

Международный союз электросвязи

МСЭ-Т

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

Y.2051

(02/2008)

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

Сети последующих поколений – Структура и
функциональные модели архитектуры

Общий обзор сети последующих поколений на базе IPv6

Рекомендация МСЭ Т Y.2051

РЕКОМЕНДАЦИИ МСЭ-Т СЕРИИ Y

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

ГЛОБАЛЬНАЯ ИНФОРМАЦИОННАЯ ИНФРАСТРУКТУРА	
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
АСПЕКТЫ ПРОТОКОЛА ИНТЕРНЕТ	
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
IP TV по NGN	Y.1900–Y.1999
СЕТИ ПОСЛЕДУЮЩИХ ПОКОЛЕНИЙ	
Структура и функциональные модели архитектуры	Y.2000–Y.2099
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
БУДУЩИЕ СЕТИ	Y.3000–Y.3499
ОБЛАЧНЫЕ ВЫЧИСЛЕНИЯ	Y.3500–Y.3999
ИНТЕРНЕТ ВЕЩЕЙ И "УМНЫЕ" ГОРОДА И СООБЩЕСТВА	
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.

Рекомендация МСЭ-Т Y.2051

Общий обзор СПП на базе IPv6

Резюме

В Рекомендации МСЭ-Т Y.2051 определяется сеть последующих поколений (СПП), которая выполняет операции главным образом по требованиям протокола Интернет версии 6 (IPv6). Эта Рекомендация содержит общие требования к СПП на базе IPv6 и к ее общей архитектуре.

Хронологическая справка

Издание	Рекомендация	Утверждение	Исследовательская комиссия	Уникальный идентификатор*
1.0	МСЭ-Т Y.2051	29.02.2008 г.	13-я	11.1002/1000/9350

Ключевые слова

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 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 с целью 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 2017

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 данной рекомендации	1
4 Сокращения и акронимы	2
5 Соглашения по терминологии	2
6 Обзор сетей на базе IP	2
6.1 Классификация сетей IP	2
6.2 Основные особенности сетей на базе IPv6 в сравнении с сетями на базе IPv4	3
7 Обзор СПП на базе IPv6	5
7.1 Определение СПП на базе IPv6	5
7.2 Функциональная архитектура СПП на базе IPv6	6
7.3 Влияние внедрения протокола IPv6 на СПП	7
7.4 Связь с другими сетями IP	7
8 Общие требования к СПП на базе IPv6	8
9 Аспекты безопасности	8
Библиография	9

Введение

Протокол Интернет версии 6 (IPv6) становится основой сетей последующих поколений (СПП). Ожидается, что сети на базе IPv6 заменят сети на базе IPv4, чтобы преодолеть основные ограничения протокола Интернет версии 4 (IPv4). То есть СПП будут постепенно переходить на протокол IPv6.

СПП является сетью с пакетной коммутацией, которая предоставляет услуги электросвязи с помощью основных транспортных технологий и технологий доступа. IPv6 является четко определенным транспортным протоколом для поддержки транспортных функций СПП. Протокол обеспечивает значительную гибкость СПП. Эта гибкость полезна для улучшения настройки и работы сети, а также для предоставления услуг провайдером и пользователям СПП.

Рекомендация МСЭ-Т Y.2051

Общий обзор СПП на базе IPv6

1 Сфера применения

Эта рекомендация дает определение СПП на базе IPv6 для поддержки адресации, сигнализации, множественной адресации и миграции. Кроме того, рекомендация определяет общую архитектуру и общие требования к СПП на базе IPv6. Сфера применения данной рекомендации охватывает:

- классификацию сетей на базе IP,
- определение СПП на базе IPv6,
- функциональную архитектуру СПП на базе IPv6,
- общие требования к 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.2011] Recommendation ITU-T Y.2011 (2004), *General principles and general reference model for Next Generation Networks*.

[ITU-T Y.2012] Recommendation ITU-T Y.2012 (2006), *Functional requirements and architecture of the NGN release 1*.

3 Определения

3.1 Термины, определенные в других документах

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

3.1.1 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 услуг и/или выбираемым ими услугам. Она поддерживает универсальную подвижность, которая обеспечивает постоянное и повсеместное предоставление услуг пользователям.

3.2 Термины, определенные в данной рекомендации

В этой рекомендации определены следующие термины:

3.2.1 сеть СПП на базе IPv6 (IPv6-based NGN): Данный термин относится к СПП, обеспечивающим поддержку адресации, протоколов маршрутизации и услуг, связанных с IPv6. В СПП на базе IPv6 должны быть реализованы распознавание и обработка заголовков и опций IPv6, с учетом работы по различным базовым транспортным технологиям в страте транспортирования.

3.2.2 функции IP и функциональные объекты на базе IPv6 (IPv6-based functions and FEs): Это такие функции сетей СПП и функциональные объекты, которые распознают и обрабатывают протокол IPv6 с его заголовками и опциями. Эти функции выполняют специальные задачи, включая функции IPv6.

3.2.3 функции IP и функциональные объекты с поддержкой IPv6 (IPv6-enabled functions and FEs): Это такие функции СПП и функциональные объекты, которые распознают протокол IPv6 с его заголовками и опциями. Эти функции выполняют свои специальные задачи в СПП, за исключением функций IPv6.

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы:

АН	Authentication Header		Заголовок аутентификации
ESP	Encapsulating Security Payload		Инкапсуляция полезной нагрузки безопасности
FE(s)	Functional Entity(-ies)		Функциональный объект(ы)
ICMPv6	Internet Control Message Protocol for the Internet Protocol Version 6		Протокол межсетевых управляющих сообщений для протокола Интернет версии 6
IP	Internet Protocol		Протокол Интернет
IPsec	Internet Protocol Security		Набор протоколов для защиты данных, передаваемых по протоколу IP
IPv4	Internet Protocol Version 4		Протокол Интернет версии 4
IPv6	Internet Protocol Version 6		Протокол Интернет версии 6
NAC	Network Attachment Control		Управление присоединением сети
NAPT	Network Address and Port Translation		Преобразование сетевых адресов и портов
NGN	Next Generation Network	СПП	Сеть последующих поколений
QoS	Quality of Service		Качество обслуживания
RA	Router Advertisement		Объявление маршрутизатора
RAC	Resource and Admission Control		Управление ресурсами и допуском
RSVP	Resource ReserVation Protocol		Протокол резервирования сетевых ресурсов
SIP	Session Initiation Protocol		Протокол установления сеанса

5 Соглашения по терминологии

Отсутствуют.

6 Обзор сетей на базе IP

6.1 Классификация сетей IP

Сети IP классифицируют как IPv4 и IPv6, согласно типу протокола IP. Поведение этих сетей отличается в зависимости от особенностей каждой версии протокола. Этот критерий классификации сетей по IP применим также для различения спецификаций характеристик СПП, так как СПП базируется главным образом на транспортных технологиях, использующих IP.

С учетом этого, относящиеся к СПП сети IP должны классифицироваться, согласно следующим положениям:

- СПП на базе IPv6: это СПП, которая поддерживает протоколы адресации и маршрутизации, а также услуги, связанные с IPv6.
- СПП на базе IPv4: это СПП, которая поддерживает протоколы адресации и маршрутизации, а также услуги, связанные с IPv4.
- Сеть на базе IPv6, не являющаяся СПП: это сеть с коммутацией пакетов по IPv6, которая не удовлетворяет требованиям СПП.
- Сеть на базе IPv4, не являющаяся СПП: это сеть с коммутацией пакетов по IPv4, которая не удовлетворяет требованиям СПП.

На рисунке 1 показаны различные сети IP с точки зрения СПП.

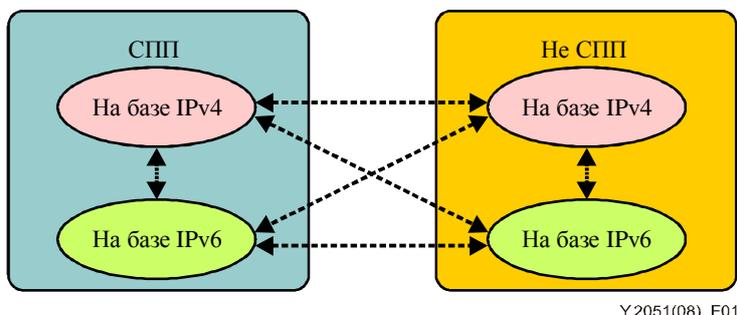


Рисунок 1 – Классификация сетей на базе IP

6.2 Основные особенности сетей на базе IPv6 в сравнении с сетями на базе IPv4

Уточнение различий между IPv4 и IPv6 является весьма полезным для идентификации операций по IPv4 и по IPv6, которые влияют на проектирование и обслуживание сети.

Ключевые особенности протоколов IPv4 и IPv6 приведены в таблице 1.

Таблица 1 – Ключевые особенности протоколов IPv4 и IPv6

		IPv4	IPv6
Формат пакета	Размер заголовка IPv6	Переменный размер	Постоянный размер
	Опциональные заголовки	Опциональные заголовки	Расширенные заголовки и опции
Адресация	Адресные пространства	Нехватка пространства адресов	Увеличенное пространство адресов
	Сквозное соединение	Нет	Есть
	Типы адресов	Одноадресная, многоадресная и широковещательная	Одноадресная, многоадресная и адрес произвольной группы
	Области адресов	Локальные и глобальные	Локальные для линии, локальные и глобальные
	Конфигурация адреса к интерфейсу	Один адрес	Множество адресов
	Распределение адресов к оборудованию	Множество адресов к одному интерфейсу	Множество адресов к нескольким интерфейсам
	Автоконфигурация адреса	Использование частных адресов	Использование общедоступных адресов
	Иерархия адресации	–	Есть

Таблица 1 – Ключевые особенности протоколов IPv4 и IPv6

		IPv4	IPv6
	Изменение порядка адресов	–	Есть
QoS	Управление конфликтами услуг	Поле типа услуги	Поле класса трафика
	Идентификация потоков трафика	Нет	Поле метки потока
	Распознавание данных управления/приоритетных данных	Нет	Заголовок расширения для каждого транзитного участка
Безопасность	Заголовок AH	Опционально	Обязательно
	Заголовок ESP	Опционально	Обязательно
Мобильность	Обнаружение новых сетей	–	Сообщения RA
	Генерация новых адресов	–	Автоконфигурация
	Заголовки мобильности	–	Обязательны
	Заголовок опции: опция пункта назначения, маршрута и т. д.	Опционально	Обязательно

Имеются ключевые особенности IPv6, которые могут существенно влиять различными способами на СПП, как например, схемы адресации, QoS, безопасность и мобильность.

- *Упрощенный формат пакетов*

Заголовки IPv6 упрощены по сравнению с заголовками IPv4. Некоторые поля заголовков IPv4 были опущены или сделаны опциональными для ограничения стоимости полосы пропускания. Кроме того, для уменьшения общей стоимости обработки пакета эти поля имеют постоянный размер.

- *Схема расширенной адресации*

Благодаря увеличенному размеру полей адресации в протоколе IP, схемы адресации IPv6 имеют большое адресное пространство, что обеспечивает больше уровней адресной иерархии, гораздо большее число адресуемых узлов и интерфейсов, а также более простую автоконфигурацию адресов. Улучшена масштабируемость многоадресной маршрутизации путем добавления поля "scope" при многоадресной рассылке. Кроме того, определен и используется новый тип адреса, "адрес произвольной группы", для отправки пакета в любую группу узлов.

- *QoS*

В заголовок IPv6 добавлены поля метки потока и класса трафика. Это дает возможность маркировать пакеты, которые принадлежат к особым "потокам" трафика и для которых отправитель требует специальной обработки, например качества обслуживания "не по умолчанию" или в "реальном времени". Кроме того, пересылаемый от одного транзитного участка к другому транзитному участку заголовок IPv6 с опцией предупреждения маршрутизатора будет указывать на содержимое пакетов IPv6, что позволит выборочно обрабатывать их на промежуточных узлах.

- *Обеспечение безопасности*

Протокол IPv6 поддерживает встроенные в IPsec службы, такие как аутентификация, целостность и конфиденциальность данных, используя расширенные заголовки аутентификации (AH) и инкапсуляции полезной нагрузки безопасности (ESP). Эти службы обеспечивают безопасность во всем глобальном пространстве адресов IP, от начального пункта до конечного, даже в тех случаях, когда промежуточные узлы не понимают заголовки протоколов IPsec.

- *Обеспечение мобильности*

Функциональные возможности IPv6, такие как выявление соседнего узла, разрешение адреса и обнаружение достижимости поддерживают услуги, связанные с мобильностью, путем использования заголовков для выбора варианта пункта назначения, маршрутизации и расширения мобильности.

7 Обзор СПП на базе IPv6

7.1 Определение СПП на базе IPv6

Сеть СПП на базе IPv6 определяют как СПП, которая поддерживает адресацию, маршрутизацию, протоколы и службы, связанные с IPv6. Это относится не только к транспортным аспектам сетей доступа и базовым сетям, но также включает другие функции, такие как функции поддержки конечного пользователя, управления транспортом и приложений/служб в рекомендациях [ITU-T Y.2011] и [ITU-T Y.2012].

Принимая во внимание эти определения и свойства, СПП на базе IPv6 можно представить, как показано на рисунке 2.

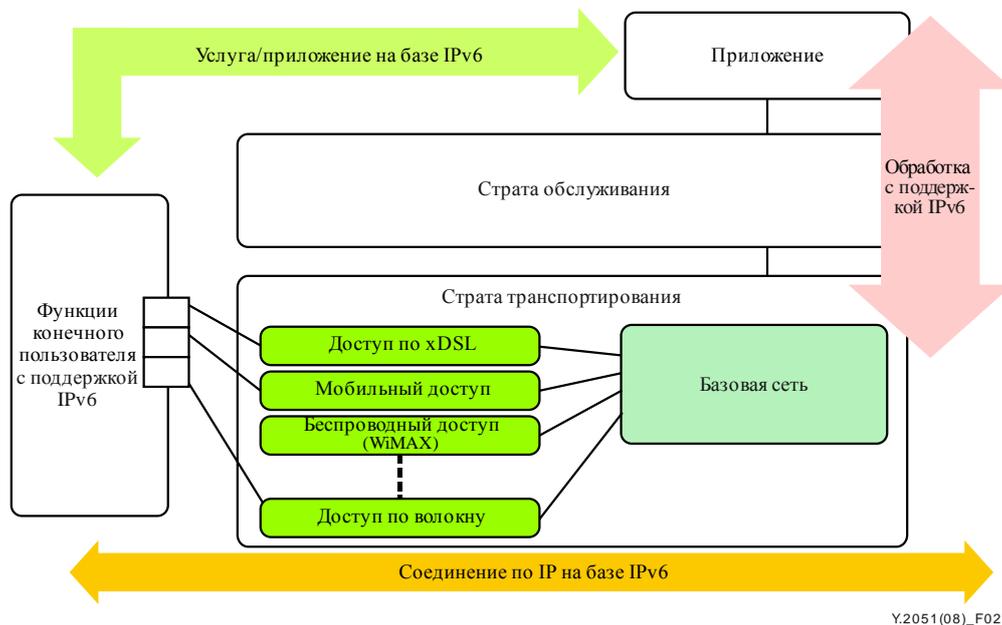


Рисунок 2 – Обзор СПП на базе IPv6

Как видно из рисунка 2, между функциями СПП и функциональными объектами (FEs) существует три взаимосвязи, которые описывают СПП на базе IPv6.

Во-первых, взаимосвязь между функциями конечного пользователя и стратой транспортирования. Сеть СПП на базе IPv6 позволяет гибко использовать различные инфраструктуры доступа для максимизации выгоды от использования IPv6. Один из таких примеров – использование функций множественной адресации и мобильности. Так, в сети СПП на базе IPv6, терминал пользователя или оборудование во время перемещения информации между сетями имеют возможность оперировать множеством неоднородных интерфейсов доступа и/или множеством адресов IPv6 через единственный или множество интерфейсов доступа.

Во-вторых, существует взаимосвязь между функциями конечного пользователя и приложениями. Функции конечного пользователя, активируемые протоколом IPv6, могут получать информацию через приложения, чтобы обеспечить безопасный и надежный транспорт по IPv6. Один из таких примеров – управление ключом для безопасности IP.

Наконец, существует взаимосвязь между стратой приложения и стратой транспортирования. Страта приложения может запросить страту транспортирования поддержать высокое качество обслуживания. Один из таких примеров – резервирование ресурсов.

7.2 Функциональная архитектура СПП на базе IPv6

Сеть СПП на базе IPv6 должна соответствовать принципам СПП, поэтому общая архитектура должна основываться на архитектуре СПП, определенной в [ITU-T Y.2012]. Эта сеть включает также страту транспортирования и страту обслуживания, как показано на рисунке 3.



Рисунок 3 – Функциональная архитектура СПП на базе IPv6

В этой модели архитектуры некоторые функции зависят от особенностей протокола IPv6: транспортные функции, функции конечного пользователя, функции управления присоединением к сети (NAC), функции управления ресурсами и допуском (RAC), а также функции поддержки приложений и услуг.

Функции транспортирования на базе IPv6 должны использоваться для присоединения различных сетей доступа и для транспортирования услуг IPv6 по базовой транспортной сети с использованием свойств множественной и иерархической адресации в IPv6. Эти сети доступа могут быть однородными или неоднородными. Если они являются неоднородными, транспортные функции на базе IPv6 должны поддерживать свойство множественной адресации, чтобы обеспечить множество сетевых подключений пользователям по различным неоднородным сетям доступа. Следовательно, все функции транспортирования и функциональные объекты (FEs) должны полностью поддерживать все свойства IPv6.

Чтобы обеспечить множество сетевых подключений конечному пользователю, функции конечного пользователя, активируемые протоколом IPv6, должны поддерживать свойства IPv6.

Функции NAC, активируемые протоколом IPv6, должны обеспечить такие свойства IPv6, как автоконфигурация, множественная адресация и обнаружение присоединения к сети. Функции NAC отвечают за динамическую конфигурацию адресов IPv6 и другие параметры конфигурации, связанные с оборудованием пользователя. Поэтому для поддержки услуг мобильности по протоколу IPv6 функции NAC должны обеспечить свойства автоконфигурации и множественной адресации.

Функции RAS, активируемые протоколом IPv6, должны поддерживать свойства IPv6 с точки зрения QoS и миграции IPv4/IPv6. Чтобы обеспечить высокое качество предоставления услуг, функции RAS должны обрабатывать заголовки расширения и опции IPv6. Кроме того, для поддержки миграции IPv4/IPv6, должна быть расширена функция преобразования сетевого адреса.

Приложения, активируемые протоколом IPv6, должны также поддерживать свойства IPv6, поскольку в данные этих приложений должны быть включены адреса IPv6, а чтобы оперировать вложенными в приложения IPv6 данными, потребуются функции шлюза уровня приложения.

7.3 Влияние внедрения протокола IPv6 на СПП

IPv6 является четко определенным транспортным протоколом, который обеспечивает транспортные функции СПП. Этот раздел в основных чертах и с различных точек зрения определяет следствия от использования протокола IPv6 в СПП.

- *Расширенные возможности обслуживания*

Протокол IPv6 позволяет управлять перегрузкой/потоками с помощью дополнительной информации QoS, как например, метки потока и т. д. Поле метки потока в заголовке протокола IPv6 идентифицирует поток независимо от протоколов транспортного уровня. Это означает, что в СПП могут быть легко введены новые расширенные возможности обслуживания.

Протокол IPv6 обеспечивает повышение мобильности путем устранения проблемы "треугольника маршрута".

Протокол IPv6 обеспечивает безопасность сети с помощью встроенных в IPv6 таких механизмов безопасности, как ESP и AH.

- *Соединение по IP "каждого с каждым"*

Чтобы справиться с растущим числом конечных пользователей/устройств, соединение по сети IP становится одной из жизненно важных функций. Использование глобальной маршрутизации адресов IPv4 в сети с миллионами устройств, например датчиков, невозможно. С другой стороны, протокол IPv6 предлагает преимущества локализации трафика с однозначными локальными адресами. Это делает некоторые устройства глобально доступными за счет присвоения адресов, область действия которых – весь мир. Таким образом, величайший потенциал IPv6 будет реализован для соединения "каждого объекта с каждым". Протокол IPv6 может выполнить этот принцип на всей сети Интернет.

- *Самоорганизация и обнаружение услуг с помощью автоконфигурации*

Протокол IPv6 предоставляет возможность автоконфигурации по протоколам обнаружения соседних объектов (NDP) и др. Путем соединения уровня IP с более низкими уровнями, автоконфигурация легко позволит управлять самоорганизацией и обнаружением услуг при управлении сетью, а также снизит общие требования к управлению. Кроме того, автоконфигурация адреса в протоколе IPv6 поможет динамическому присвоению адресов и идентификации множества пользователей/сетей в СПП. То есть за счет расширенных схем адресации в IPv6 конечные пользователи СПП получают множество общедоступных и частных идентификаторов.

- *Множественная адресация при использовании IPv6*

Протокол IPv6 может обслуживать множество неоднородных интерфейсов доступа и/или множество адресов IPv6 с помощью единственного или многих интерфейсов доступа. Множественная адресация обеспечит резервирование и отказоустойчивость.

7.4 Связь с другими сетями IP

Сеть СПП на базе IPv6 будет внедряться постепенно, в то время как СПП ближайшего будущего будут создаваться главным образом на базе IPv4. Это означает, что аналогично изучению вопросов, связанных с IPv6, потребуются также исследования для тех СПП на базе IPv4, которые будут преобразовываться в сети на базе IPv6, а также для взаимодействия между этими сетями и т. д. Эти исследования должны распространяться на другие сети на базе IP, которые не являются СПП.

Рисунок 4 поясняет взаимосвязи СПП на базе IPv6 с другими сетями на базе протокола IP. Этот рисунок показывает взаимоотношения различных сетей связи, принимая во внимание существование других сетей на базе IP: внутри СПП, вне СПП и взаимодействие с сетями, не являющимися СПП.

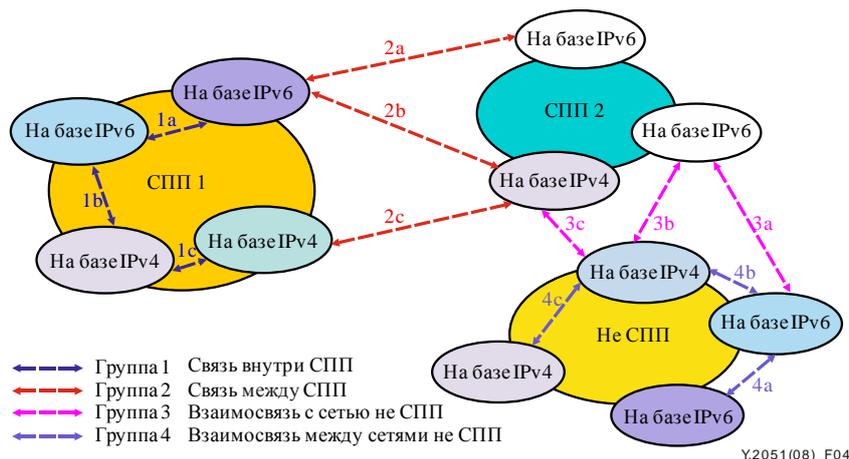


Рисунок 4 – Взаимодействие СПП на базе IPv6 с другими сетями на базе IP

8 Общие требования к СПП на базе IPv6

Протокол IPv6 обеспечивает не только расширение пространства адресов IP, но также различные дополнительные возможности, которые влияют на функции СПП и соответствующие функциональные объекты. В этом разделе определены общие требования к СПП на базе IPv6, которые зависят от свойств этого протокола. общепринято, что сеть СПП на базе IPv6 должна удовлетворять требованиям СПП версии 1. Дополнительные функции IPv6, указанные в этом разделе, будут рассмотрены в контексте требований к СПП версии 2 с точки зрения протокола IPv6.

- От СПП на базе IPv6 требуется поддержка заголовков IPv6 и их опций.
 - Сеть СПП должна распознавать и обрабатывать заголовки IPv6 и опции.
- От СПП на базе IPv6 требуется обеспечение возможности использования схем адресации протокола IPv6.
 - Эта сеть должна поддерживать все пространство адресов IPv6.
 - Эта сеть должна обеспечить автоконфигурацию и обнаружение соседних объектов по IPv6.
 - Эта сеть должна обеспечить множественную адресацию, используя свойства протокола IPv6.
- От сетей с поддержкой функций и функциональных объектов (FEs) IPv6 требуется поддержка заголовков IPv6 и их опций.
 - Эти сети должны распознавать заголовки IPv6 и опции.
 - Эти сети должны отличать в общем пакете IPv6 информацию управления, связанную с QoS.
- От СПП на базе IPv6 требуется обеспечить миграцию и взаимодействие без ущерба для предоставляемых пользователям услуг.
 - Эта сеть должна обеспечить взаимодействие с СПП на базе IPv4.
 - Эта сеть должна обеспечить взаимодействие с сетью на базе IPv4 и/или IPv6, которая не является СПП.

9 Аспекты безопасности

Эта рекомендация не требует каких-либо аспектов по безопасности и совместима с требованиями безопасности в [b-ITU-T Y.2701].

Библиография

- [b-ITU-T Y.2111] Recommendation ITU-T Y.2111 (2006), *Resource and admission control functions in Next Generation Networks*.
- [b-ITU-T Y.2201] Recommendation ITU-T Y.2201 (2006), *NGN release 1 requirements*.
- [b-ITU-T Y.2701] Recommendation ITU-T Y.2701 (2007), *Security requirements for NGN release 1*.
- [b-IETF RFC 2402] IETF RFC 2402 (1998), *IP Authentication Header*.
<<http://www.ietf.org/rfc/rfc2402.txt?number=2402>>
- [b-IETF RFC 2406] IETF RFC 2406 (1998), *IP Encapsulating Security Payload (ESP)*.
<<http://www.ietf.org/rfc/rfc2406.txt?number=2406>>
- [b-IETF RFC 2460] IETF RFC 2460 (1998), *Internet Protocol, Version 6 (IPv6) Specification*.
<<http://www.ietf.org/rfc/rfc2460.txt?number=2460>>
- [b-IETF RFC 2461] IETF RFC 2461 (1998), *Neighbor Discovery for IP Version 6 (IPv6)*.
<<http://www.ietf.org/rfc/rfc2461.txt?number=2461>>
- [b-IETF RFC 2474] IETF RFC 2474 (1998), *Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers*.
<<http://www.ietf.org/rfc/rfc2474.txt?number=2474>>
- [b-IETF RFC 2675] IETF RFC 2675 (1999), *IPv6 Jumbograms*.
<<http://www.ietf.org/rfc/rfc2675.txt?number=2675>>
- [b-IETF RFC 2711] IETF RFC 2711 (1999), *IPv6 Router Alert Option*.
<<http://www.ietf.org/rfc/rfc2711.txt?number=2711>>
- [b-IETF RFC 2766] IETF RFC 2766 (2000), *Network Address Translation – Protocol Translation (NAT-PT)*.
<<http://www.ietf.org/rfc/rfc2766.txt?number=2766>>
- [b-IETF RFC 3493] IETF RFC 3493 (2003), *Basic Socket Interface Extensions for IPv6*.
<<http://www.ietf.org/rfc/rfc3493.txt?number=3493>>
- [b-IETF RFC 3587] IETF RFC 3587 (2003), *IPv6 Global Unicast Address Format*.
<<http://www.ietf.org/rfc/rfc3587.txt?number=3587>>
- [b-IETF RFC 3697] IETF RFC 3697 (2004), *IPv6 Flow Label Specification*.
<<http://www.ietf.org/rfc/rfc3697.txt?number=3697>>
- [b-IETF RFC 3775] IETF RFC 3775 (2004), *Mobility Support in IPv6*.
<<http://www.ietf.org/rfc/rfc3775.txt?number=3775>>
- [b-IETF RFC 4007] IETF RFC 4007 (2005), *IPv6 Scoped Address Architecture*.
<<http://www.ietf.org/rfc/rfc4007.txt?number=4007>>
- [b-IETF RFC 4193] IETF RFC 4193 (2005), *Unique Local IPv6 Unicast Addresses*.
<<http://www.ietf.org/rfc/rfc4193.txt?number=4193>>
- [b-IETF RFC 4291] IETF RFC 4291 (2006), *IP Version 6 Addressing Architecture*.
<<http://www.ietf.org/rfc/rfc4291.txt?number=4291>>
- [b-IETF RFC 4311] IETF RFC 4311 (2005), *IPv6 Host-to-Router Load Sharing*.
<<http://www.ietf.org/rfc/rfc4311.txt?number=4311>>
- [b-IETF RFC 4443] IETF RFC 4443 (2006), *Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification*.
<<http://www.ietf.org/rfc/rfc4443.txt?number=4443>>

СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

Серия А	Организация работы МСЭ-Т
Серия D	Общие принципы тарификации
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	Оконечное оборудование, субъективные и объективные методы оценки
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 межсетевых протоколов, сети последующих поколений, интернет вещей и "умные" города
Серия Z	Языки и общие аспекты программного обеспечения для систем электросвязи