том случае, если граничный узел намерен напрямую управлять конфигурацией префиксов/адресов. Основываясь на данной идентификационной информации, граничные функции определяют префикс, который будет объявлен конкретному оборудованию CPE.

8.1.2 Функции, поддерживающие установление соединений, совместимых с IPv4

- Рекомендуется, чтобы граничные узлы поддерживали функции двойного стека.
- Рекомендуется, чтобы граничные узлы поддерживали функции туннелирования IPv4 через IPv6.
- В сценариях трансляции граничные узлы должны поддерживать функции трансляции протоколов IPv6/IPv4.

8.1.3 Функции поддержки механизмов безопасности

- Функции транспортирования позволяют оборудованию пользователя генерировать свой адрес с собственными параметрами. Что касается адреса, сгенерированного оборудованием пользователя, например CGA, рекомендуется, чтобы граничные функции поддерживали операции управления, которые могут регистрировать самогенерированные адреса пользователя на стороне сети (например, на сервере DHCPv6).
- В зависимости от того, соответствует ли адрес CGA конфигурации сети, граничные функции предоставляют право его использования или информируют пользовательское устройство о необходимости генерации другого CGA.
- Если граничный узел или узел сети доступа включает DHCPv6 и использует CGA, то рекомендуется, чтобы граничные функции и функции сети доступа поддерживали соответствующую функцию валидации адреса.

8.2 Функции конечного пользователя

Так как функции конечного пользователя тесно взаимодействуют с функциями транспортирования и функциями управления транспортированием, то функции конечного пользователя, активируемые протоколом IPv6 (такие как функции оборудования CPE и оконечного устройства), должны соответствовать следующим требованиям.

8.2.1 Функции, поддерживающие установление соединения по IPv6

- При каскадном делегировании рекомендуется, чтобы функции конечного пользователя применяли делегированный префикс и соответствующие политики или правила для домашней сети, в которой каскадный маршрутизатор поддерживает отправку каскадируемого префикса расположенному ниже маршрутизатору.
- При изменении нумерации префиксов рекомендуется, чтобы оборудование CPE проверяло новый префикс интерфейса LAN, содержащийся в сообщении реконфигурации DHCPv6, полученном от граничного узла, и запускало сообщение RS для обновления префикса интерфейса WAN.

- Если граничный узел инициирует изменение нумерации маршрутизатора, рекомендуется, чтобы после получения данного сообщения на интерфейсе WAN оборудование CPE могло обнаруживать обновленный префикс на интерфейсе WAN и запускать реконфигурацию делегирования префикса по протоколу DHCPv6.
- Функции конечного пользователя должны поддерживать роль клиента DHCPv6, взаимодействовать с параметрами функций транспортирования и отправлять серверу DHCPv6 (встроенному в узел доступа/граничный узел или независимому) запрос на конфигурацию адреса.

8.2.2 Функции, поддерживающие установление соединений, совместимых с IPv4

- Рекомендуется, чтобы оборудование пользователя поддерживало протоколы двойного стека.
- Если оператор разворачивает механизм совместного использования адресов IPv4, от оборудования пользователя может потребоваться поддержка функции трансляции сетевых адресов IPv4.

8.2.3 Функции, поддерживающие механизмы безопасности

Рекомендуется, чтобы функции конечного пользователя поддерживали валидацию адреса источника, в случае если функции конечного пользователя используют CGA в качестве адреса источника.

9 Аспекты безопасности

Настоящая Рекомендация в целом соответствует требованиям по безопасности, изложенным в [ITU-T Y.2701]. Для фильтрации адресов характерны следующие аспекты.

Как указано в разделе 6, для узлов IPv6 характерны многоадресные интерфейсы. В частности при множественной адресации узлы могут использовать несколько префиксов. В соответствии с политикой фильтрации, заданной поставщиком интернет-услуг, пакеты могут отклоняться при прохождении через расположенный выше шлюз, если префиксы адресов назначены другими поставщиками услуг интернета. Из-за наличия нескольких адресов узла IPv6 стандартная входная фильтрация более сложна, чем при использовании IPv4.

Библиография

[[b-ITU-T Y.2052] Рекомендация МСЭ-Т Y.2052 (2008 г.), *Структура множественной адресации в СПП на базе IPv6.*

[b-IETF RFC 1035] IETF RFC 1035 (1987), *Domain Names – Implementation and Specification.*

[b-IETF RFC 2894] IETF RFC 2894 (2000), *Router Renumbering for IPv6.*

[b-IETF RFC 3315] IETF RFC 3315 (2003), *Dynamic Host Configuration Protocol for IPv6 (DHCPv6).*

[b-IETF RFC 3633] IETF RFC 3633 (2003), *IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6.*

[b-IETF RFC 3971] IETF RFC 3971 (2005), *Secure Neighbour Discovery (SEND).*

[b-IETF RFC 4861] IETF RFC 4861 (2007), *Neighbour discovery for IP version 6 (IPv6).*

[b-IETF RFC 4862] IETF RFC 4862 (2007), *IPv6 Stateless Address Autoconfiguration.*

[b-IETF RFC 5072] IETF RFC 5072 (2007), *IP Version 6 over PPP.*

[b-IETF RFC 5113] IETF RFC 5113 (2008), *Network Discovery and Selection Problem.*

[b-IETF RFC 5172] IETF RFC 5172 (2008), *Negotiation for IPv6 Datagram Compression Using IPv6 Control Protocol.*

[b-IETF RFC 6146] IETF RFC 6146 (2011), *Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers.*

[b-IETF RFC 6147] IETF RFC 6147 (2011), *DNS64: DNS Extensions for Network Address Translation from IPv6 Clients to IPv4 Servers.*

СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

Серия A	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
Серия Y	**Глобальная информационная инфраструктура, аспекты межсетевого протокола, сети последующих поколений, интернет вещей и "умные" города**
Серия Z	Языки и общие аспекты программного обеспечения для систем электросвязи

Отпечатано в Швейцарии
Женева, 2019 г.