

МСЭ-Т

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

Y.2053

(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

Функциональные требования к переходу к IPv6 в СПП

Рекомендация МСЭ-Т Y.2053

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
IPTV по СПП	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 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
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.2053

Функциональные требования к переходу к IPv6 в СПП

Резюме

В Рекомендации МСЭ-Т Y.2053 приводятся возможные сценарии перехода к IPv6 и необходимые для их осуществления функциональные требования.

Хронологическая справка

Издание	Рекомендация	Утверждение	Исследовательская комиссия	Уникальный идентификатор*
1.0	МСЭ-Т Y.2053	29.02.2008 г.	13-я	11.1002/1000/9352

Ключевые слова

IPv4, IPv6, переход, 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 2019

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	2
5.1 Нативное IPv6-устройство	2
5.2 Механизм перехода к IPv6.....	2
5.3 Основные механизмы перехода к IPv6.....	2
6 IP как функция транспортирования в СПП.....	2
7 Основные подходы к сетевому взаимодействию и переходу к IPv6.....	3
7.1 Двойной IP-уровень (двойной стек)	3
7.2 Конфигурируемое туннелирование	3
7.3 Трансляция сетевых адресов и трансляция протоколов	3
8 Сценарии перехода к IPv6	4
8.1 Варианты 1 ~ 3 (с NAT-PT).....	6
8.2 Варианты 4 ~ 7 (с конфигурируемым туннелированием).....	6
8.3 Вариант 8 (с NAT-PT).....	6
8.4 Вариант 9 (с конфигурируемым туннелированием)	7
8.5 Варианты 10 ~ 11 (с двойным стеком)	7
8.6 Вариант 12 (с нативным IPv6)	7
9 Функциональные требования к переходу к IPv6 в страте транспортирования.....	7
9.1 Функции страты транспортирования	7
9.2 Функции конечного пользователя	12
9.3 Функции других сетей, не относящихся к СПП.....	12
10 Аспекты безопасности	12
Дополнение I – Переход к IPv6 в сетях СПП.....	13
I.1 Механизмы перехода к IPv6	13
I.2 Пример сценариев перехода согласно таблице 1	15
Библиография	20

Рекомендация ИТУ-Т Y.2053

Функциональные требования к переходу к IPv6 в СПП

1 Сфера применения

Целью настоящей Рекомендации является определение возможных сценариев перехода к IPv6 и необходимых для их осуществления функциональных требований.

Страта транспортирования СПП предоставляет пользователям СПП услуги по IP-подключению, однако конкретная версия протокола IP для действующих СПП не предполагается. Это означает, что протоколы IPv4 и IPv6 могут сосуществовать в СПП в процессе замены IPv4 на IPv6. Таким образом на этот период необходимо временное решение, например механизм перехода к IPv6 (см. разделы 6 и 7).

Если в СПП вводится механизм перехода к IPv6, то могут существовать разнообразные сценарии перехода, удовлетворяющие требованиям различных приложений или требованиям поставщика услуг; эти сценарии будут также влиять на существующие функциональные объекты СПП.

Таким образом в настоящей Рекомендации представлены возможные сценарии перехода к IPv6 и функциональные требования, необходимые для поддержки каждого из сценариев.

2 Справочные документы

Указанные ниже Рекомендации и другие источники 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 пользователям данной Рекомендации предлагается изучить возможность применения последнего издания Рекомендаций и других источников, перечисленных ниже. Список действующих в настоящее время Рекомендаций МСЭ-Т регулярно публикуется. Ссылка на документ, приведенный в настоящей Рекомендации, не придает ему как отдельному документу статус Рекомендации.

[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*.

[ITU-T Y.2111] Рекомендация МСЭ-Т Y.2111 (2006 год), *Функции управления ресурсами и установлением соединений в сетях последующих поколений*.

[ITU-T Y.2701] Recommendation ITU-T Y.2701 (2007), *Security requirements for 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 хост (host) [b-ITU-T Y.1540]: Компьютер, осуществляющий соединения посредством протоколов Интернет. На хосте реализуются функции маршрутизации (то есть он функционирует на уровне IP), а также могут быть реализованы дополнительные функции, включая протоколы высокого уровня (например, TCP на хосте-отправителе или хосте-получателе) и протоколы низкого уровня (например, ATM).

3.1.2 маршрутизатор (router) [b-ITU-T Y.1540]: Хост, который создает возможность связи между другими хостами путем пересылки IP-пакетов, используя содержимое их полей IP-адреса получателя.

3.1.3 двойной IP-уровень (dual IP layer) [b-IETF RFC 4213]: Двойной IP-уровень – это метод, позволяющий узлу поддерживать оба интернет-протокола – IPv4 и IPv6. Двойной IP-уровень называют также двойным стеком.

3.1.4 конфигурируемое туннелирование (configured tunneling) [b-IETF RFC 4213]: Конфигурируемое туннелирование – это метод для установления туннелей от пункта к пункту путем инкапсуляции пакетов IPv6 в IPv4 для транспортирования их по инфраструктурам IPv4 и наоборот.

3.2 Термины, определенные в настоящей Рекомендации

В настоящей Рекомендации определены следующие термины.

3.2.1 узел (node): Устройство, подключенное как часть компьютерной сети. Узлами могут быть компьютеры, сотовые телефоны, а также другие сетевые устройства, например маршрутизаторы, коммутаторы и концентраторы.

3.2.2 подсеть (subnet): Физическая сеть, обслуживаемая одним маршрутизатором, например сеть Ethernet (состоящая из одного или нескольких сегментов сети Ethernet или локальных сетей, присоединенных коммутаторами и шлюзами) или виртуальная локальная сеть (VLAN).

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы.

ALG	Application Layer Gateway	Шлюз уровня приложений
CPE	Customer Premises Equipment	Оборудование в помещении клиента
FE	Functional Entity	Функциональный объект
NAT-PT	Network Address Translation and Protocol Translation	Трансляция сетевых адресов и трансляция протоколов
SCF	Service Control Function	Функция управления услугами
SIT	Stateless IP/ICMP Translation Algorithm	Алгоритм трансляции IP/ICMP без сохранения состояния

5 Соглашения по терминологии

5.1 Нативное IPv6-устройство

Устройство, поддерживающее только стек IPv6.

5.2 Механизм перехода к IPv6

Механизм, обеспечивающий переход от протокола IPv4 к протоколу IPv6. Существует большое число механизмов перехода к IPv6, и пользователь может выбрать наиболее подходящий для среды развертывания.

5.3 Основные механизмы перехода к IPv6

К основным механизмам перехода к IPv6 относятся двойной IP-уровень и конфигурируемое туннелирование, которые могут быть реализованы на узле IPv6 [b-IETF RFC 4213].

6 IP как функция транспортирования в СПП

Функции СПП делятся на функции страты обслуживания и функции страты транспортирования, как указано в [ITU-T Y.2011]. Страта транспортирования обеспечивает возможность подключения через IP к страте обслуживания и пользователям СПП под управлением функций транспортирования. Таким образом протокол IP играет ключевую роль как функция транспортирования в СПП.

В сетях СПП большинство услуг предоставляется по IP-протоколу, при этом в основе самих IP-соединений могут лежать такие технологии, как ATM, Ethernet и др. Согласно спецификации СПП версии 1 предполагается, что версия IP-протокола не является фиксированной. Это означает, что протоколы IPv4 и IPv6 могут сосуществовать в СПП в процессе замены IPv4 на IPv6, и, следовательно, для поддержки перехода к IPv6 на этот период требуется специальный механизм.

Группой IETF представлено несколько механизмов в качестве рекомендаций по переходу к IPv6 [b-IETF RFC 4213]. Эти механизмы могут также представлять собой рекомендации для сети СПП, использующей IP как функцию транспортирования. Изучение IPv6 в СПП еще не завершено.

В настоящей Рекомендации используются такие механизмы перехода к IPv6, как двойной стек, конфигурируемое туннелирование, а также трансляция сетевых адресов и трансляция протоколов (NAT-PT) [b-IETF RFC 4213]. Более подробно эти механизмы рассматриваются в разделе 7.

При внедрении в СПП механизмов перехода к IPv6 возможны различные сценарии перехода. В настоящей Рекомендации, наряду с прочим, приведены вероятные сценарии такого рода.

7 Основные подходы к сетевому взаимодействию и переходу к IPv6

Сеть состоит из различных сетей на базе IPv4 и IPv6, расположенных в разных географических точках, соединение которых обеспечивается через основную транспортную сеть.

При организации взаимодействия и перехода от сети на базе IPv4 к сети на базе IPv6 применяются три основных подхода: двойной IP-уровень, конфигурируемое туннелирование и NAT-PT.

Более подробно эти механизмы рассматриваются в Дополнении I.

7.1 Двойной IP-уровень (двойной стек)

Узел с двойным IP-уровнем обеспечивает реализацию обеих версий протокола Интернет (IPv4 и IPv6), которые также поддерживаются одновременно. Этот узел может напрямую взаимодействовать с узлом, работающим только с IPv4, используя пакеты IPv4, а также напрямую взаимодействовать с узлом, работающим только с IPv6, используя пакеты IPv6. При связи с узлом двойного стека преобразование IP-протокола не производится ни в тракте передачи, ни в тракте сигнализации. Подробная информация по узлу с двойным IP-уровнем приведена в [b-IETF RFC 4213].

7.2 Конфигурируемое туннелирование

Конфигурируемое туннелирование представляет собой метод организации туннелей от пункта к пункту путем инкапсуляции пакетов IPv6 в IPv4 для транспортирования их по инфраструктурам IPv4 и наоборот.

В большинстве сценариев развертывания в будущем предусматривается создание инфраструктуры маршрутизации IPv6. По мере развертывания инфраструктуры IPv6 существующая инфраструктура маршрутизации IPv4 может сохраняться и использоваться для переноса трафика IPv6. Туннелирование обеспечивает возможность использования существующей инфраструктуры маршрутизации IPv4 для переноса трафика IPv6.

Узлы двойного стека могут направлять по туннелю пакеты IPv6 через области топологии маршрутизации IPv4 благодаря их инкапсуляции в пакеты IPv4. Туннелирование можно использовать различными способами:

- между маршрутизаторами;
- между хостами и маршрутизаторами;
- между хостами.

Конфигурируемое туннелирование можно использовать во всех указанных выше случаях, но наиболее вероятное использование этого метода соответствует сценарию между маршрутизаторами в связи с необходимостью четко установить конечные точки туннелирования.

7.3 Трансляция сетевых адресов и трансляция протоколов

Механизм NAT-PT использует трансляцию адресов (например, NAT) и трансляцию протоколов IPv6/IPv4 согласно алгоритму трансляции IP/ICMP без сохранения состояния (SIIT) [b-IETF RFC 2765] для обеспечения прозрачной маршрутизации к конечным хостам в сегменте IPv6, которые пытаются установить прямое и обратное соединение с конечными хостами в сегменте IPv4.

Алгоритм SPT определяет механизм трансляции протоколов, позволяющий устанавливать связь между хостами, работающими только с IPv6 и работающими только с IPv4, путем трансляции пакетов IPv4 и IPv6 без привязки к протоколу. При этом информация о состоянии для сеанса не требуется.

Некоторые приложения передают сетевые адреса в разделах полезной информации. Алгоритм NAT-PT не обладает информацией о приложениях и не отслеживает полезную информацию. Шлюз уровня приложений (ALG) может работать совместно с NAT-PT, поддерживая многие из таких приложений.

Как правило, функция NAT-PT размещается на краю сети. Если функция NAT-PT размещается в ядре сети, общая производительность сети будет значительно снижена, поскольку функция NAT-PT восстанавливает все проходящие через нее IP-пакеты.

NAPT-PT расширяет принципы трансляции на один этап, транслируя также идентификатор транспортирования (например, номера портов TCP и UDP, идентификаторы запросов ICMP). Функция NAPT-PT (трансляция сетевых адресов на уровне портов и трансляция протоколов), позволяет узлам IPv6 устанавливать прозрачное соединение с узлами IPv4, используя один адрес IPv4. Порты TCP/UDP узлов IPv6 транслируются в порты TCP/UDP для зарегистрированного адреса IPv4.

8 Сценарии перехода к IPv6

Существуют различные сценарии перехода к IPv6, удовлетворяющие требованиям пользователей, приложений или поставщиков услуг. В данном разделе приведены некоторые сценарии перехода с точки зрения страты транспортирования. По каждому сценарию в разделе 9 приведены пояснения функциональных требований по соответствующему функциональному объекту (FE). См. таблицу 1.

Пояснения к таблице 1

- IPv6/двойной стек – узел, работающий только с IPv6, или узел с двойным стеком
- IPv4/двойной стек – узел, работающий только с IPv4, или узел с двойным стеком
- IPv4 – узел, работающий только с IPv4
- IPv6 – узел, работающий только с IPv6
- Синяя ячейка – объект с поддержкой IPv6
- Красная ячейка – объект с поддержкой IPv4

Таблица 1 – Роль функциональных элементов в различных сценариях перехода

		Функция конечного пользователя А	EN-FE	ABG-FE	IBG-FE	NACF	RACF	Функция конечного пользователя В
NAT-PT	ВАРИАНТ 1	IPv6/ двойной стек	NAT-PT	IPv4	IPv4	–	Управление с NAT-PT	IPv4/ двойной стек
	ВАРИАНТ 2	IPv6/ двойной стек	IPv6/ двойной стек	NAT-PT	IPv4	–	Управление с NAT-PT	IPv4/ двойной стек
	ВАРИАНТ 3	IPv6/ двойной стек	IPv6/ двойной стек	IPv6/ двойной стек	NAT-PT	–	Управление с NAT-PT	IPv4/ двойной стек
Туннелирование	ВАРИАНТ 4	Конечная точка туннеля	IPv4	IPv4	IPv4	Информация о конечной точке туннеля	–	IPv6/ двойной стек
	ВАРИАНТ 5	IPv6/ двойной стек	Конечная точка туннеля	IPv4	IPv4	–	–	IPv6/ двойной стек
	ВАРИАНТ 6	IPv6/ двойной стек	IPv6/ двойной стек	Конечная точка туннеля	IPv4	–	–	IPv6/ двойной стек
	ВАРИАНТ 7	IPv6/ двойной стек	IPv6/ двойной стек	IPv6/ двойной стек	Конечная точка туннеля	–	–	IPv6/ двойной стек
NAT-PT	ВАРИАНТ 8	Пользовательская сеть с IPv6 (NAT-PT)	IPv4	IPv4	IPv4	–	Управление с NAT-PT	IPv4/ двойной стек
Туннелирование	ВАРИАНТ 9	Пользовательская сеть с двойным стеком (конечная точка туннеля)	IPv4	IPv4	IPv4	Информация о конечной точке туннеля	–	IPv6/ двойной стек
Двойной стек	ВАРИАНТ 10	Двойной стек	Двойной стек	Двойной стек	Двойной стек	–	–	Двойной стек
	ВАРИАНТ 11	Пользовательская сеть с двойным стеком	Двойной стек	Двойной стек	Двойной стек	–	–	Двойной стек
IPv6	ВАРИАНТ 12	IPv6	IPv6	IPv6	IPv6	–	–	IPv6

8.1 Варианты 1 ~ 3 (с NAT-PT)

В вариантах с 1-го по 3-й обе функции конечного пользователя имеют разные версии стека IP (либо функция конечного пользователя представляет собой двойной стек, но услуга/приложение поддерживает только стек IP, который отличается от других функций конечного пользователя). NAT-PT поддерживает функции конечного пользователя, имеющие другие стеки IP, для связи друг с другом путем трансляции пакетов IPv6 в пакеты IPv4 (и наоборот). Для этого один из функциональных объектов на пути между функциями конечного пользователя должен обеспечивать функцию NAT-PT.

В большинстве случаев функция NAT-PT не должна размещаться в базовом функциональном объекте, поскольку она отслеживает и переформирует все пакеты. Если функция NAT-PT размещается в базовом функциональном объекте, общая производительность сети может снизиться. Таким образом применение функционального объекта пограничного шлюза межсетевое соединения (IBG-FE) для функции NAT-PT не рекомендуется.

Для варианта 1 определены следующие требования:

- объект EN-FE использует двойной стек;
- объект EN-FE использует общедоступный адрес IPv4 для области IPv4 и глобальный адрес IPv6 для области IPv6;
- объект EN-FE использует функцию NAT-PT;
- объект EN-FE может использовать соответствующий шлюз ALG для конкретного приложения;
- функция RACF обеспечивает функции управления NAT-PT.

В вариантах 2 и 3 предъявляются те же требования, что и в варианте 1, за исключением того, что функция NAT-PT размещается на функциональном объекте ABG-FE или IBG-FE.

8.2 Варианты 4 ~ 7 (с конфигурируемым туннелированием)

В вариантах с 4-го по 7-й обе функции конечного пользователя представляют собой узлы IPv6, а сети между двумя функциями конечного пользователя поддерживают только IPv4. В этой ситуации для связи друг с другом функции могут использовать механизмы конфигурируемого туннелирования. При конфигурируемом туннелировании требуются две конечные точки туннеля для инкапсуляции и декапсуляции пакетов IPv4. Два функциональных объекта на линии связи должны быть конечной точкой туннеля.

Для варианта 5 определены следующие требования:

- объект EN-FE использует двойной стек;
- объект EN-FE использует общедоступный адрес IPv4 для конечной точки туннеля и глобальный адрес IPv6 для области IPv6;
- объект EN-FE использует функцию конечной точки туннеля;
- конечной точкой туннеля для функции конечного пользователя В может служить любой из функциональных объектов EN-FE, ABG-FE, IBG-FE в области функций конечного пользователя В.

В вариантах 6 и 7 предъявляются те же требования, что и в варианте 5, за исключением того, что конечной точкой туннеля для функции конечного пользователя А является функциональный объект ABG-FE или IBG-FE.

В ряде случаев сама функция конечного пользователя может служить конечной точкой туннеля. Это отображено в варианте 4. В этом варианте функция NACF должна предоставлять информацию для другой конечной точки туннеля.

8.3 Вариант 8 (с NAT-PT)

В этом варианте функция конечного пользователя А использует пользовательскую сеть с IPv6, а другая функция конечного пользователя представляет собой узел IPv4; таким образом функция конечного пользователя А должна использовать функцию NAT-PT. Другие ситуации совпадают с вариантами 1 ~ 3.

Для варианта 8 определены следующие требования:

- функция конечного пользователя А использует двойной стек;
- функция конечного пользователя А использует общедоступный адрес IPv4 для области IPv4 и глобальный адрес IPv6 для области IPv6;
- функция конечного пользователя А использует функцию NAT-PT;
- функция конечного пользователя А может использовать соответствующий шлюз ALG для конкретного приложения;
- функция RACF предоставляет функции управления NAT-PT.

8.4 Вариант 9 (с конфигурируемым туннелированием)

В этом варианте функцией конечного пользователя А является пользовательская сеть с IPv6, а другой функцией конечного пользователя – узел IPv6; таким образом функция конечного пользователя А должна являться конечной точкой туннеля. Другие ситуации совпадают с вариантом 4.

8.5 Варианты 10 ~ 11 (с двойным стеком)

Варианты 10 ~ 11 являются оптимальными. В этом случае каждый функциональный объект использует двойной стек, благодаря чему большинство приложений и услуг могут связываться друг с другом без учета конкретной версии IP.

8.6 Вариант 12 (с нативным IPv6)

Вариант 12 представляет собой конечный этап перехода к IPv6. В этом варианте каждый функциональный объект, каждое приложение и каждая услуга работают только с IPv6.

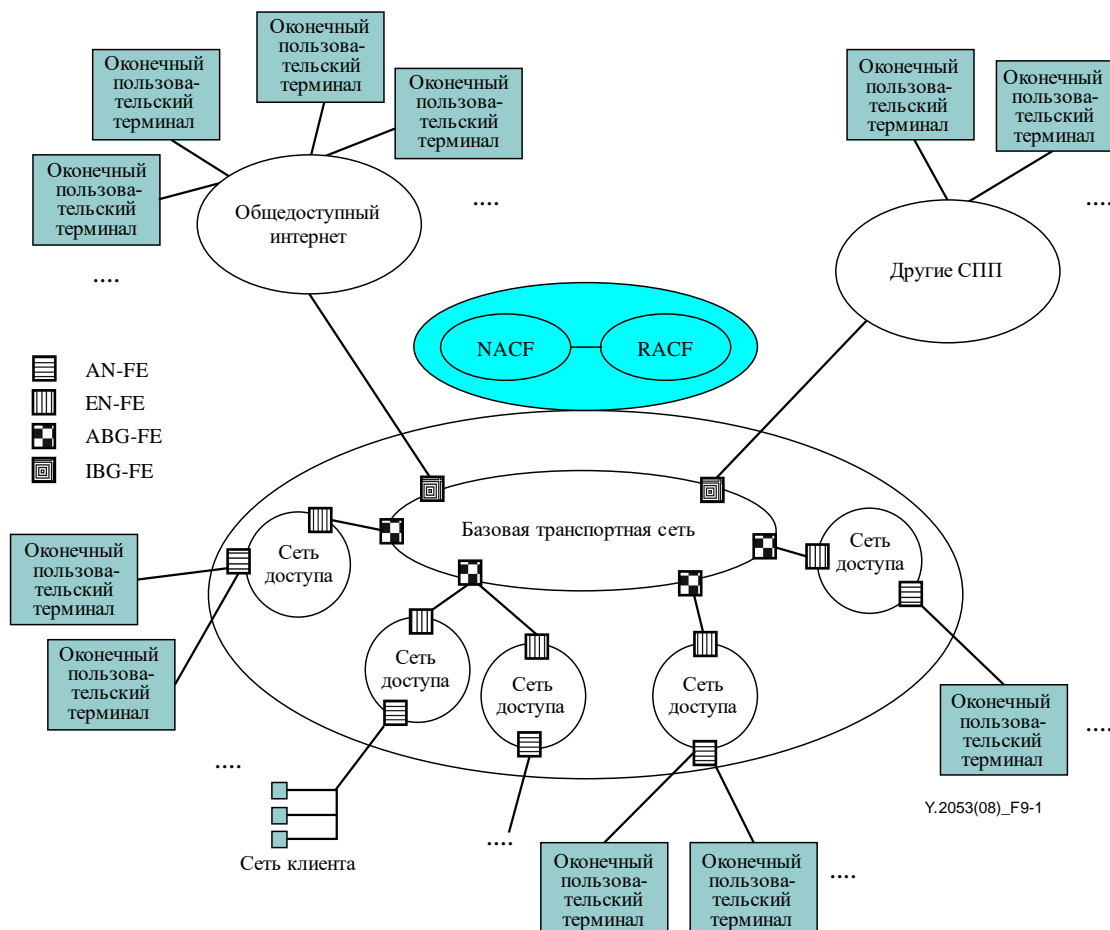
9 Функциональные требования к переходу к IPv6 в страте транспортирования

Как указано в разделе 8, некоторые функциональные объекты в страте транспортирования должны поддерживать функцию перехода к IPv6 в соответствии с конкретным сценарием. В данном разделе определяются функциональные объекты, связанные с переходом к IPv6, и приводятся функциональные требования к этим объектам.

9.1 Функции страты транспортирования

Функции транспортирования СПП обеспечивают возможность подключения по IP к страте обслуживания СПП и оборудованию конечных пользователей под контролем компонентов NACF и RACF. На рисунке 9-1 показан пример конфигурации СПП с точки зрения страты транспортирования.

Набор функциональных объектов, связанных с переходом к IPv6, может быть другим в каждом конкретном сценарии перехода.



**Рисунок 9-1 – Пример конфигурации СПП
(представление со стороны страты транспортирования)**

9.1.1 Функции транспортирования

Функции транспортирования включают в себя функции транспортирования сети доступа и функции транспортирования базовой сети. Относящиеся к ним функции EN-FE, ABG-FE, IBG-FE связаны с переходом к IPv6

9.1.1.1 Функции транспортирования сети доступа

Функции транспортирования сети доступа обеспечивают доступ конечных пользователей к сети, а также сбор и агрегирование трафика, создаваемого обращениями пользователей к базовой сети. Таким образом в качестве функций транспортирования сети доступа могут использоваться функция конечной точки туннеля и функция NAT-PT.

а) *Функциональный объект узла доступа (AN-FE)*

В настоящей Рекомендации предполагается, что AN-FE представляет собой устройство 2-го уровня; таким образом, он не входит в функциональные возможности протокола доступа.

б) *Функциональный объект пограничного узла (EN-FE)*

Объект EN-FE в составе функций транспортирования сети доступа подключается к функциям транспортирования пакетов базовой сети. В случае подключения к функциям транспортирования базовой IP-сети данный функциональный объект должен являться устройством 3-го уровня, обладающим возможностями переадресации по IP-протоколу.

В варианте 1 и варианте 5 EN-FE может быть конечной точкой туннеля и/или устройством NAT-PT. В обоих случаях объект EN-FE должен использовать двойной стек.

- Конечная точка туннеля. Функция конечного пользователя с IPv6 пытается связаться с другой функцией конечного пользователя IPv6 в другой сети через базовую транспортную сеть IPv4. В этом случае EN-FE должен являться конечной точкой туннеля (вариант 5). Когда объект EN-FE принимает пакеты IPv6 от функций конечного пользователя с IPv6, он инкапсулирует его в заголовке IPv4 и перенаправляет на другую конечную точку туннеля.
 - Сценарий варианта 5. Функция конечного пользователя А и функция конечного пользователя В являются узлами IPv6. Одной конечной точкой туннеля для функции конечного пользователя А является объект EN-FE, а другой конечной точкой туннеля может быть либо объект EN-FE, либо АВG-FE, либо IBG-FE в области функции конечного пользователя В. Функциональные объекты на линии между обеими конечными точками туннеля поддерживают IPv4.

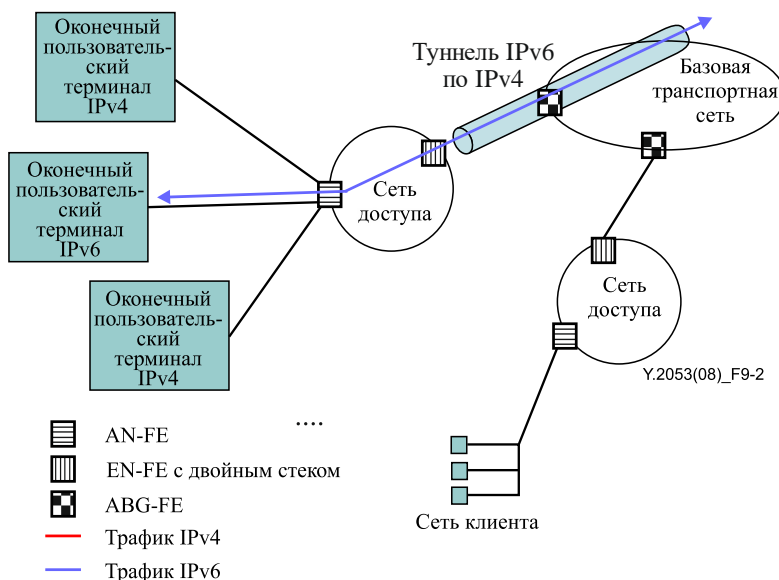


Рисунок 9-2 – EN-FE как конечная точка туннеля

- NAT-PT. Если объект EN-FE поддерживает функцию NAT-PT, функция конечного пользователя IPv6 может связываться с другими функциями конечного пользователя IPv4. В случаях, когда EN-FE поддерживает функцию NAT-PT, объект EN-FE транслирует пакеты IPv6 с оконечных пользовательских терминалов IPv6 в пакеты IPv4 и обратно. Если объект EN-FE использует функцию NAT-PT, он должен управляться функцией RACF [ITU-T Y.2111].
 - Сценарий варианта 1. Функция конечного пользователя А с IPv6 пытается установить соединение с функцией конечного пользователя В, поддерживающей только IPv4. Объект EN-FE в области функции конечного пользователя А использует функцию NAT-PT. Другие функциональные объекты на линии поддерживают IPv4.

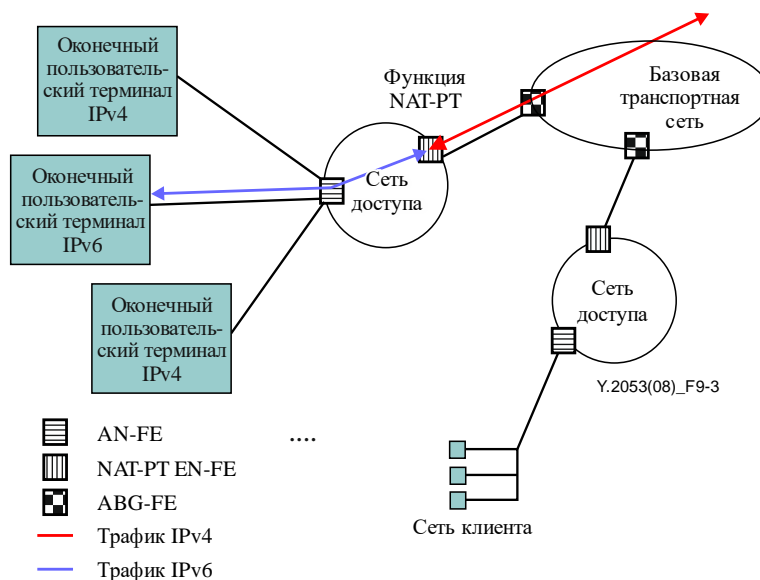


Рисунок 9-3 – EN-FE как NAT-PT

- Развертывание нативных IPv6-устройств. Если к объекту (объектам) AN-FE, которым(и) управляет объект EN-FE, не подключен окончательный пользовательский терминал с IPv4, то EN-FE может являться нативным IPv6-устройством. Если объект EN-FE обновлен до нативного IPv6-устройства, он просто перенаправляет трафик IPv6 на объект ABG-FE.
 - Сценарий варианта 2. Если функция конечного пользователя IPv6 намерена установить соединение с другими функциями конечного пользователя IPv4, объект ABG-FE должен являться NAT-PT-устройством.
 - Сценарий варианта 6. Если функция конечного пользователя IPv6 намерена установить соединение с другими функциями конечного пользователя IPv6, объект ABG-FE должен являться конечной точкой туннеля.

9.1.1.2 Функции транспортирования базовой сети

Функции транспортирования базовой сети отвечают за транспортирование информации по всей базовой сети. Функция конечной точки туннеля и функция NAT-PT могут размещаться на объектах ABG-FE и IBG-FE, однако размещение функции NAT-PT на функциональных объектах базовой сети не рекомендуется.

а) Функциональный объект пограничного шлюза (ABG-FE)

Объект ABG-FE – это пакетный шлюз между сетью доступа и базовой транспортной сетью. Объект(ы) EN-FE, агрегирующий пользовательский трафик в СПП, подключаются к ABG-FE. Объект ABG-FE может быть конечной точкой туннеля и/или устройством с поддержкой NAT-PT в вариантах 2 и 6. В обоих случаях объект EN-FE должен использовать двойной стек.

- Конечная точка туннеля. Если объект EN-FE не поддерживает конечную точку туннеля, то объект ABG-FE должен являться конечной точкой туннеля для трафика IPv6 с окончательных пользовательских терминалов. В этом случае объект ABG-FE выполняет больше функций, чем в варианте 5, поскольку объект ABG-FE дополнительно служит конечной точкой терминала, в которой сосредотачивается весь трафик IPv6 с подключенных объектов EN-FE.
 - Сценарий варианта 6. Если объект EN-FE использует двойной стек, но не поддерживает конечную точку туннеля или все функции конечного пользователя, а объекты EN-FE обновлены до нативных IPv6-устройств, объект ABG-FE должен являться конечной точкой туннеля для трафика IPv6 с окончательных пользовательских терминалов. Другой конечной точкой туннеля может быть либо объект EN-FE, либо ABG-FE, либо IBG-FE в области другой функции конечного пользователя.

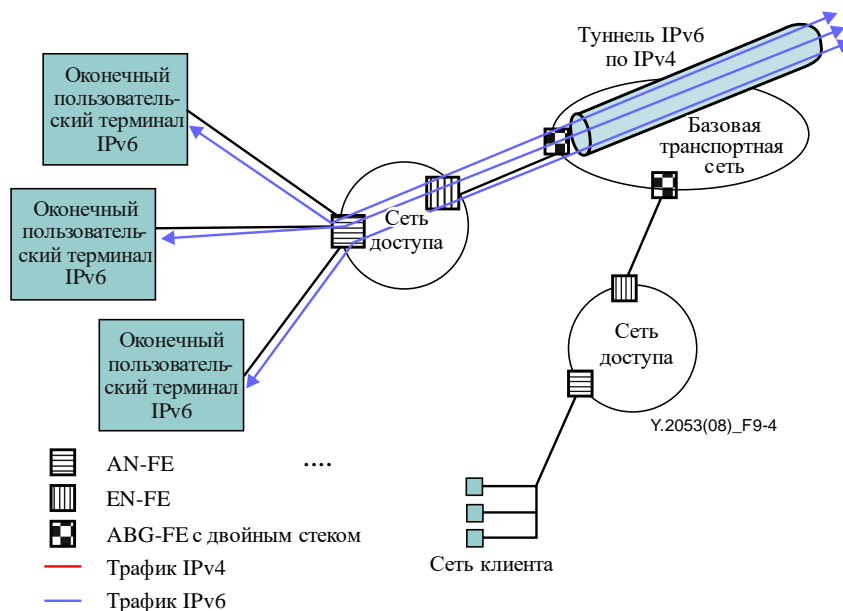


Рисунок 9-4 – ABG-FE как конечная точка туннеля

- NAT-PT. Если функция конечного пользователя IPv6 намерена установить соединение с функцией конечного пользователя IPv4, а объект EN-FE не поддерживает NAT-PT, то объект ABG-FE должен поддерживать функцию NAT-PT.
 - Сценарий варианта 2. Функция конечного пользователя А, поддерживающая только IPv6, пытается установить соединение с функцией конечного пользователя В, поддерживающей только IPv4. Объект EN-FE может быть нативным IPv6-устройством или использовать двойной стек. В этом случае ABG-FE должен обладать функцией NAT-PT. Другие функциональные объекты поддерживают IPv4.
- Развертывание нативных IPv6-устройств. Если все объекты EN-FE и все объекты ABG-FE обновлены до нативного IPv6-устройства.
 - Сценарий варианта 3. Если функция конечного пользователя IPv6 намерена установить соединение с другими функциями конечного пользователя IPv4, объект IBG-FE должен являться NAT-PT-устройством.
 - Сценарий варианта 7. Если функция конечного пользователя IPv6 намерена установить соединение с другими функциями конечного пользователя IPv6, объект IBG-FE должен являться конечной точкой туннеля.

б) Функциональный объект пограничного шлюза присоединения (IBG-FE)

Объект IBG-FE – это пакетный шлюз, используемый для соединения базовой транспортной сети оператора с базовой транспортной сетью другого оператора, поддерживающей пакетные услуги (см. рисунок 9-1). На начальном этапе большинство объектов IBG-FE поддерживают только IPv4, однако в конечном итоге базовая транспортная сеть будет полностью поддерживать двойной стек и в конце концов станет нативной IPv6-сетью (варианты 10, 11 и 12). В течение переходного периода, если объект ABG-FE, подключенный к IBG-FE, обновляется до нативного IPv6-устройства, объект IBG-FE должен являться конечной точкой туннеля или NAT-PT (варианты 3 и 7).

- Сценарий варианта 7. Если объект ABG-FE использует двойной стек, но не поддерживает конечную точку туннеля или все функции конечного пользователя, а объекты EN-FE и ABG-FE обновлены до нативных IPv6-устройств, объект IBG-FE должен являться конечной точкой туннеля для трафика IPv6 от функций конечного пользователя. Другой конечной точкой туннеля может быть либо IBG-FE, либо ABG-FE, либо EN-FE в области другой функции конечного пользователя.

Если функция конечного пользователя IPv6 намерена установить соединение с функцией конечного пользователя IPv4, а объект ABG-FE не поддерживает NAT-PT, то объект IBG-FE должен поддерживать функцию NAT-PT (вариант 3). Однако не рекомендуется использовать функцию NAT-PT между базовыми транспортными сетями

- Сценарий варианта 3. Функция конечного пользователя А, поддерживающая только IPv6, пытается установить соединение с функцией конечного пользователя В, поддерживающей только IPv4. Объект ABG-FE может быть нативным IPv6-устройством или использовать двойной стек. В этом случае IBG-FE должен обладать функцией NAT-PT. Другие функциональные объекты поддерживают IPv4.

9.1.2 Функции управления в страте транспортирования

9.1.2.1 Функции контроля доступа к сети (NACF)

а) Функциональный объект конфигурации доступа к сети (NAC-FE)

NAC-FE отвечает за распределение IP-адресов пользовательским устройствам [ITU-T Y.2012]. Он также может распределять другие параметры конфигурации сети, такие как адрес серверов DNS или посредников сигнализации и так далее. Таким образом, если функция конечного пользователя является конечной точкой туннеля или использует двойной стек, объект NAC-FE должен предоставлять следующую дополнительную информацию.

- Функция конечного пользователя использует двойной стек. Если функция конечного пользователя использует двойной стек, объект NAC-FE должен распределять адрес IPv6 и IPv4 функции конечного пользователя.
- Функция конечного пользователя является конечной точкой туннеля. Если функция конечного пользователя является пользовательским терминалом с двойным стеком или сетью клиента, она может являться конечной точкой туннеля (варианты 4 и 9). В этом случае объект NAC-FE должен распределять информацию о конфигурации другой конечной точки туннеля (см. [b-IETF draft-03]).

9.1.2.2 Функции управления ресурсами и установлением соединений (RACF)

Функция RACF [ITU-T Y.2111] определяет соответствующие требования и функциональную архитектуру, охватывающие такие аспекты, как резервирование ресурсов, управление установлением соединения и управление шлюзом, трансляция сетевых адресов на уровне портов (NAPT) и управление работой брандмауэра, и обход транслятора сетевых адресов (NAT). Таким образом, если NAT-PT используется в качестве механизма перехода к IPv6, функция RACF должна учитывать требования для сценариев NAT-PT (варианты 1, 2, 3 и 8).

9.2 Функции конечного пользователя

9.2.1 Терминал

Сам оконечный пользовательский терминал может являться конечной точкой туннеля (вариант 4). В этом случае другой конечной точкой туннеля может являться еще один оконечный терминал – EN-FE, ABG-FE или IBG-FE.

9.2.2 Сеть клиента

В этом случае оборудование CPE может являться конечной точкой туннеля или NAT-PT-устройством (варианты 8 и 9).

9.3 Функции других сетей, не относящихся к СПП

Если функция пользователя СПП пытается установить соединение с функциями других сетей, не относящихся к СПП, соответствующий объект другой такой сети должен играть роль, аналогичную описанной в разделе 8.

10 Аспекты безопасности

Настоящая Рекомендация не содержит каких-либо специальных требований по безопасности и поддерживает требования по безопасности, приведенные в [ITU-T Y.2701].

Дополнение I

Переход к IPv6 в сетях СПП

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации.)

I.1 Механизмы перехода к IPv6

В данном разделе показаны три архитектуры перехода к IPv6 с точки зрения архитектуры механизмов перехода к СПП.

а) Двойной стек

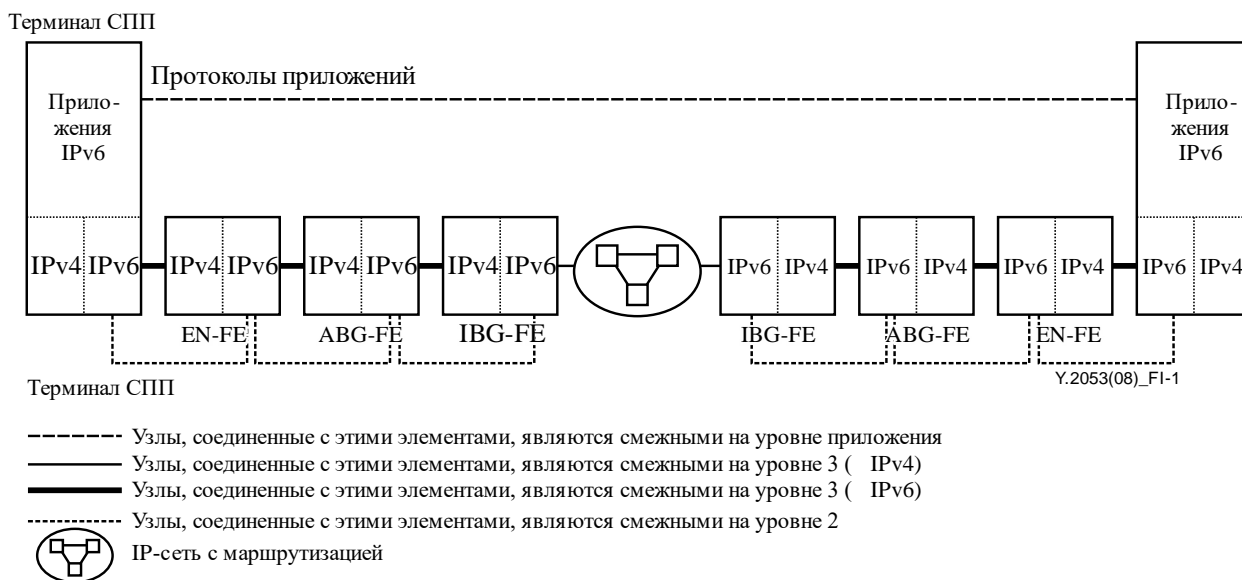


Рисунок I.1 – Пример сценария связи с использованием полного двойного стека

Для узлов IPv6 наиболее простой способ поддержания совместимости с узлами, работающими только с IPv4, – это полная поддержка IPv4. Узлы IPv6, обеспечивающие полную поддержку IPv4 и IPv6, называются "узлы с двойным стеком". Узлы с двойным стеком способны отправлять и принимать пакеты обоих протоколов – IPv4 и IPv6. Они могут напрямую взаимодействовать с узлами IPv4, используя пакеты IPv4, а также напрямую взаимодействовать с узлами IPv6, используя пакеты IPv6.

На рисунке I.1 показана ситуация, в которой услуги IPv6 связываются друг с другом в сети с двойным стеком.

b) *Конфигурируемый туннель*

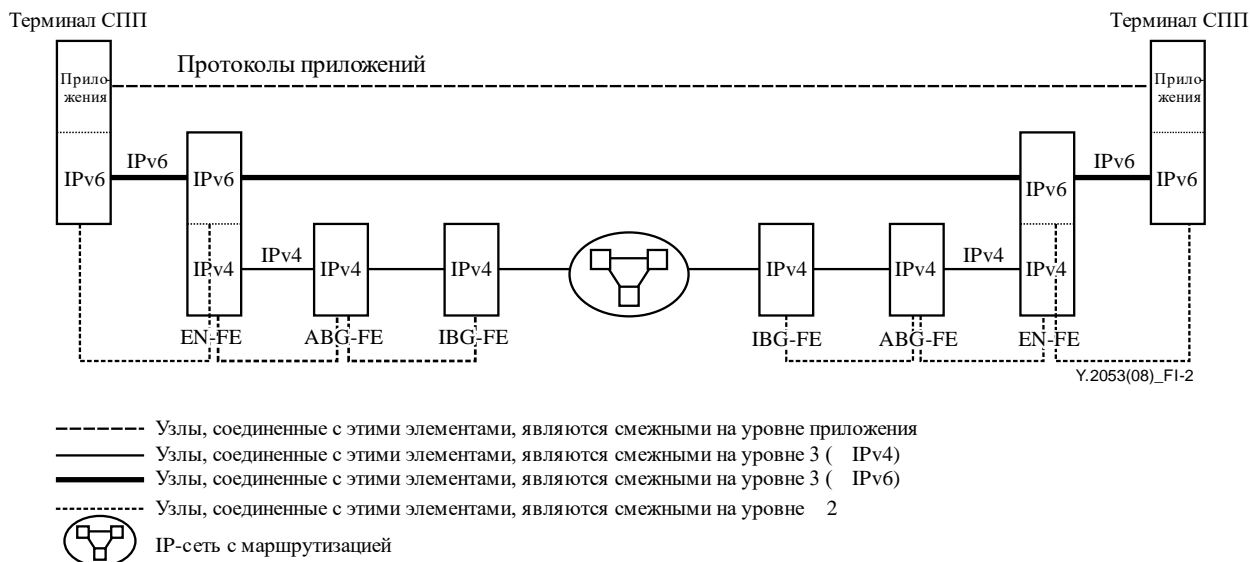


Рисунок I.2 – Пример сценария связи с использованием конфигурируемого туннеля

На начальном этапе перехода к IPv6 большинство узлов поддерживают только IPv4. То есть работать с IPv6 способно лишь небольшое количество маршрутизаторов в базовой транспортной сети. На этом этапе целесообразно использовать конфигурируемый туннель.

В этом случае используются узлы с двойным стеком. Приложения, поддерживающие IPv6, запускаются на обоих конечных узлах, соединенных по стеку IPv6, и пакеты IPv6 передаются по стеку IPv4 базовой транспортной сети. С этой точки зрения конечной точкой туннеля, смежной с объектом EN-FE на уровне 3, является другой объект EN-FE.

В этом сценарии объект EN-FE агрегирует трафик с оконечных IPv6-устройств сети СПП, образуя узел с двойным стеком. Некоторые из оконечных устройств сетей СПП, подключенных к EN-FE, намерены пользоваться услугами IPv6. Конфигурируемый туннель является наиболее оптимальным средством, позволяющим предоставлять им услуги IPv6, поскольку большинство функциональных объектов базовой транспортной сети поддерживают только IPv4. В этом случае две конечные точки туннеля – это объекты EN-FE. Объект EN-FE агрегирует конечные точки туннеля нескольких оконечных устройств СПП, которые намерены пользоваться услугами IPv6.

c) *NAT-PT*

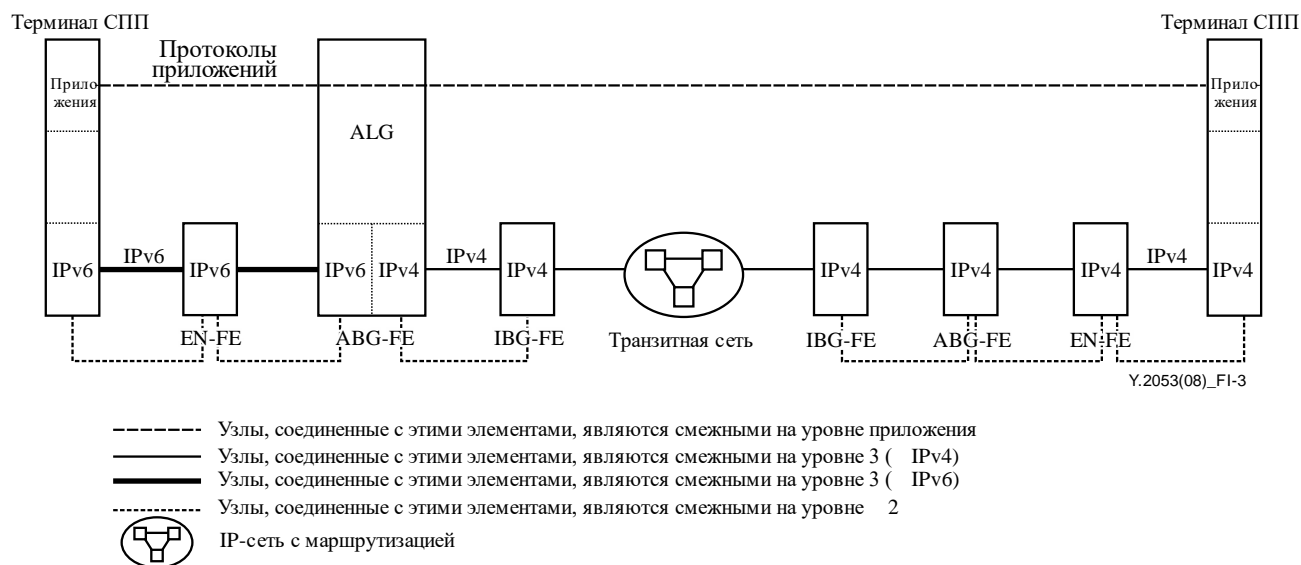


Рисунок I.3 – Пример сценария развертывания сети с NAT-PT

Механизм NAT-PT (трансляция IPv4/IPv6) обычно используется в пограничных подсетях на базе "острова" IPv6. Оконечные IPv6-устройства в сетях СПП, подключенные после устройства NAT-PT, могут через них связываться с другими оконечными IPv6-устройствами СПП или другими IPv4-устройствами СПП.

NAT-PT транслирует заголовок IPv6 в заголовок IPv4 и обратно. Шлюз ALG транслирует заголовок прикладного протокола, если тот содержит какую-либо информацию уровня IP.

Все пакеты, проходящие через устройство NAT-PT, восстанавливаются, если каждый конечный узел соединения использует другой стек протокола IP. Это приводит к снижению производительности сети. Таким образом механизм NAT-PT нецелесообразно использовать в базовой сети.

1.2 Пример сценариев перехода согласно таблице 1

В процессе перехода к IPv6 могут сосуществовать узлы нескольких типов, например узлы с двойным стеком, узлы, поддерживающие только IPv6 или только IPv4. В данном разделе для каждого конкретного варианта представлены сценарии развертывания сети в течение переходного периода.

А) Сценарий вариантов 10, 11 (с двойным стеком)

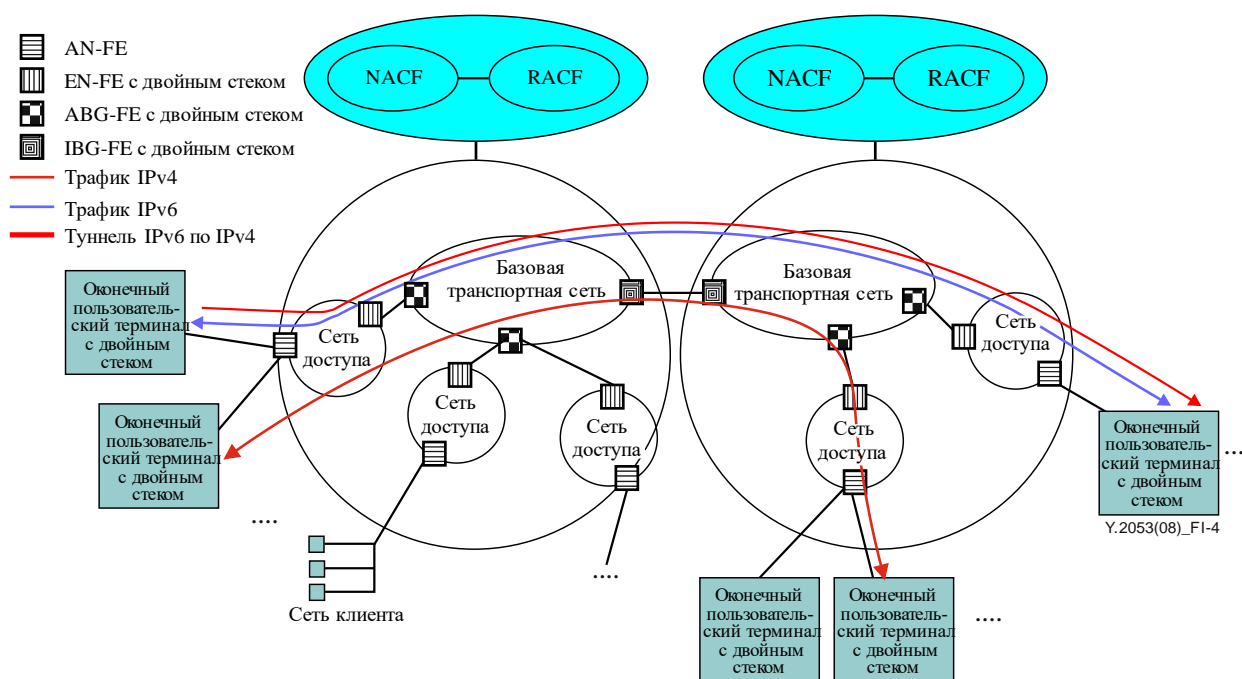


Рисунок 1.4 – Сценарий "узел с двойным стеком – узел с двойным стеком"

Данный сценарий является наиболее оптимальным. Все оконечные пользовательские терминалы и переходные функциональные объекты базовой сети и сети доступа используют двойной стек и маршрутизируемый адрес IPv4/IPv6. Приложения IPv4 и IPv6 могут запускаться на оконечном пользовательском терминале с двойным стеком и связываться с другими приложениями, запущенными на другом таком терминале с двойным стеком без поддержки со стороны других механизмов перехода к IPv6.

- DNS

В этом случае DNS играет важную роль.

Система доменных имен (DNS) используется в протоколах IPv4 и IPv6 для установления соответствия между именами хостов и IP-адресами. Библиотека разрешения имен DNS на узле с двойным стеком должна быть способна обрабатывать записи A и AAAA. Если результат запроса DNS одновременно содержит записи A и записи AAAA, библиотека разрешения имен может перегруппировать результаты, возвращаемые приложению, чтобы повлиять на версию пакетов IP, используемых для связи с данным узлом, то есть использовать первыми либо пакеты IPv6, либо пакеты IPv4.

Приложения должны быть способны определять, какие записи им требуются – IPv4, IPv6 или оба типа. В соответствии с этим распознаватель просматривает те или иные семейства адресов. Поскольку большинство приложений обрабатывают адреса в порядке их получения от распознавателя, это может повлиять на то, каким версиям IP отдадут "предпочтения" приложения.

Вопросы и оперативные руководящие указания по использованию IPv6 с DNS подробно описаны в [b-IETF RFC 4472].

В) *Сценарий варианта 4 (варианты 5, 6, 7 и 9 аналогичны) – конфигурируемое туннелирование*

Если базовая транспортная сеть работает на протоколе IPv4, для перенаправления трафика IPv6 в целевую сеть доступа может использоваться конфигурируемый туннель.

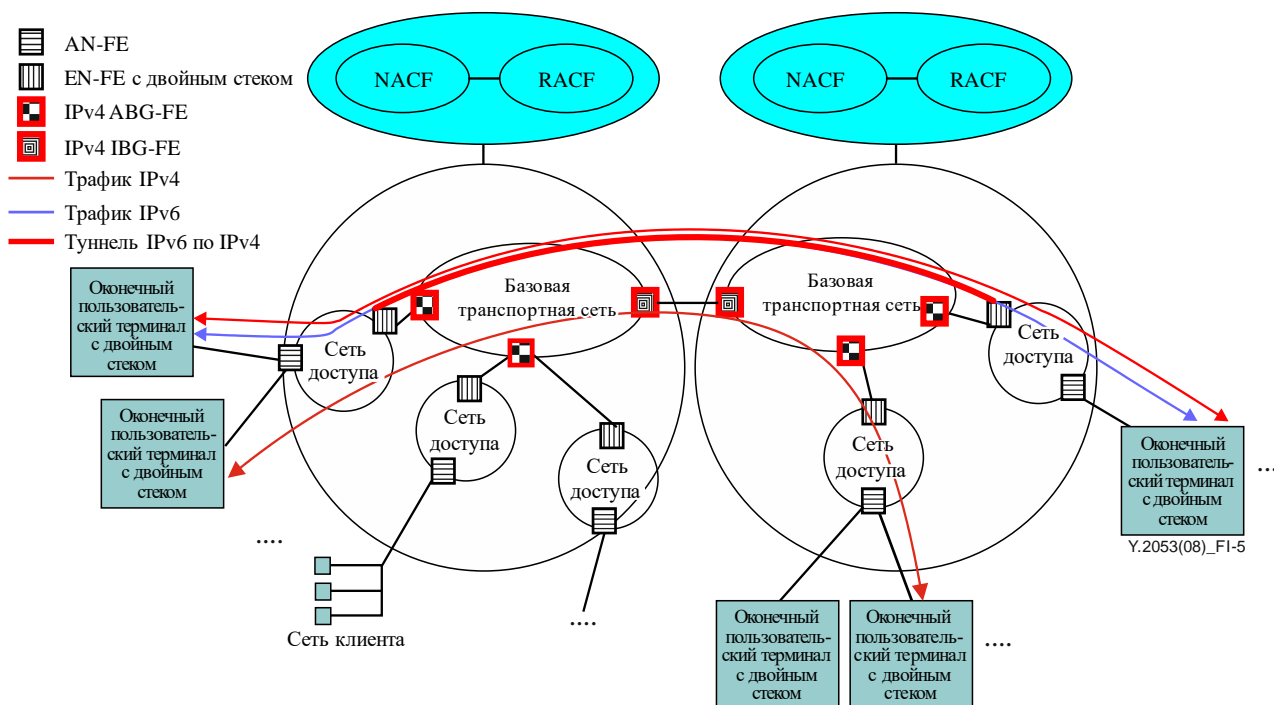


Рисунок I.5 – Сценарий "узел с двойным стеком – узел с двойным стеком" (базовая транспортная сеть IPv4)

С) *Сценарий варианта 4 (варианты 5, 6, 7 и 9 аналогичны) – двойной стек ↔ поддержка только IPv4*

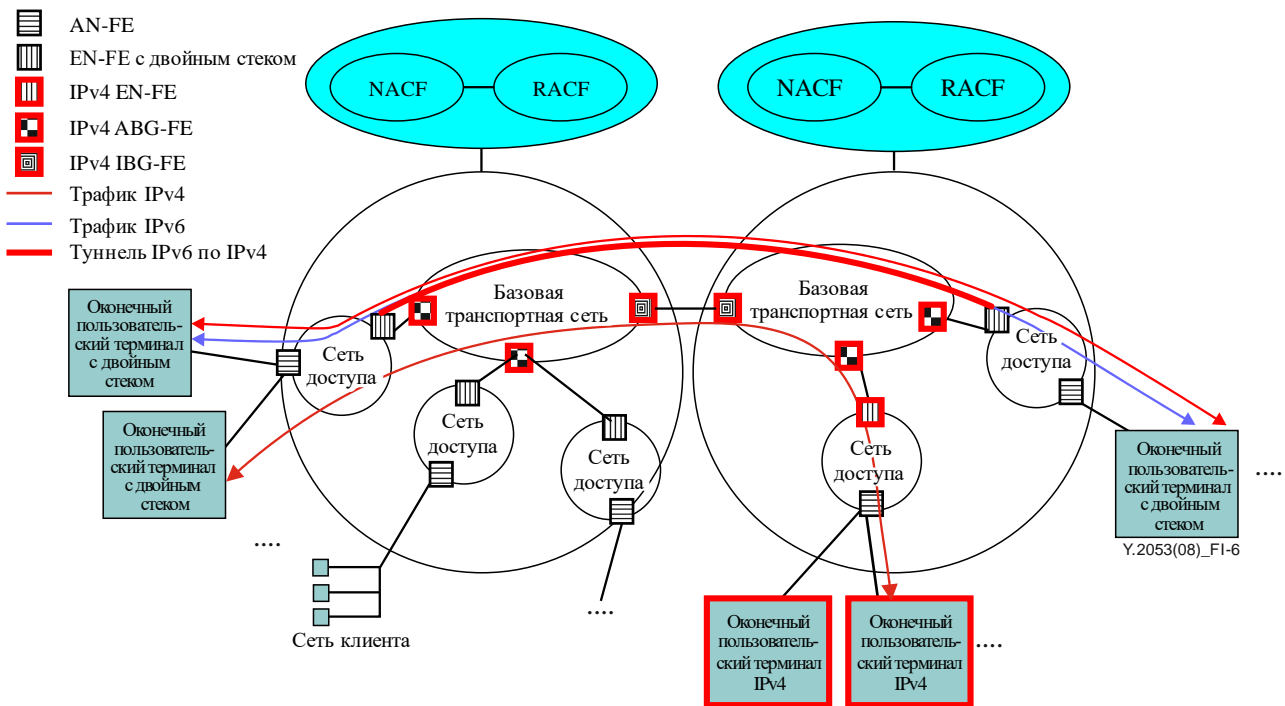


Рисунок I.6 – Узел с двойным стеклом – узел IPv4 (базовая транспортная сеть IPv4)

Еще одним примером может служить следующий вариант на основе С.

Д) *Сценарий варианта 4 (варианты 5, 6, 7 и 9 аналогичны) – двойной стек ↔ поддержка только IPv6*

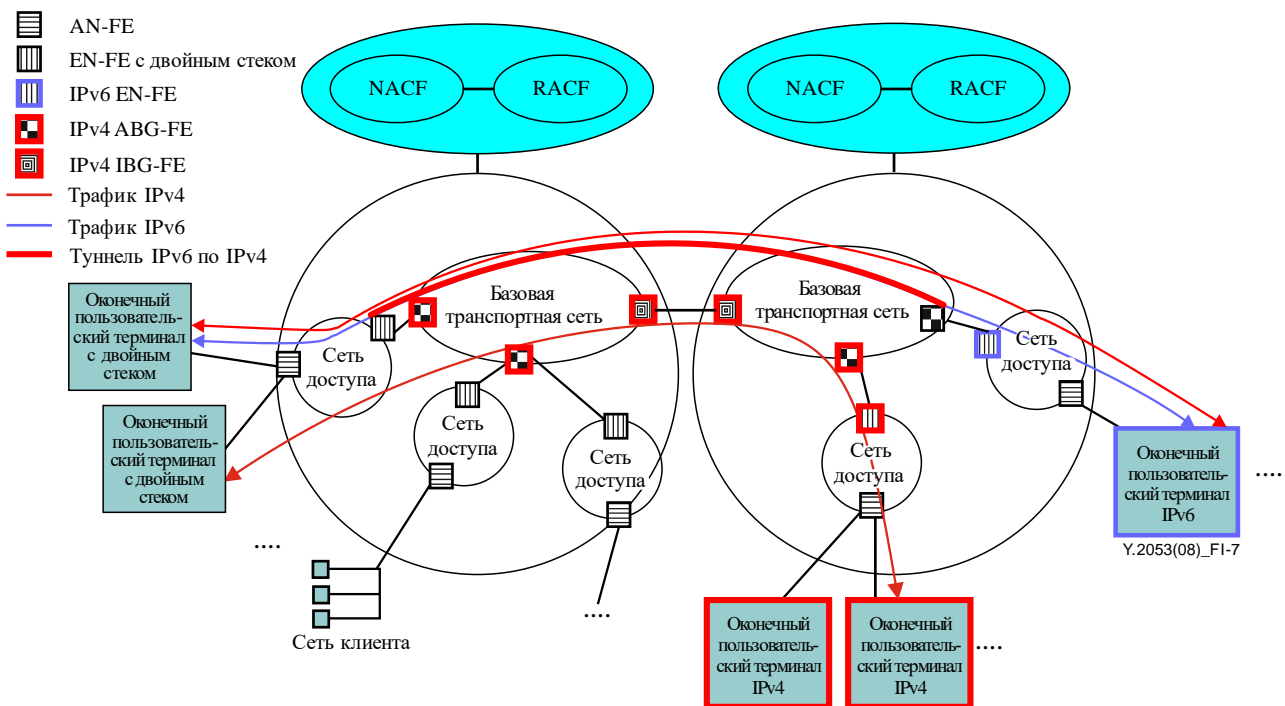


Рисунок I.7 – Узел с двойным стеклом – узел IPv6 (базовая транспортная сеть IPv4)

Еще одним примером может служить следующий вариант на основе С.

Е) Сценарий варианта 1 (варианты 2, 3 и 8 аналогичны) – NAT-PT

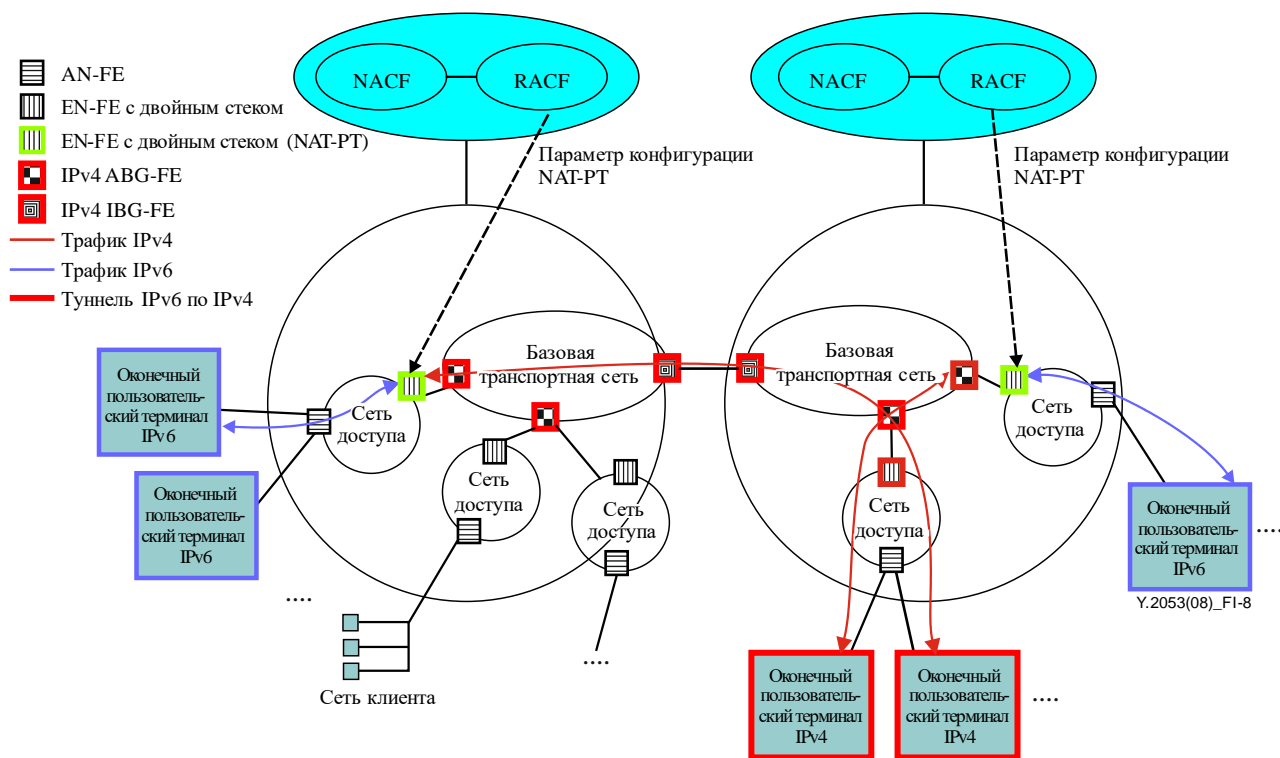


Рисунок I.8 – Узел IPv4 – узел IPv6 (базовая транспортная сеть IPv4)

Оконечный пользовательский терминал IPv6 может связываться с терминалом IPv4 через устройство NAT-PT. В этом примере NAT-PT устанавливается на объекте EN-FE. Кроме того, NAT-PT может устанавливаться на ABG-FE или IBG-FE. Устройство NAT-PT транслирует пакеты IPv6 в пакеты IPv4 и обратно.

Функция RACF управляет политикой трансляции и другими параметрами конфигурации NAT-PT. Функция RACF предоставляет эту информацию устройству NAT-PT по мере необходимости.

F) *Сценарий варианта 4 (варианты 5, 6, 7 и 9 аналогичны) – поддержка только IPv6 ↔ поддержка только IPv4*

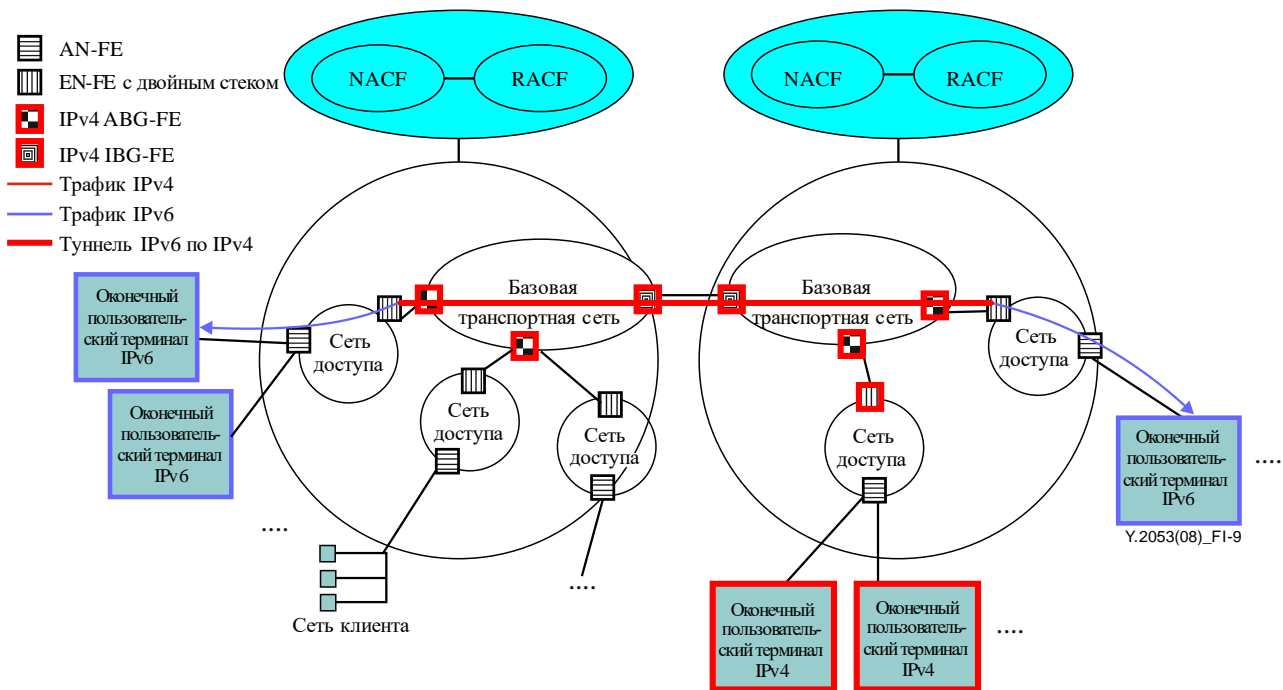


Рисунок I.9 – Узел IPv6 – узел IPv6 (базовая транспортная сеть IPv4)

Этот вариант аналогичен В. Для передачи данных по базовой транспортной сети IPv4 в этом варианте используется конфигурируемый туннель.

Библиография

- [b-ITU-T Y.1540] Recommendation ITU-T Y.1540 (2007), *Internet protocol data communication service – IP packet transfer and availability performance parameters*.
- [b-IETF RFC 2765] IETF RFC 2765 (2000), *Stateless IP/ICMP Translation Algorithm (SIIT)*, (Standards Track).
<<http://www.ietf.org/rfc/rfc2765.txt?number=2765>>
- [b-IETF RFC 2766] IETF RFC 2766 (2000), *Network Address Translation – Protocol Translation (NAT-PT)*, (Standards Track).
<<http://www.ietf.org/rfc/rfc2766.txt?number=2766>>
- [b-IETF RFC 4213] IETF RFC 4213 (2005), *Basic Transition Mechanisms for IPv6 Hosts and Routers*, (Standards Track).
<<http://www.ietf.org/rfc/rfc4213.txt?number=4213>>
- [b-IETF RFC 4472] IETF RFC 4472 (2006), *Operational Considerations and Issues with IPv6 DNS*.
<<http://www.ietf.org/rfc/rfc4472.txt?number=4472>>
- [b-IETF draft-03] IETF draft-03, *IPv6 Tunnel Broker with the Tunnel Setup Protocol (TSP)*.
<<http://tool.ietf.org/html/draft-blanchet-v6ops-tunnelbroker-tsp-03>>

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
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