ГОСУДАРСТВЕННЫЙ СТАНДАРТ РЕСПУБЛИКИ БЕЛАРУСЬ

СТБ ETSI TS 102 361-3/ОР

Электромагнитная совместимость и спектр радиочастот (ERM)

СИСТЕМЫ ЦИФРОВОВОЙ ПОДВИЖНОЙ РАДИОСВЯЗИ (DMR)

Часть 3 DMR протокол передачи данных

Электрамагнітная сумяшчальнасць і спектр радыёчастот (ERM)

СІСТЭМЫ ЛІЧБАВАЙ РУХОМАЙ РАДЫЁСУВЯЗІ (DMR)

Частка 3 DMR пратакол перадачы дадзеных

(ETSI TS 102 361-3: 2013, IDT)

Настоящий проект стандарта не подлежит применению до его утверждения

Госстандарт
Минск

УДК МКС 33.070.01 КП 02 IDT

Ключевые слова: совместимость, радиооборудование, цифровые радиосистемы, профессиональная подвижная радиосвязь, полоса частот, радиоканалы, передача голоса, передача данных, взаимодействие

Предисловие

Цели, основные принципы, положения по государственному регулированию и управлению в области технического нормирования и стандартизации установлены Законом Республики Беларусь от 05.01.2004 №262-З «О техническом нормировании и стандартизации».

1 ПОДГОТОВЛЕН открытым акционерным обществом «Гипросвязь» (ОАО «Гипросвязь»)
ВНЕСЕН Министерством связи и информатизации Республики Беларусь

2 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ постановлением Госстандарта Республики Беларусь от …….. №

3 Настоящий стандарт идентичен Европейской спецификации ETSI TS 102 361-3: 2013 Electromagnetic compatibility and Radio spectrum Matters (ERM); Digital Mobile Radio (DMR) Systems; Part 3: DMR data protocol (Электромагнитная совместимость и спектр радиочастот (ERM). Системы цифровой подвижной радиосвязи (DMR). Часть 3. DMR протокол передачи данных.).

Европейские спецификации разработаны ETSI – European Telecommunications Standards Institute (Европейский институт по стандартизации в области электросвязи).

Перевод с английского языка (en).

Сведения о соответствии государственного стандарта ссылочному европейскому стандарту приведены в дополнительном приложении Д.А.

Степень соответствия – идентичный (IDT).

4 ВВЕДЕН ВПЕРВЫЕ

Издан на русском языке

Содержание

Введение

Настоящий стандарт является частью 3 из группы стандартов, устанавливающих технические требования для радиооборудования, работающего по протоколу DMR:

Часть 1: "DMR протокол радиоинтерфейса";

Часть 2: "Речевые и общие услуги и функциональные возможности DMR";

Часть 3: "DMR протокол передачи данных";

Часть 4: "Транкинговый DMR протокол".

ГОСУДАРСТВЕННЫЙ СТАНДАРТ РЕСПУБЛИКИ БЕЛАРУСЬ

Электромагнитная совместимость и спектр радиочастот (ERM)
Системы цифровой подвижной радиосвязи (DMR)
Часть 3. DMR протокол передачи данных

Электрамагнітная сумяшчальнасць і спектр радыёчастот (ERM)
Сістэмы лічбавага рухомага радыё (DMR)
Частка 3 DMR пратакол перадачы дадзеных

Electromagnetic compatibility and Radio spectrum Matters (ERM);
Digital Mobile Radio (DMR) Systems;
Part 3: DMR data protocol

Дата введения 2017- -

1 Область применения

Настоящий стандарт устанавливает технические требования для систем цифровой мобильной радиосвязи (DMR), работающих в существующих лицензированных полосах частот сухопутной подвижной службы, как определено в CEPT ERC T/R 25-08 [3].

В настоящем стандарте описывается протокол пакетной передачи данных (PDP) масштабируемой системы цифровой мобильной радиосвязи, которая охватывает три уровня возможных продуктов:

- Уровень I: DMR оборудование, имеющее встроенную антенну и работающее в прямом режиме (без связи с инфраструктурой) в рамках общего разрешения, без работы по каким-либо индивидуальным разрешениям;

- Уровень II: DMR системы, работающие по индивидуальным лицензиям в прямом режиме или с использованием базовой станции (BS) для ретрансляции.

- Уровень III: транкинговые DMR системы, работающие по индивидуальным лицензиям, с функцией контроллера, который автоматически регулирует процесс связи.

Примечание 1 – Оборудование Уровня II и Уровня III включает в себя как циркулярные, так и нециркулярные системы.

Примечание 2 – три уровня оборудования могут работать только независимо и не могут взаимодействовать.

Настоящий стандарт описывает протокол пакетной передачи данных (PDP) для DMR, который был специально разработан с целью быть подходящим для продуктов всех указанных уровней. Протокол DMR применяется в полосах частот сухопутной подвижной службы, и физические параметры оборудования: канальный и дуплексный разнос, допустимые диапазоны, параметры спектра остаются без изменений.

2 Ссылки

2.1 Нормативные ссылки

Ссылки являются либо определенными (определяемыми датой опубликования и/или номером редакции или версии), либо неопределенными. В случае определенных ссылок применяется только размещенная на Веб сайте версия. В случае неопределенных ссылок применяется последняя версия ссылочного документа (включая поправки).

Ссылочные документы, не имеющиеся в свободном доступе в указанном местоположении, могут быть найдены по адресу: http://docbox.etsi.org/Reference.

Примечание – Гиперссылки, входящие в состав настоящего стандарта, были действительны на момент его публикации, ETSI не может гарантировать их долгосрочное действие.

Следующие ссылочные документы необходимы для применения настоящего стандарта:

[1] ETSI TS 102 361-1 Электромагнитная совместимость и спектр радиочастот (ERM). Системы цифрового мобильного радио (DMR). Часть 1. DMR протокол радиоинтерфейса (AI).

[2] ETSI TS 102 361-2 Электромагнитная совместимость и спектр радиочастот (ERM). Системы цифрового мобильного радио (DMR). Часть 2. DMR протокол передачи голоса и общие услуги и возможности.

[3] CEPT/ERC T/R 25-08 Критерии планирования и координации частот для сухопутной подвижной службы в диапазоне частот от 29,7 до 921 МГц.

[4] IETF RFC 791 "Internet Protocol; DARPA Internet Program; Protocol Specification" (Интернет-протокол).

[5] IETF RFC 792: "Internet Control Message Protocol; DARPA Internet Program; Protocol Specification" (Протокол межсетевых управляющих сообщений).

[6] IETF RFC 1918: "Address Allocation for Private Internets" (Распределение адресов для частных сетей Интернет).

[7] IETF RFC 826: "Ethernet Address Resolution Protocol: Or converting network protocol addresses to 48.bit Ethernet address for transmission on Ethernet hardware" (Протокол определения адреса Ethernet или преобразование адреса сетевого протокола в 48-ми битный адрес Ethernet для передачи оборудованием Ethernet.)

[8] IETF RFC 2460: "Internet Protocol, Version 6 (IPv6) Specification" (Интернет – протокол, спецификация версии 6 (IPv6).

[9] IETF RFC 2529: "Transmission of IPv6 over IPv4 Domains without Explicit Tunnels". (Передача IPv6 через Домены IPv4 без «Явных Туннелей»).

[10] IETF RFC 3056: "Connection of IPv6 Domains via IPv4 Clouds". (Подключение Доменов IPv6 через Облака IPv4).

[11] IETF RFC 3142: "An IPv6-to-IPv4 Transport Relay Translator". (Транспортный релейный Транслятор протокола IPv6 в IPv4).

[12] IETF RFC 4213: "Basic Transition Mechanisms for IPv6 Hosts and Routers".[Основные механизмы перехода для хостов и маршрутизаторов].

[13] ETSI TS 100 392-18-1: "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D) and Direct Mode Operation (DMO); Part 18: Air Interface optimized applications; Sub-part 1: Location Information Protocol (LIP)" (Наземное транкинговое радио (TETRA) Голос плюс данные (V+D) и режим прямой работы (DMO). Часть 18. Радиоинтерфейс оптимизированных приложений. Раздел 1. Протокол локальной информации (LIP).

[14] IETF RFC 768: "User Datagram Protocol" (Протокол дейтаграмм пользователя).

[15] IETF RFC 2781: "UTF-16, an encoding of ISO 10646". (UTF-16, кодировка из ISO 10646).

2.2 Информативные ссылки

Ссылки отсутствуют.

3 Определения и сокращения

3.1 Определения

В настоящем стандарте применяются следующие термины и определения

3.1.1 базовая станция (Base Station (BS))**:** Фиксированное оконечное оборудование, используемое для предоставления услуг DMR.

3.1.2 типовой сервис (bearer service)**:** Телекоммуникационная услуга предоставляющая возможность передачи информации между точками доступа.

3.1.3 пакет (burst)**:** Элементарное количество битов в физическом канале.

Примечания

1 Существует три различных пакета с различным числом битов. Информационный пакет состоит из 264 битов, пакет CACH состоит из 24 битов, а пакет RC состоит из 96 битов.

2 Пакет может содержать защитный интервал в начале и конце пакета, используемый для постепенного повышения/снижения мощности.

3 Более подробное определение пакета приведено в пункте 4.2.1.

3.1.4 вызов (call)**:** Завершенная последовательность связанных транзакций между MS.

Примечание – Транзакциями могут быть один или более пакетов, содержащих информацию, относящуюся к конкретному вызову.

3.1.5 плоскость управления (Control plane (C-plane))**:** Часть стека протокола DMR, выделенная для управления и услуг передачи данных.

3.1.6 конвенционная связь (conventional)**:** Режим не транкинговой связи.

Примечание – Это метод связи, при котором любая подвижная станция MS может осуществлять связь с одной или несколькими другими подвижными станциями (MSs) без использования протокола автоматического перераспределения каналов связи, и может работать либо в прямом режиме, либо через использование какого-либо дополнительного оборудования (например, BS).

3.1.7 цифровая подвижная радиосвязь (Digital Mobile Radio (DMR))**:** Группа физических объектов, которая содержит все подвижное и/или фиксированное конечное оборудование, которое используется для получения услуг DMR

3.1.8 прямой режим (direct mode)**:** Режим работы, при котором MS могут поддерживать связь вне управления сети.

Примечания
1 Режим является технологией связи, в которой любое устройство радиосвязи (MS) может поддерживать связь с одним или несколькими другими устройствами радиосвязи (BS) без необходимости в каком-либо дополнительном оборудовании (например, BS).
2 Режим поддерживает один сеанс радиосвязи на полосу радиочастот 12,5 кГц; полоса 12,5 кГц эквивалентна спектральной эффективности (12,5e).

3.1.9 дуплексный режим (duplex)**:** Режим работы, посредством которого информация может передаваться в обоих направлениях, при этом оба направления независимы.

Примечание – Для обозначения дуплексного режима также применяется термин «полный дуплекс».

3.1.10 фрейм (frame)**:** два последовательных временных слота, обозначенных как слот 1 и слот 2.

Примечание – Кадр имеет длину 60 мс.

3.1.11 логический канал (logical channel)**:** Отдельный канал передачи данных между логическими конечными точками.

Примечание – Логические каналы обозначены как 1 и 2. Логический канал может состоять из подканалов, например SYNC, встроенная сигнализация и т.д.

3.1.12 подвижная станция (Mobile Station (MS))**:** Группа физических объектов, которая содержит все подвижное оборудование, используемое для получения услуг DMR.

3.1.13 полезная нагрузка (payload)**:** Биты информационного поля.

3.1.14 физический канал (physical channel)**:** Радиочастотная несущая, которая модулируется информационными битами пакетов.

Примечание – Радиочастотная несущая является как одночастотной, так и дуплексной парой частот. Физический канал подсистемы DMR требуется для поддержки логических каналов.

3.1.15 блок данных протокола (Protocol Data Unit (PDU))**:** Информационный блок, состоящий из управляющей информации (сигнализации) и пользовательских данных, которыми обмениваются объекты одного уровня.

3.1.16 радиочастотный канал (Radio Frequency channel)**:** Радиочастотная несущая (RF несущая).

Примечание – Определенная часть РЧ спектра. В системе DMR разнос РЧ несущих составляет 12,5 кГЦ. Физический канал может быть, как одночастотным, так и дуплексной парой частот

3.1.17 режим репитера (repeater mode)**:** Режим работы, при котором MS могут поддерживать связь через BS.

Примечание – Технология связи, в которой любая радиостанция (MS) может связываться с одним или несколькими радиостанциями с (MS) с задействованием промежуточной BS.

3.1.18 процедура сохранения и подтверждения переданных данных (sliding window)**:** Процедура управления потоком передаваемых данных, подтвержденных на канальном уровне DLL, которая требует от получателя сохранять пакеты данных и обеспечивать отправление подтвержденного ответа на все сохраненные данные по запросу от источника.

3.1.19 процедура ответа подтверждающего передачу данных (stop and wait)**:** Процедура управления потоком передаваемых данных, подтвержденных на канальном уровне DLL которая требует от получателя отправлять ответ о подтверждении после получения каждого пакета данных.

3.1.20 суперфпейм (superframe)**:** 6 последовательных пакетов трафика в логическом канале обозначенных от «A» до «F».

Примечание – Суперкадр имеет длину 360 мс и используется только для речевого трафика.

3.1.21 временной слот (слот) (time slot (or slot))**:** Элементарный временной интервал в физическом канале.

Примечание – Временной слот имеет длину 30 мс и может быть пронумерован как «1» либо «2».

3.1.22 передача (transmission)**:** Период передачи пакетов, содержащих информацию или сигнализацию.

Примечание – Передача может быть непрерывной, то есть передача множества пакетов без линейного нарастания и снижения мощности, либо прерывистой, то есть передача каждого пакета с периодом линейного нарастания и снижения мощности.

3.1.23 транкинг (trunking)**:** Радиосвязь, управляемая сетью.

Примечание – Технология связи, при которой любая радиостанция (MS) может поддерживать связь с одной или несколькими другими радиостанциями (MS), с применением протокола транкинговой связи, при этом все MS будут находится под управлением сети.

3.1.24 плоскость пользователя (User plane (U-plane))**:** Часть стека протоколов DMR, предназначенная для речевых услуг пользователя.

3.2 Сокращения

В настоящем стандарте применяются следующие сокращения:

AB – Appended Block – добавленный блок;
ACK – (positive) ACKnowledgement – подтверждение получения;
AI – Air Interface – радиоинтерфейс;
ARP – Address Resolution Protocol – протокол разрешения адресов;
AT – Access Type – тип доступа;
BMP – Basic Multilingual Plane – базовая многоязычная плоскость;
BS – Base Station – базовая станция;

Примечание – Обозначает стационарное оконечное устройство.

CACH – Common Announcement Channel – общий канал передачи уведомлений;
CCL – Call Control Layer – уровень управления вызовами;
CRC – Cyclic Redundancy Checksum for data error detection – циклическая избыточная контрольная сумма для обнаружения ошибок в данных;
C-plane – Control plane – плоскость управления;
DAID – Destination (IP) Address Identifier – идентификатор IP адреса назначения;
DD – Defined Data – определенные данные;
DLL – Data Link Layer – канальный уровень;
DMR – Digital Mobile Radio – цифровое мобильное радио;
DNF – Do Not Fragment – не фрагментировать;
DPF – Data Packet Format – формат пакета данных;
DPID (UDP) – Destination Port Identifier – идентификатор порта назначения;
ERC – European Radiocommunication Committee – Европейский Комитет по радиосвязи;
FEC – Forward Error Correction – предварительная коррекция ошибок;
FID – Feature set ID – идентификатор (ID) набора функций;
FLCO – Full Link Control Opcode – код операции управления соединением;
FMF – Full Message Flag – флаг сообщения;
FULL LC – Full Link Control – управление соединением;
HMSC – High level Message Sequence Chart – диаграмма последовательности сообщения высокого уровня;
ICMP – Internet Control Message Protocol – интернет-протокол управления сообщением;
ID – Identifier – идентификатор;
IHL – Internet Header Length – длина заголовка IP-пакета;
IP – Internet Protocol – интернет-протокол;
IPv4 – Internet Protocol version 4 – интернет-протокол 4-й версии;
IPv6 – Internet Protocol version 6 – интернет-протокол 6-й версии;
IT – Impolite Type – тип связи без использования протокола LBT;
LAN – Local Area Network – локальная сеть;
LC – Link Control – управление соединением;
LLC – Link Layer Control – управление логическим каналом;
LLID – Logical Link ID – ID логического соединения;
LSB – Least Significant Bit – младший бит;
MAC – Medium Access Control – управление доступом к среде передачи;
MFID – Manufacturer's FID – идентификатор набора функций изготовителя;
MS – Mobile Station – подвижная станция;

Примечание – Ссылка обозначает возимую или портативную (носимую) радиостанцию.

MSB – Most Significant Bit – старший бит;
MSC – Message Sequence Chart – диаграмма последовательности сообщения;
MTU – Maximum Transfer Unit – максимальный передаваемый блок;
NA – Not Applicable – не применяется;
NACK – Negative ACKnowledgement – подтверждение не получения;
NAT – Network Address Translator – трансляция сетевых адресов;
PDP – Packet Data Protocol – протокол пакетной передачи данных;

PDU – Protocol Data Unit – блок данных протокола;
PF – Protect Flag – флаг защиты;
PL – Physical Layer [физический уровень;
RAN – Radio Area Network – радиосеть;
RF – Radio Frequency – радиочастота;
RFC – Request For Comments – запрос комментариев;
RX – Receive – прием;
RX_LB – Receive Last Block – прием последнего блока;
SACK – Selective ACKnowledgement – выборочное подтверждение;
SAID – Source (IP) Address Identifier – IP адрес идентификатора источника;
SAP – Service Access Point – точка доступа к услуге;

Примечание – В случае, если сеть предоставляет услугу.

SARQ – Selective Automatic Repeat request – выборочный повторяемый автоматический запрос;
SDL – Specification and Description Language – язык спецификаций и описаний;
SPID (UDP) – Source Port Identifier – идентификатор порта источника;
TCP – Transmission Control Protocol – протокол управления передачей;
TD – Terminator Data – признак конца передачи данных;
TDMA – Time Division Multiple Access – многостанционный доступ с временным разделением каналов;
TOS – Type Of Service – тип обслуживания;
TX – Transmit – передача;
UDP – User Datagram Protocol – протокол дейтаграммы пользователя;
USB – Universal Serial Bus – универсальная последовательная шина;
UTF-16BE – Unicode Transformation Format 16 bit Big-Endian – формат 16 – битного порядка обратного преобразования универсального кода;
U-plane – User plane – плоскость пользователя.

4 Общие положения

В настоящем стандарте описывается система цифрового подвижного радио (DMR) для продуктов Уровней I, II и III, которые используют технологию с временным разделением каналов (TDMA) с 2-х слотовым решением и шириной полосы FM несущей – 12,5 кГц (см. примечание 1).

Примечание – DMR система для продуктов уровня I использует непрерывное изменение передачи раннее упомянутой технологии.

В настоящем стандарте описывается уровень управления вызовами (CCL) по отношению к радиоинтерфейсу (AI) DMR для управления вызовами пакетной передачи данных. Радиооборудование (стационарное, возимое или носимое), которое соответствует настоящему стандарту, должно быть совместимо по радиоинтерфейсу с оборудованием других производителей. Радиооборудование, попадающее под действие настоящего стандарта, должно также соответствовать ETSI TS 102 361-1 [1].

Настоящий стандарт не дает спецификации или рабочие детали для реализуемых систем, которые включают, но не ограничивают транкинг, роуминг, управление сетью, вокодер, безопасность, передачу голоса и общие услуги и возможности, подсистемы интерфейсов и передачу данных между частными и общественными коммутируемыми телефонными сетями. В нем описываются только соответствующие требования доступа, совместимые с радиоинтерфейсом.

Примечание – DMR стандарт состоит из нескольких частей, на которые в настоящем стандарте будут сделаны ссылки, если это необходимо.

4.1 Архитектура протокола

Настоящий подраздел описывает модель, в которой различные функции и процессы определены и распределены по различным уровням в стеке протоколов DMR системы.

Множество протоколов DMR системы и всех других положений, касающихся описания и указания интерфейсов, не означает ограничение или запрещение любых реализаций.

Архитектура протокола DMR имеет общую слоистую структуру, которая описывается ссылками и спецификациями слоистой архитектуры связи OSI.

Система DMR определяет стандартные протоколы для следующей трехуровневой модели, как показано на рисунке 4.1.

Основным протоколом в стеке является физический уровень PL, который является уровнем 1.

Канальный уровень (DLL), который является уровнем 2, должен регулировать обмен между всеми пользователями.

На уровне DLL, стек протокола должен быть разделен вертикально на две части, плоскость пользователя (U-plane), для передачи информации без возможности адресации (например, голос), и плоскость управления (C-plane) для информации сигнализации, как управления, так и данных, с возможностью адресации, как показано на рисунке 4.1.

Примечание 1 – Необходимо иметь в виду различные требования к информации C-plane и U-plane. Информация C- plane нужна только при дискретном (или не непрерывном) физическом соединении по отношению к прошедшей информации, несмотря на необходимость непрерывного виртуального соединения для поддержки услуги. Это также может быть услуга вызова сигнализации или пакетного режима. Запрос подтверждения может или быть или не быть. Информация U-plane, с другой стороны, требует непрерывного физического соединения, для доступности, так, что задержка услуги может постоянно поддерживаться. Это можно также назвать как услуга в режиме с коммутацией каналов.

Примечание 2 - Уровень DLL, приведенный на рисунке 4.1, может быть дополнительно подразделен по протоколу радиоинтерфейса на функциональный подуровень «управление доступом к среде передачи» (MAC) и подуровень «управление соединением» (LLC), который часто реализуется в радиооборудовании и соответствующих протоколах радиоинтерфейсов, из-за специализированного характера из этих двух задач. Такое разделение не представлено в настоящем стандарте, и зависит от конкретной реализации. Особенностью дальнейшей реализации уровня 2 в плоскости управления является предложение MAC только для услуги.

Уровень управления вызовами (CCL), который является уровнем 3 лежит в C-плоскости и отвечает за управление вызовом (адресации, функции и т.д.), предоставляет услуги, поддерживаемые DMR, а также поддерживает услугу передачи коротких сообщений и пакетную передачу данных. U-plane на уровне 2 (DLL) поддерживает доступ к голосовым услугам, которые доступны в DMR. Уровень управления, для управления вызовом данных, предложенный в DMR, описан в настоящем стандарте. DMR протокол передачи голоса, основные услуги и функциональные возможности, предложенные в DMR, описаны в TS 102 361-2 [2].

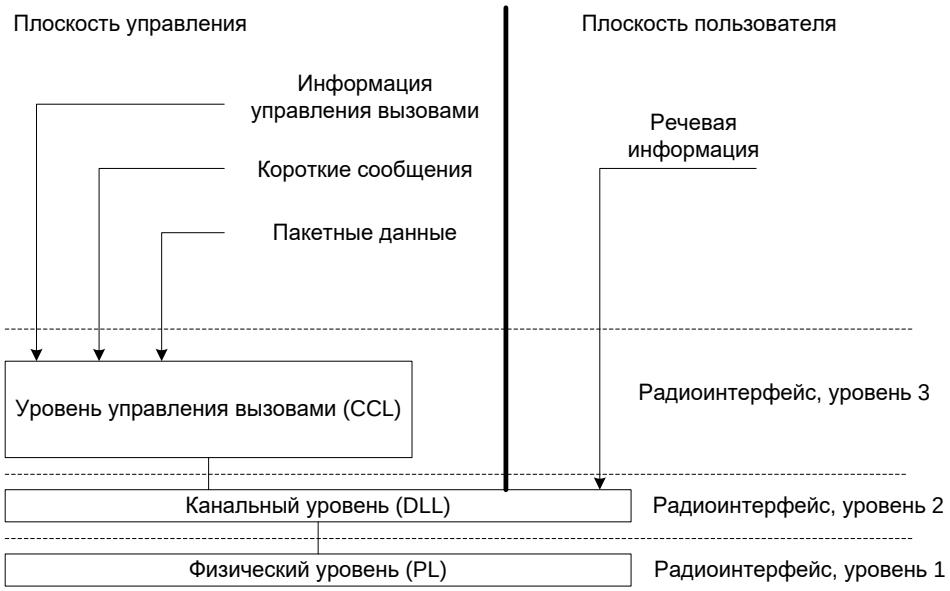

Рисунок 4.1 – Стек протокола системы DMR

4.1.1 Радиоинтерфейс физического уровня (уровень 1)

Радиоинтерфейс уровня 1 является физическим интерфейсом. На этом уровне сформированный физический кадр (блок), состоящий из битов, должен быть отправлен и/или получен. Физический уровень описан в TS 102 361-1 [1].

На уровне 1 выполняются следующие функции:

- модуляция / демодуляция сигнала;
- переключение на передачу и прием;
- поддержание радиочастотных характеристик в требуемых пределах;
- определение битов и символов;
- синхронизация частоты и символов;
- создание пакетов.

4.1.2 Радиоинтерфейс канального уровня (уровень 2)

Радиоинтерфейс уровня 2 управляет логическими соединениями и должен скрывать физическую среду от верхних слоев (является промежуточным уровнем между PL и CCL). Канальный уровень описан в TS 102 361-1 [1].

Основными функциями являются:

- канальное кодирование FEC, CRC;

- перемежение, деперемежение и упорядочение битов;
- механизм подтверждения и повтора;
- управление доступом к среде и управление каналами;
- создание фреймов, суперфреймов и синхронизация;
- определение пакетов (блоков) и параметров;
- создание адреса (источника и/или узла назначения);
- интерфейс голосовых приложений (данные вокодера) с PL;
- передача данных между интерфейсами «абонент – сеть»;
- обмен служебной информацией и/или пользовательскими данными посредством CCL.

4.1.3 Радиоинтерфейс уровня управления вызовами (уровень 3)

Радиоинтерфейс уровня 3 применим только к C-плоскости, и функционально должен быть объектом для услуг и средств, поддерживаемых протоколом DMR на верхней части уровня 2. Функции уровня CCL для голоса, общих услуг и средств описаны в TS 102 361-2 [2] (пункт 5).

На уровне 3 выполняются следующие функции:

- активация / деактивация BS;
- установление, поддержание и завершение вызова;
- индивидуальный или групповой вызов передачи / приема;
- назначение адресации (DMR-идентификаторов или шлюза по мере необходимости);
- поддержка внутрисетевых услуг (передача служебной информации, приоритетное прерывание обслуживания, регистрация с задержкой и т.д.);
- контроль вызова передачи данных;
- сигнализация уведомлений.

4.2 Общие сведения о DMR-протоколе пакетной передачи данных (PDP)

Протокол передачи пакетных данных, описанный для DMR, связан с процедурой передачи пакетных данных, например, неподтвержденных данных, подтвержденных данных, подтвержденных данных с ответом и т.д.

Протокол пакетных данных для DMR содержит внутреннюю (встроенную) сигнализацию или процедуры, которые могут относиться к одной или более процедур передачи данных в пакетном режиме.

Все пользователи, связанные с сигнализацией или презентацией выше уровня 3 не являются частью настоящего стандарта и конкретной реализации.

Протокол пакетной передачи данных, описанный в настоящем стандарте, может быть использован для DMR продуктов и называется "протокол пакетной передачи данных по умолчанию".

В стандарте DMR существует возможность, которая позволяет производителям определять и реализовывать «частные» наборы функций, которые содержат дополнительную "частную" сигнализацию, которая может быть не понята продуктами, не поддерживающими этот "частный" набор функций.

Протокол передачи пакетных данных содержит следующие типы передачи данных на канальном уровне DLL:

- передача неподтвержденных данных;
- подтвержденные данные:
  - передача данных;
  - передача ответа.

Протокол передачи пакетных данных содержит следующие типы передачи данных соответствующие 3 уровню носителя услуг:

- интернет протокол;
- короткие данные:
  - необработанные данные;
  - статусные / предварительно кодированные данные;
  - определенные данные.

Передача данных 3 уровня построена на вершине передачи данных DLL.

Настоящий стандарт определяет DMR протокол пакетной передачи данных (PDP) для операции пакетной передачи данных. Данные сообщений произвольной длины передаются по DMR радиоинтерфейсу с использованием технологии пакетной передачи. На уровне 2 DMR протокол PDP с блоками данных протокола (PDUs) приведен в TS 102 361-1 [1] (пункт 8).

При описании протокола передачи пакетных данных используются SDL диаграммы, где это необходимо, чтобы проиллюстрировать и выделить специфические точки, как в прямом режиме, так и режиме через базовую станцию (BS). Другие аспекты радиосистемы DMR требуют HMSC и MSC диаграмм высокого уровня HL MS SDL и HL BS SDL.

Диаграммы и состояния для высокого уровня SDL приведены в TS 102 361-1 [1], (приложение G).

5 Интернет протокол (IP) передачи данных DMR

Настоящий стандарт поддерживает следующий протокол сетевого уровня:

- интернет-протокол 4-й версии (IPv4).

Примечание – Подробное описание протокола приведено в RFC 791 [4].

IPv4 обеспечивает, без установления соединения, лучшую доставку дейтаграммы между двумя точками доступа. Протокол IPv4 вызывается с помощью «хост-хост» протоколов (например, TCP, UDP) в интернет среде. Вызовы IPv4 осуществляются по радиоинтерфейсу, и IP-дейтаграмма передается по радио.

Услуга передачи DMR IP между двумя точками доступа построена на вершине канального уровня (DLL) (неподтвержденные данные и подтвержденные данные), и определена в подразделах 5.3 и 5.4 настоящего стандарта.

DMR PDP расширяет возможности DMR и действует как протокол IP подсети. Это позволяет прикладным программистам создавать свои приложения в стандартизированной среде. Реализация в BS IP-маршрутизатора и ретранслятора также удачное решение для подключения к внешним сетям, но выходит за рамки настоящего стандарта.

4.3 Особенности совместимости

Идентификатор вида данных (FID) идентифицирует один из нескольких разных видов данных и устанавливается только во втором заголовке данных.

Совместимость по радиоинтерфейсу при передаче пакетных данных, которые стандартизированы в настоящем стандарте, и имеются в оборудовании, обеспечивается только через один заголовок данных.

Передача пакетных данных, которые не стандартизированы в настоящем стандарте, обеспечивается только через опцию альтернативного производителя MFID во втором заголовке данных.

5.1 IP адресация

5.1.1 IP-адресация, извлекаемая из DLL

В настоящем пункте рассматриваются: значение IP адреса MS, адрес IP периферийного устройства способного подключаться к MS, и адрес группы, когда IP-адрес является производным от адреса DLL. Все адреса IPv4 (MSs, IP периферийных устройств, а также групп MSs) должны быть уникальными.

Уникальный адрес IPv4, получается из DLL-адреса MS, который определен в приложении A к TS 102 361-1 [1]. Использование производного IP-адреса упрощает конфигурацию MS. Это также устраняет необходимость в использовании протокола Address Resolution Protocol (ARP).

Если подсети соединяются с общественным интернетом, транслятор сетевых адресов (NAT) должен быть представлен в DMR объекте, когда происходит такое соединение.

Примечание – ARP (протокол разрешенных адресов) представляет собой протокол, используемый IPv4, чтобы сопоставить IP-адреса с адресами, используемыми в протоколе управления соединением при передаче данных. Термин "разрешенные адреса" относится к процессу поиска адресов.

Сеть радиосвязи может быть способна поддерживать несколько разных подсетей. Некоторые примеры приведены ниже.

Когда необходимо проверить соответствие между индивидуальным адресом MS DLL и IP-адресом MS (включая IP ее периферийного устройства) должны применяться следующие правила:

a) IP – адрес MS и ее периферийного устройства являются адресом «класса A» (рисунок 5.1);

b) Хостовый номер поля IP – адреса MS или ее периферии является 24-битным DLL адресом MS;

c) Поле «ID сети» IP-адреса MS является либо настроенным значением или значением по умолчанию;

d) Поле "ID сети" IP-адреса, IP периферийного устройства является полем "ID сети" MS + 1.

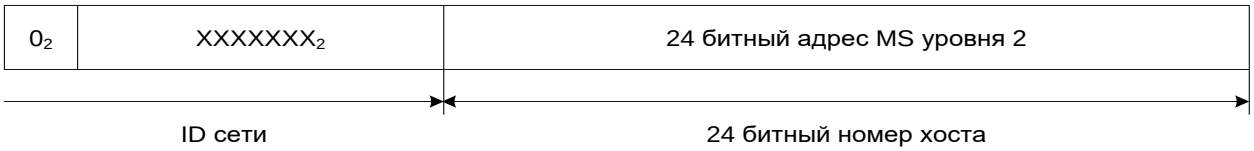

Рисунок 5.1 – Формат адреса класса A

IP-адрес группы должен быть адресом класса D, (рисунок 5.2). Соответствие между DLL адресом группы и IP-адресом группы должно следовать следующим правилам:

Когда необходимо проверить соответствие между DLL групповым адресом MS и IP групповым адресом MS должны применяться следующие правила:

a) групповой IP – адрес MS является адресом класса D, (рисунок 5.2);

b) наиболее значимые 8 бит IP-адреса группы (за исключением группы вещательных данных) являются конфигурацией адреса "класса D" с 4 значащими битами из набора для E_{16};

c) наименее значимые 24 бита IP-адреса группы для групповых данных являются одинаковыми с DLL адресом группы.

d) если поддерживается ограничение IP-вещания (т.е. мультикастинг), IP- адрес вещания (т.е. группы, содержащей все MSs) отображается как $FFFFFFFF_{16}$ по отношению к $FFFFFF_{16}$ в DLL;

Примечание – Адрес FFFFFFFF16 обозначает вещание по локальной сети через аппаратные средства и информация не должна быть направлена за пределы 3-го уровня маршрутизатора. Локальная сеть аппаратных средств является физическим соединением, к которой подключен хост для всех его ближайших соседей.

e) не должны использоваться адреса в диапазоне от 224.0.0.0 до 224.255.255.255.

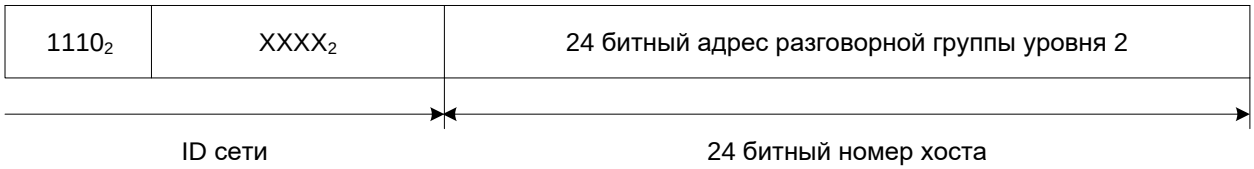

Рисунок 5.2 – Формат адреса класса D

5.1.1 IP-адресация, не связанная с DLL

В настоящем пункте рассматриваются присвоение значения IP-адреса MS и IP-адреса взаимосвязанных с ними периферийных устройств, для случаев, когда адрес DLL не связан с IP-адресом. Тем не менее возможно использование ARP таблицы с фиксированной связью между IP и DMR адресами и реализацией изготовителя слева. Все адреса IPv4 (MSs, IP периферийных устройств) должны быть уникальными. Если любая MS, или связанное с ней IP периферийное устройство, подключается к общему интернету, уникальные IP-адреса должны соответствовать адресам из рекомендации RFC 1918 [6]. Они перечислены ниже для справки.

10.0.0.0 – 10.255.255.255 (10/8 приставка).

172.16.0.0 – 172.31.255.255 (172.16/12 приставка).

192.168.0.0 – 192.168.255.255 (192.168/16 приставка).

Так как этот метод адресации не связывает адрес DLL с IP-адресом, ARP должна быть поддержана, чтобы обеспечить способ определения адреса DLL, когда известен только IP-адрес.

Протокол ARP приведен в RFC 826 [7], и реализует услугу передачи неподтвержденных данных, как это определено в пункте 5.3 настоящего стандарта.

Пакеты ARP запроса и ARP ответа имеют длину 22 байта, рисунок 5.3.

Заголовок данных для передачи по ARP должен использовать информационный элемент ARP SAP ID, как это определено в TS 102 361-1 [1] (пункт 9.3.18) и все единицы Idn адреса, как это определено в TS 102 361-1 [1] (приложение A)

Рисунок 5.3 – Формат ARP пакета

5.2 Сообщения об ошибках в IP

Чтобы сообщить об ошибке при обработке дейтаграммы, Интернет-протокол (IP) использует Internet Control Message Protocol (ICMP). Интернет-протокол IP не предназначен, чтобы обеспечить надежность. Целью протокола ICMP является извещение обратной стороны о проблемах в коммуникационной среде, а не сделать надежным протокол IP. Нет гарантий того, что дейтаграмма будет доставлена или сообщение-отчет будет возвращено. Некоторые дейтаграммы могут быть не доставлены без какого-либо отчета их утере. Протоколы более высокого уровня, которые используют IP, должны реализовать свои собственные процедуры надежности, если требуется надежная связь.

Примечание – Подробное описание в RFC 792 [5].

ICMP, как правило, сообщает об ошибках при обработке дейтаграмм. Для того, чтобы избежать бесконечного регресса сообщений о сообщениях и т.д., никакие сообщения ICMP не посылаются о сообщениях ICMP. Сообщения ICMP передаются с использованием базового заголовка IP. Как правило, он имеет длину 36 октетов.

В таблице 5.1 показан минимальный набор ICMP сообщения, который должен быть поддержан.

Таблица 5.1 – ICMP сообщения

Сообщение ICMP, наименование (тип)	Код	Комментарии
Не достигло места назначения	Сеть недоступна	Конечный пункт назначения IP сообщения, полученного от MS, не достигнут.
	Хост недоступен	1) отправитель исчерпал максимальное число повторных попыток на уровне радиоинтерфейса; или 2) полученное сообщение вызывает переполнение очереди сообщений получателя; или 3) время выдержки сообщения в очереди превысило установленный предел
	Необходима фрагментация и набор DNF	IP-сообщение, полученное от MS, превышает максимальную единицу передачи (MTU) для предназначенного (вспомогательного) интерфейса и дейтаграмма имеет не фрагментированный набор битов (DNF) в IP заголовке.
	Сеть назначения неизвестна	IP-сообщение, полученное на MS, указывает назначение класса сети, которая не поддерживается системой
Проблема параметра	Испорчен заголовок IP пакета	IP- сообщение, полученное на MS, имеет неподходящее форматирование его IP заголовка и не соответствует формату IPv4.

5.3 Передача неподтвержденных данных DLL

Передача неподтвержденных данных DLL обеспечивает лучшие возможности доставки данных между индивидуальными пользователями, либо между пользователем и группой пользователей. Для этого может быть использован либо IP протокол, либо передача коротких сообщений между точками доступа.

Примечание – Этот пункт определяет конкретные процедуры передачи неподтвержденных данных DLL по IP-протоколу между точками доступа. Процедуры передачи коротких сообщений между точками доступа одни и те же что и передача данных по IP протоколу кроме случаев, когда имеются отличия в передаче коротких данных оговоренных в настоящем стандарте.

При передаче неподтвержденных данных IP должен использоваться протокол LBT (LBT по отношению к собственному Цветовому коду или LBT ко всем) в качестве механизма доступа к каналу, как это определено в TS 102 361-1 [1] (пункт 5.2.1). В режиме ретрансляции через BS передача данных должна предшествовать активации BS для линии связи вниз, как это определено в TS 102 361-2 [2], (пункт 5.1.1.1), когда базовая станция находится в состоянии ожидания, как это определено в TS 102 361-1 [1], (пункт G.2). Первый пакет при передаче неподтвержденных данных IP несет необходимую информацию о передаваемых данных, позволяющую сделать выбор индивидуальные / групповые или уведомления. Это должен быть завершенный пакет неподтвержденных данных с заголовком пакета (U_HEAD) PDU в котором указан тип данных. Информационный элемент ID SAP в U_HEAD PDU должен быть основан на IP-значении пакетных данных, как это определено в TS 102 361-1 [1] (пункт 9.3.18). Опционально, если необходим собственный заголовок, второй передаваемый заголовок (P_HEAD) PDU передается с помощью пакета заголовка типа данных (Data Header Data Type).

Блоки данных должны передаваться посредством процедур «Блок передачи Данных» и «Последний Блок передачи данных» PDUs для выбранной скорости кодирования FEC, как это определено в TS 102 361-1 [1], (пункт 8.2.2). Процедура «Тип Данных» блоков данных должна указывать скорость кодирования FEC. Во время передачи данных скорость кодирования FEC и, следовательно, «тип данных» всех блоков данных должны быть одинаковыми.

5.3.1 Типы и PDU неподтвержденных IP данных

5.3.1.1 Типы и PDU неподтвержденных IP данных для скорости кодирования 1/2

Передача IP неподтвержденных данных для скорости кодирования 1/2 для прямого режима и режима ретранслятора требует наличия двух типов данных и трех блоков PDU. Они перечислены в таблице 5.2. Если поддерживается собственный заголовок, требуется четвертый блок PDU.

Таблица 5.2 – Типы неподтвержденных IP данных в PDUs

Тип данных	Значение	Назначение	PDU	DPF
Заголовок данных	0110_2	Адресация	U_HEAD	0010_2
		Собственный заголовок	P_HEAD	1111_2
Передаваемые данные со скоростью кодирования 1/2	0111_2	Блок данных	R_1_2_DATA	NA
		Последний блок данных	R_1_2_LDATA	NA

5.3.1.2 Типы и PDUs неподтвержденных IP данных для скорости кодирования 3/4

Передача IP неподтвержденных данных для скорости кодирования 3/4 для прямого режима и режима ретранслятора требует наличия двух типов данных и трех блоков PDU. Они перечислены в таблице 5.3. Если поддерживается собственный заголовок, требуется четвертый блок PDU.

Примечание – Заголовки для скорости кодирования ¾ неподтвержденных IP данных кодируются также как и для скорости кодирования 1/2.

Таблица 5.3 – Типы неподтвержденных IP данных в PDUs

Тип данных	Значение	Назначение	PDU	DPF
Заголовок данных	0110_2	Адресация	U_HEAD	0010_2
		Собственный заголовок	P_HEAD	1111_2
Передаваемые данные со скоростью кодирования 3/4	1000_2	Блок данных	R_3_4_DATA	NA
		Последний блок данных	R_3_4_LDATA	NA

5.3.1.3 Типы и PDUs неподтвержденных IP данных со скоростью кодирования 1

Передача неподтвержденных IP данных со скоростью кодирования 1 для прямого режима и режима ретранслятора требует наличия двух типов данных и трех PDU. Они перечислены в таблице 5.4. Если поддерживается собственный заголовок, требуется четвертый PDU.

Примечание – Заголовки для скорости кодирования 1 неподтвержденных IP данных кодируются также как и для скорости кодирования 1/2.

Таблица 5.4 – Типы и PDUs неподтвержденных IP данных со скоростью кодирования 1

Тип данных	Значение	Назначение	PDU	DPF
Заголовок данных	0110_2	Адресация	U_HEAD	0010_2
		Собственный заголовок	P_HEAD	1111_2
Передаваемые данные со скоростью кодирования 1	1010_2	Блок данных	R_1_DATA	NA
		Последний блок данных	R_1_LDATA	NA

5.3.2 SDL неподтвержденных IP данных

Процедуры доступа к каналу построены на процедурах, определенных в TS 102 361-1 [1] (пункт 5). Конкретные правила доступа к каналу для передачи неподтвержденных данных проиллюстрированы посредством SDL на рисунке 5.4. Они включает в себя добавление T_DataTxLmt и DLL повторного запуска процесса, когда канал занят.

Рисунок 5.4 иллюстрирует DLL уровень, когда он получает простую IP_Data от CCL (IP Layer). DLL запускает таймер T_DataTxLmt и таймер T_IdleSrch и переходит в состояние Qualify_Idle. T_DataTxLmt является таймером, который ограничивает количество времени, в течение которого DLL, будет пытаться передавать данные.

В состоянии Qualify_Idle DLL пытается определить состояние канала. Если канал свободен DLL будет передавать данные. Если истекает T_IdleSrch, а канал занят, DLL вызывает T_Holdoff и переходит в состояние Holdoff.

T_Holdoff случайный таймер используется для уменьшения коллизий, когда канал становится неактивным. Когда T_Holdoff заканчивается DLL запускает T_IdleSrch и повторяет процесс оценки состояния канала.

Когда DLL находится в состояниях либо Qualify_Idle либо в Holdoff и закончилось T_DataTxLmt, то процесс передачи данных должен прерваться. Как показано на рисунке 5.4, DLL отправляет простую ICMP на CCL указывающую, что время задержки сообщения было превышено, и хост был недостижим.

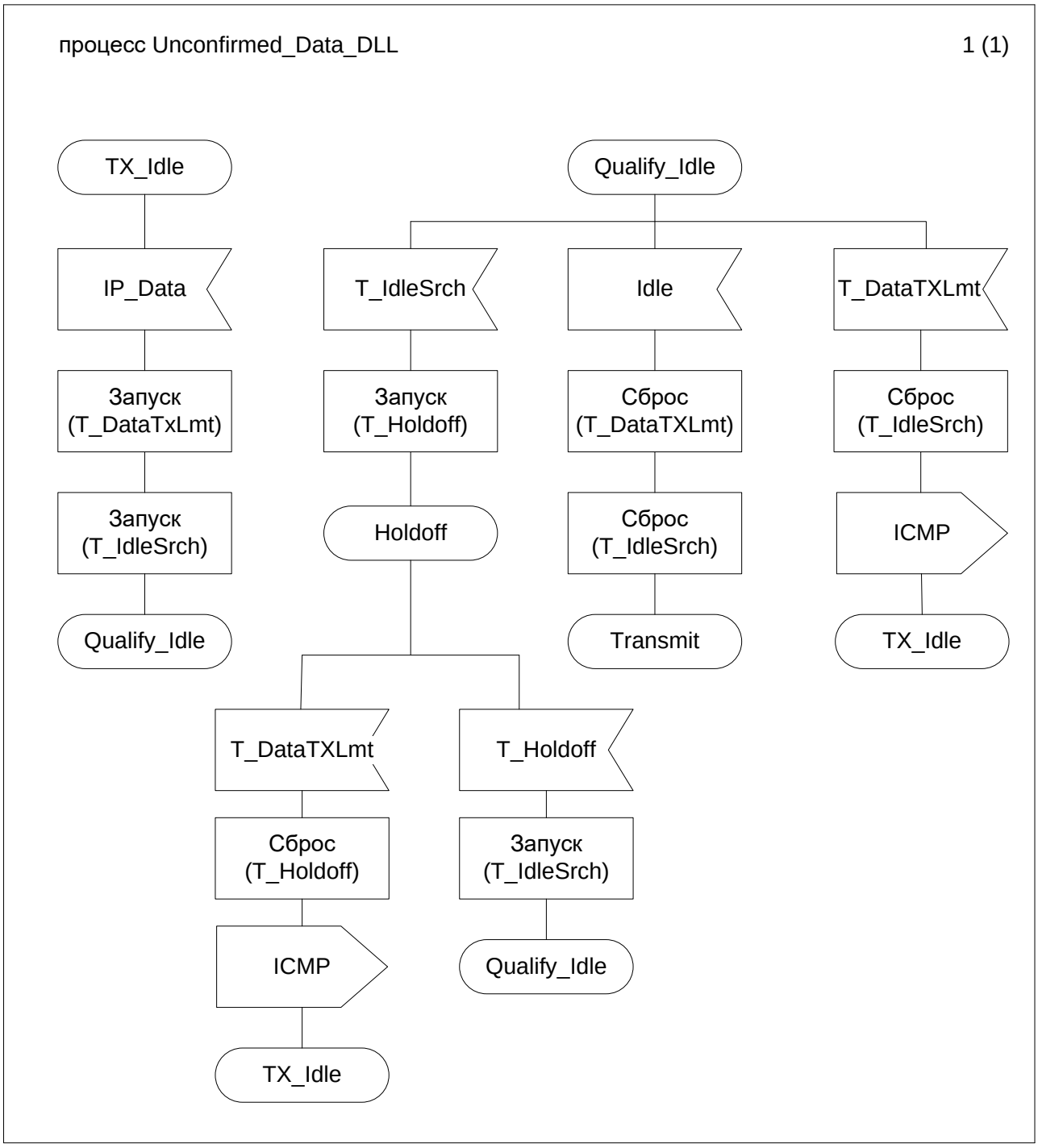

Рисунок 5.4 – SDL доступа к каналу при передаче неподтвержденных IP данных

5.3.3 MSCs неподтвержденных IP данных

Для разъяснения SDL неподтвержденных IP данных в пункте 5.3.2 используются следующие MSCs

5.3.3.1 MSCs передача неподтвержденных IP данных

Рисунок 5.5 иллюстрирует случай, когда DLL получает «IP_Data primitive», являющийся указанием доставки неподтвержденных данных от CCL. DLL запускает таймер T_DataTxLmt, а затем формирует и пытается отправить сообщение с данными, что иллюстрируется пунктом 5.3.3.2. Если время таймера T_DataTxLmt заканчивается, DLL посылает «ICMP primitive» на CCL, указывающий, что адресат недоступен и переходит в состояние PS_TX_Idle. Определения таймеров даны в пункте 5.3.2.

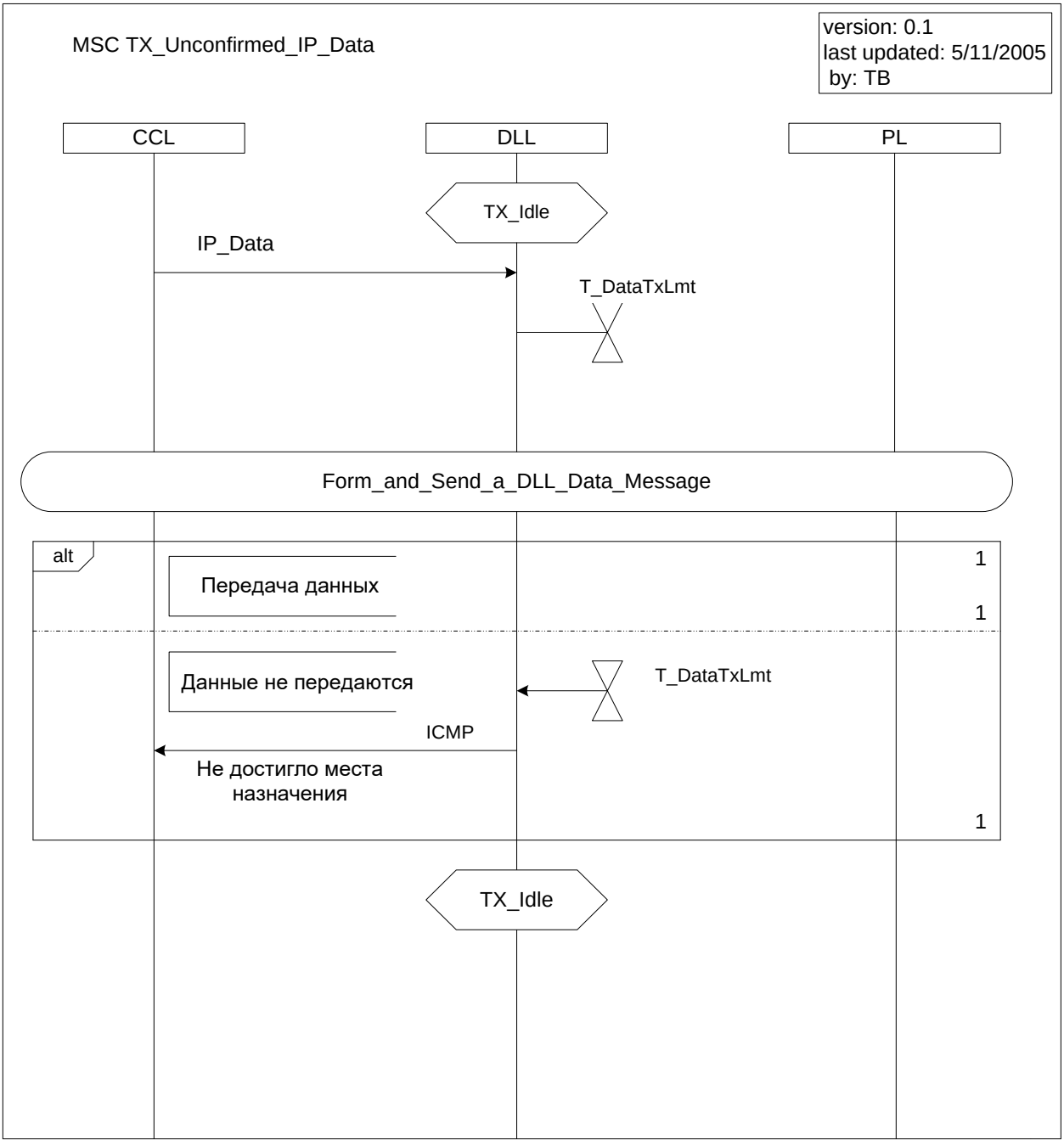

Рисунок 5.5 – MSC передача неподтвержденных IP данных

5.3.3.2 MSC формирования и отправления DLL сообщений данных

Рисунок 5.6 иллюстрирует действия MS DLL, когда она пытается передать сообщение с данными. После формирования PDU DLL запускает таймер T_IdleSrch и переходит к PS_Qualify_Idle для определения состояния канала. Если канал свободен MS сбрасывает T_DataTXLmt и передает данные. Если канал занят DLL запускает T_Holdoff. По истечении T_Holdoff DLL, перезапускает T_IdleSrch и переходит к PS_Qualify_Idle.

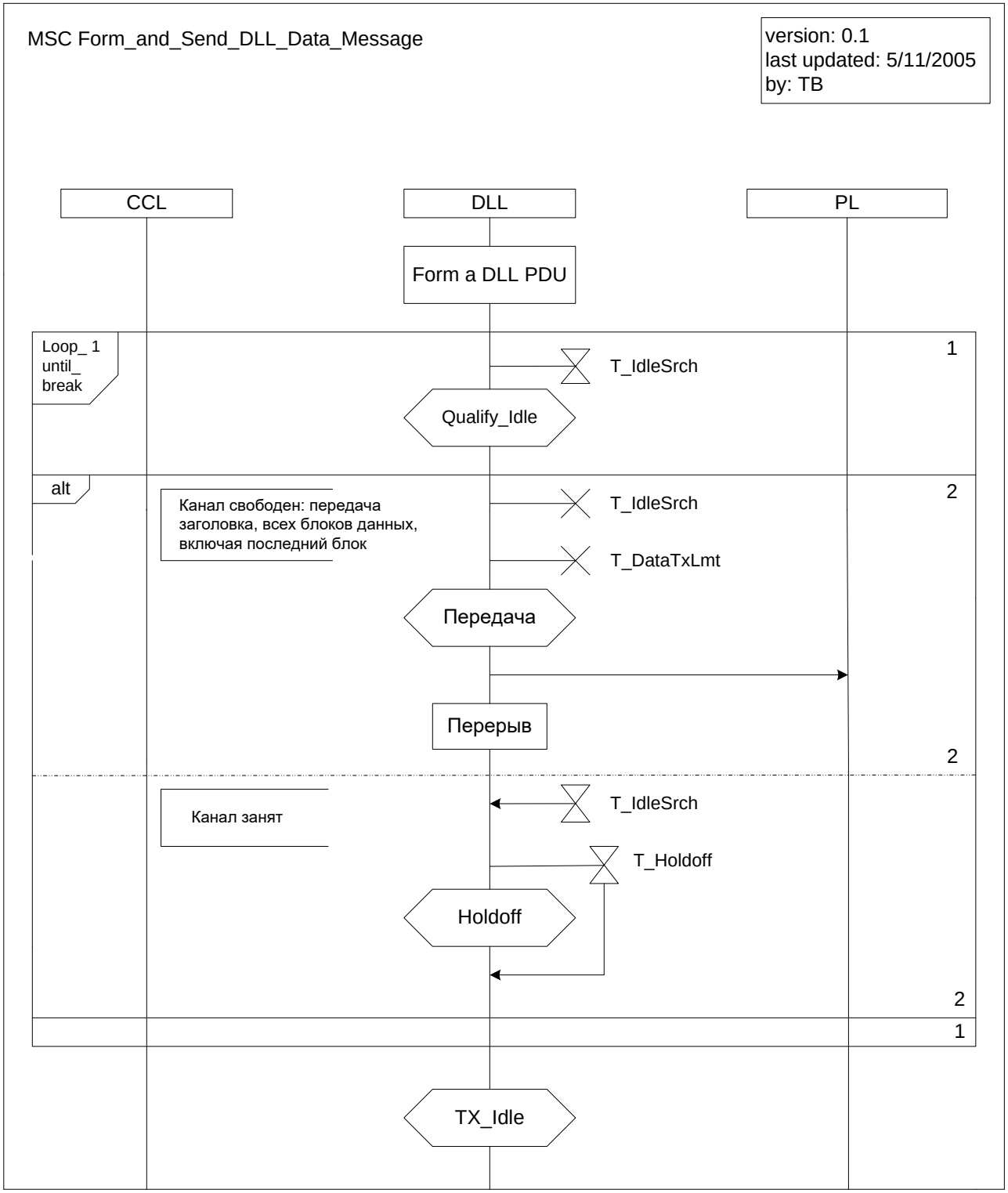

Рисунок 5.6 – MSC формирования и отправления DLL сообщений данных

5.3.3.3 Ретрансляция неподтвержденных данных

Рисунок 5.7 иллюстрирует действия BS, когда она получает заголовок неподтвержденных данных PDU (U_HEAD) на слот 1, в промежуток времени, когда она находится в состоянии «Channel_Hangtime». DLL посылает команду «Data_RX_Slot_1 primitive» на CCL_BS и также посылает команду «Data_RX primitive» на CCL_1. DLL прекращает генерировать пустые блоки PDUs, ретранслирует PDU заголовок неподтвержденных данных (U_HEAD), а затем ретранслирует все блоки неподтвержденных данных.

Во время ретрансляции данных BS должна установить бит «CACH AT» в состояние 1_2 (занято).

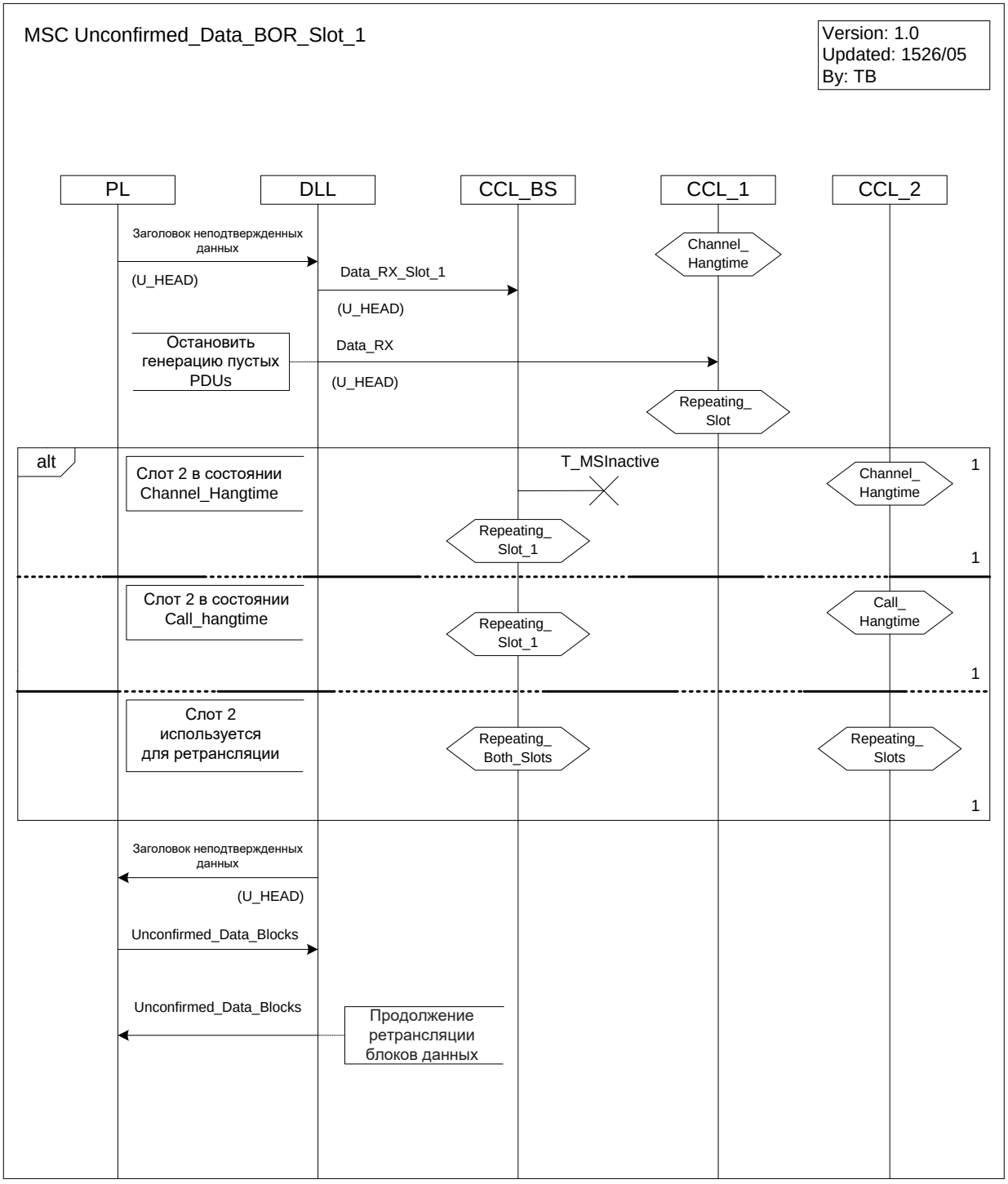

Рисунок 5.7 – MSC ретрансляции неподтвержденных данных

5.4 Передача подтвержденных данных DLL

Данная услуга обеспечивает возможность передачи подтвержденных данных между отдельным пользователем и другим отдельным пользователем или небольшой заранее определенной группой пользователей. Она может использовать IP протокол или протокол передачи коротких сообщений «bearer service».

Примечание - В данном пункте определены конкретные процедуры для передачи подтвержденных данных DLL по IP протоколу. Процедуры передачи коротких сообщений между точками доступа одни и те же, что и передача данных по IP протоколу кроме случаев, когда имеются отличия в передаче коротких данных оговоренных в настоящем стандарте.

Для контроля ошибок используется процесс обеспечения подтверждения «селективный автоматический запрос повторной передачи» (Selective Automatic Repeat reQuest) (SARQ). Передача IP подтвержденных данных посредством «bearer service» должна поддерживать процедуру «a stop and wait flow control» и может поддерживать процедуру «a sliding window flow control». Необязательная (дополнительная) процедура «sliding window» установлена в пункте 5.4.4 настоящего стандарта.

Подтвержденная передача IP данных должна использовать механизм доступа к каналу по протоколу LBT (Вежливый по отношению к собственному цветному коду или Вежливый ко всем) как определено в TS 102 361-1 [1] (пункт 5.2.1). В режиме ретрансляции через BS передача данных должна предшествовать активации BS для линии связи вниз, как это определено в TS 102 361-2 [2], (пункт 5.1.1.1), когда BS находится в состоянии «BS_Hibernating», как определено в TS 102 361-1 [1], (пункт G.2). Для получения подтверждения передачи данных, услуга передачи подтвержденных данных DMR использует процедуру контроля ошибок SARQ.

Первый пакет при передаче подтвержденных данных несет в себе информацию, позволяющую принимающей стороне быть уведомленной о передаче данных. Это достигается с помощью заголовка пакета подтвержденных данных (C_HEAD) PDU, использующего пакет «Data Header Data Type» (тип данных в заголовке данных). Информационный элемент ID SAP в U_HEAD PDU должен быть основан на значении IP данных пакета, как это определено в TS 102 361-1 [1] (пункт 9.3.18). Информационный элемент «Full Message Flag» (флаг полного сообщения) в C_HEAD PDU должен быть установлен 1_2 для индикации того, что идет передача полного сообщения, расцениваемая как передача от DLL. При работе с процедурой «stop and wait flow control», информационный элемент «Acknowledge» (A) (подтверждение) в C_HEAD PDU должен быть установлен 1_2, для индикации принимающей стороне, что подтвержденный ответ обязателен. Дополнительно, если необходим собственный (патентованный) заголовок, требуется второй заголовок (P_HEAD) PDU, который передается с использованием пакета «Data Header Data Type».

Сообщение подтвержденных данных состоит из нескольких блоков, где каждый блок имеет 7-битный серийный номер и 9-битный CRC. Все блоки отправляются во время первой передачи. Последний блок также содержит CRC сообщения для всего сообщения. Блоки данных должны быть переданы через PDU «Data Block» и «Last Data Block» с установленной скоростью кодирования FEC как определено в TS 102 361-1 [1] (пункт 8.2.2). Поле «Data Type» блоков данных должно отображать скорость кодирования FEC. Во время передачи данных скорость кодирования FEC, и, следовательно, значение поля «Data Type» всех блоков данных должны быть одинаковыми.

В прямом режиме, после того как передан PDU «Last Data Block», отправитель должен завершить передачу подтвержденных данных передачей «Terminator Data Link Control» (TD_LC) PDU, используя «терминатор» с пакетом «LC Data Type». В режиме ретрансляции отправитель не должен передавать что-либо после передачи PDU «Last Data Block». Однако BS может передать TD_LC PDU для установления зарезервированного времени ответа для принимающей стороны.

Во время приема передаваемых данных в режиме «stop and wait», принимающая сторона должна прислать ответ, который не подтверждается. В режиме ретрансляции MS должна отправить ответ, используя «невежливый» механизм доступа к каналу, как определено в TS 102 361-1 [1] (пункт 5.2.1). В прямом режиме MS должна отправить ответ, используя или «невежливый» или «вежливый» механизм доступа к каналу, как определено в TS 102 361-1 [1] (пункт 5.2.1).

MS должна отправить подтвержденный ответ «Confirmed Response» (C_RHEAD) в заголовке пакета, используя пакет «Data Header Data Type». Значение информационного элемента ID SAP в C_RHEAD PDU должно иметь то же самое значение, как и в C_HEAD PDU, когда собственный заголовок не используется. Опционально, если необходим «собственный» заголовок, то передается второй заголовок (P_HEAD) PDU с использованием пакета «Data Header Data Type». Если все принятые сообщения от отравителя прошли CRC проверки, тогда принимающая сторона завершает свой ответ после передачи заголовка(ов). Однако, если имеются ошибки во время CRC проверки для некоторых блоков, то принимающая сторона также должна отослать ответное сообщение содержащее список блоков чьи CRC не прошли проверку. Ответное сообщение использует блок «подтверждение ответа пакетных данных» C_RDATA PDU с типом данных «Rate 1/2 Coded Data».

В случае необходимости осуществления выборочной повторной передачи, отправитель снова передает блоки из принятого списка, перед которыми отправляется заголовок пакета подтвержденных

данных (C_HEAD) PDU. Информационный элемент «флаг полного сообщения» в C_HEAD PDU должен быть выставлен в значение 0_2 для индикации, что он транслирует часть сообщения, расцениваемое как передача по DLL. Этот процесс повторяется до тех пор, пока все блоки не будут приняты успешно, или число таких циклов не превысит максимального значения.

5.4.1 Типы/PDUs подтвержденных IP данных

5.4.1.1 Типы/PDUs подтвержденных IP данных для скорости кодирования 1/2

Передача IP подтвержденных данных для скорости кодирования 1/2 для прямого режима и режима ретранслятора требует наличия трех типов данных и четырех PDUs. Они перечислены в таблице 5.4. Если поддерживается собственный заголовок, требуется пятый PDU.

Таблица 5.4 – Типы/ PDUs подтвержденных IP данных для скорости кодирования 1/2

Тип данных	Значение	Назначение	PDU	DPF/FLCO
Заголовок данных	0110_2	Адресация	C_HEAD	0011_2
		Собственный заголовок	P_HEAD	1111_2
Передаваемые данные со скоростью кодирования 1/2	0111_2	Блок данных	R_1_2_DATA	NA
		Последний блок данных	R_1_2_LDATA	NA
Терминатор с LC	0010_2	Время задержки	TD_LC	110000_2

5.4.1.2 Типы/PDUs подтвержденных IP данных для скорости кодирования 3/4

Передача IP подтвержденных данных для скорости кодирования 3/4 для прямого режима и режима ретранслятора требует наличия трех типов данных и четырех PDUs. Они перечислены в таблице 5.5. Если поддерживается собственный заголовок, требуется пятый PDU.

Примечание – Заголовки для скорости кодирования 3/4 неподтвержденных IP данных кодируются также как и для скорости кодирования 1/2.

Таблица 5.5 – Типы/PDUs подтвержденных IP данных для скорости кодирования 3/4

Тип данных	Значение	Назначение	PDU	DPF/FLCO
Заголовок данных	0110_2	Адресация	C_HEAD	0011_2
		Собственный заголовок	P_HEAD	1111_2
Передаваемые данные со скоростью кодирования 3/4	1000_2	Блок данных	R_3_4_DATA	NA
		Последний блок данных	R_3_4_LDATA	NA
Терминатор с LC	0010_2	Время задержки	TD_LC	110000_2

5.4.1.2A Типы/PDUs подтвержденных IP данных для скорости кодирования 1

Передача подтвержденных IP данных со скоростью кодирования 1 для прямого режима и режима ретранслятора требует наличия трех типов данных и четырех PDUs. Они перечислены в таблице 5.5A. Если поддерживается собственный заголовок, требуется пятый PDU.

Примечание – Заголовки для скорости кодирования 1 неподтвержденных IP данных кодируются также, как и для скорости кодирования 1/2.

Таблица 5.5A – Типы/PDUs подтвержденных IP данных для скорости кодирования 1

Тип данных	Значение	Назначение	PDU	DPF/FLCO
Заголовок данных	0110_2	Адресация	C_HEAD	0011_2
		Собственный заголовок	P_HEAD	1111_2
Передаваемые данные со скоростью кодирования 1	1010_2	Блок данных	R_1_DATA	NA
		Последний блок данных	R_1_LDATA	NA
Терминатор с LC	0010_2	Время задержки	TD_LC	110000_2

5.4.1.3 Типы/PDUs ответа о передаче подтвержденных данных

Ответ о получении подтвержденных данных как для прямого режима и режима ретранслятора требует наличия двух типов данных и двух блоков PDUs. Они перечислены в таблице 5.6. Если поддерживается собственный заголовок, требуется третий PDU.

Таблица 5.6 – Типы/PDUs ответа о передаче подтвержденных данных

Тип данных	Значение	Назначение	PDU	DPF
Заголовок данных	0110_2	Адресация	C_RHEAD	0001_2
		Собственный заголовок	P_HEAD	1111_2
Данные передаваемые со скоростью кодирования 1/2	0111_2	Блок ответа пакетных данных	C_RDATA	NA

Ответное сообщение включает в заголовке блока C_RHEAD информационные элементы о классе, типе и статусе полученных данных в режиме «stop and wait», которые приведены в таблице 5.7. Информационный элемент N(S) является отправленным порядковым номером, содержащимся в C_HEAD.

Примечание – Таблица 5.7 представляет собой подмножество таблиц разновидностей ответного пакета содержащихся в TS 102 361-1 [1] (пункт 8.2.2.3).

Таблица 5.7 – Ответный пакет IP – данных

Класс	Тип	Статус	Сообщение	Комментарии
002	0012	N(S)	ACK	Все блоки всех пакетов N(S) успешно получены
012	0002	N(S)	NACK	Неправильный (несоответствующий) формат
012	0012	N(S)	NACK	Пакет N(S) CRC доставить не удалось
012	0102	N(S)	NACK	Память получателя является заполненной
012	1002	N(S)	NACK	Не подлежит доставке
102	0002	N(S)	SACK	Получатель запрашивает выборочный повтор блоков, указанных в блоке данных ответного пакета для N(S)

5.4.2 SDL подтвержденных IP данных

Этот пункт использует SDL для иллюстрации сервиса передачи данных по IP используя режим контроля stop and wait с сервисом передачи данных по DLL.

5.4.2.1 SDL отправителя подтвержденных данных

Процедуры доступа к каналу построены на процедурах описанных в TS 102 361-1 [1] (п.5). Правила доступа к конкретному каналу для подтвержденных данных продемонстрированы на рисунке 5.8 с помощью SDL. Они также дополнительно включают T_DataTxLmt и DLL процесса повторной попытки при условии занятого канала, а также T_RspnsWait и приема ответа подтверждения.

Рисунок 5.8 демонстрирует DLL уровень в момент приема примитива IP_Data от CCL (уровень IP). DLL начинается с включения обоих таймеров T_DataTxLmt и T_IdleSrch(поиск в состоянии покоя) и их перехода в состояние Qualify_Idle. DataTxLmt является таймером, ограничивающим время в течение которого DLL пытается передать данные. Он также устанавливает значение счетчика повторов радиоинтерфейса в 0.

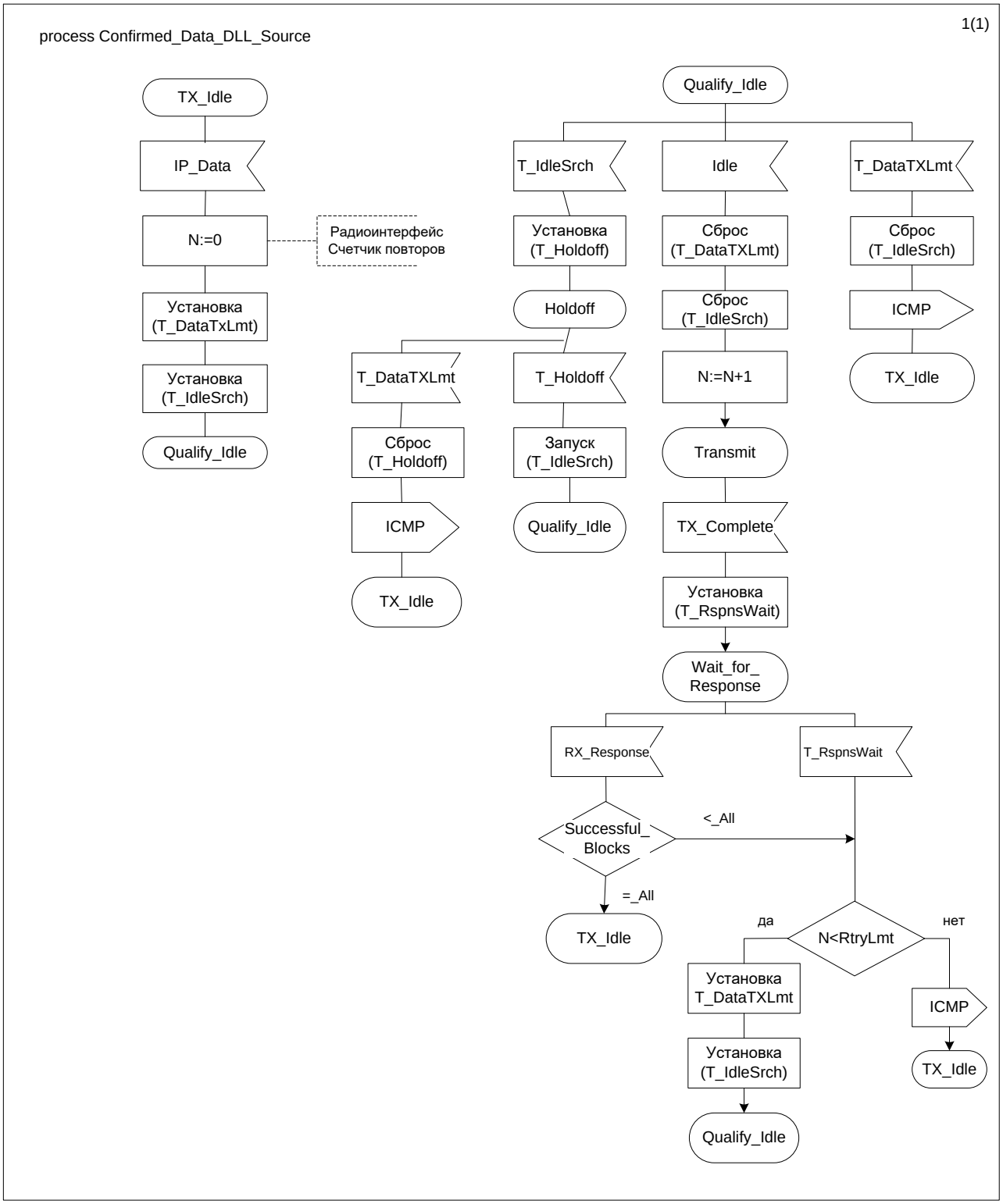

Рисунок 5.8 – SDL передача подтвержденных данных источником
(Source confirmed data transmission SDL)

В состоянии Qualify_Idle DLL пытается определить состояние канала. Если время в таймере T_IdleSrch истекло, канал считается занятым и DLL запускает таймер T_Holdoff и переходит в состояние Ожидание(Holdoff). Таймер T_Holdoff – случайный таймер который используется для минимизации коллизий когда канал становится свободным. Когда время в таймере T_Holdoff истекает, DLL запускает таймер T_IdleSrch и повторяет процесс анализа состояния канала.

Если канал свободен DLL будет передавать данные, увеличит счетчик повторов радиоинтерфейса на 1 и запустит таймер T_RspnsWait т.к. он ожидает подтверждения ответа от принимающей стороны. Если время в таймере T_RspnsWait истекает счетчик повторов радиоинтерфейса меньше значения N_RtryLmt тогда DLL запускает оба таймера T_DataTxLmt и T_IdleSrch и пытается повторно передать

данные. Если время в таймере T_RspnsWait истекло и значение счетчика повторов радиоинтерфейса равно N_RtryLmt тогда передача прекращается и DLL отправляет ICMP примитив CLL показывая что было достигнуто максимальное количество повторов попыток.

Если DLL находится в состоянии Qualify_Idle или состоянии Holdoff и время в таймере T_DataTxLmt истекает, он должен прекратить передачу данных. На рисунке DLL отправляет ICMP примитив CLL показывая что время задержки сообщения было превышено и хост недоступен.

Если ответ подтвержденных данных принят, DLL определяет какой блок должен быть отправлен повторно. Если нет блоков, которые необходимо отправить повторно, передача считается успешной. Если некоторые или все блоки необходимо отправить повторно и значение счетчика повторов радиоинтерфейса меньше N_ RtryLmt тогда DLL запускает оба таймера T_DataTxLmt и T_IdleSrch и переходит в состояние Qualify_Idle. Начиная с этого момента, процесс повторяется так, как описано выше. Если значение счетчика радиоинтерфейса равно N_RtryLmt, тогда передача останавливается и DLL отправляет ICMP примитив на уровень CCL.

5.4.2.2 SDL подтвержденных данных принимающей стороны

Рисунок 5.9 иллюстрирует действия принимающей стороны во момент приема подтвержденных данных. Каждый блок в момент приема проходит CRC проверку также как и целый фрагмент. Если некоторые блоки не проходят CRC проверку, отправитель инициирует отправку SACK ответа. Если все блоки проходят CRC проверку, но фрагмент не проходит, то отправитель инициирует отправку NACK ответа. Если все блоки прошли CRC проверку, отправитель инициирует отправку ACK ответа. В прямом режиме ответ отправляется или вежливо или невежливо в то время, как в режиме повторителя ответ отправляется невежливо.

5.4.3 Диаграммы последовательности сообщений(MSCs) подтвержденных данных

Следующие MSC используются для предоставления дополнительного разъяснения SDL подтвержденных IP данных приведенных в пунктах 5.4.2.1 и 5.4.2.2. Здесь передача IP данных использует режим контроля stop and wait с DLL передачи подтвержденных данных.

5.4.3.1 MSCs источника подтвержденных данных

5.4.3.1.1 MSC передачи подтвержденных IP данных

Рисунок 5.10 показывает как DLL принимает примитив IP_Data демонстрируя доставку подтвержденных данных от CCL. DLL запускает таймер T_DataTxLmt и затем формирует и инициирует отправку сообщения с данными, которое показано в пункте 5.4.3.1.2. Во время передачи данных DLL запускает таймер T_RspnsWait и ожидает ответа как описано в пункте 5.4.3.1.3. Если таймер T_DataTxLmt истекает, DLL отправляет ICMP примитив к CCL демонстрируя – местоназначение было не достигнуто и переходит в состояние PS_TX_Idle. Таймеры определены в пункте 5.4.2.

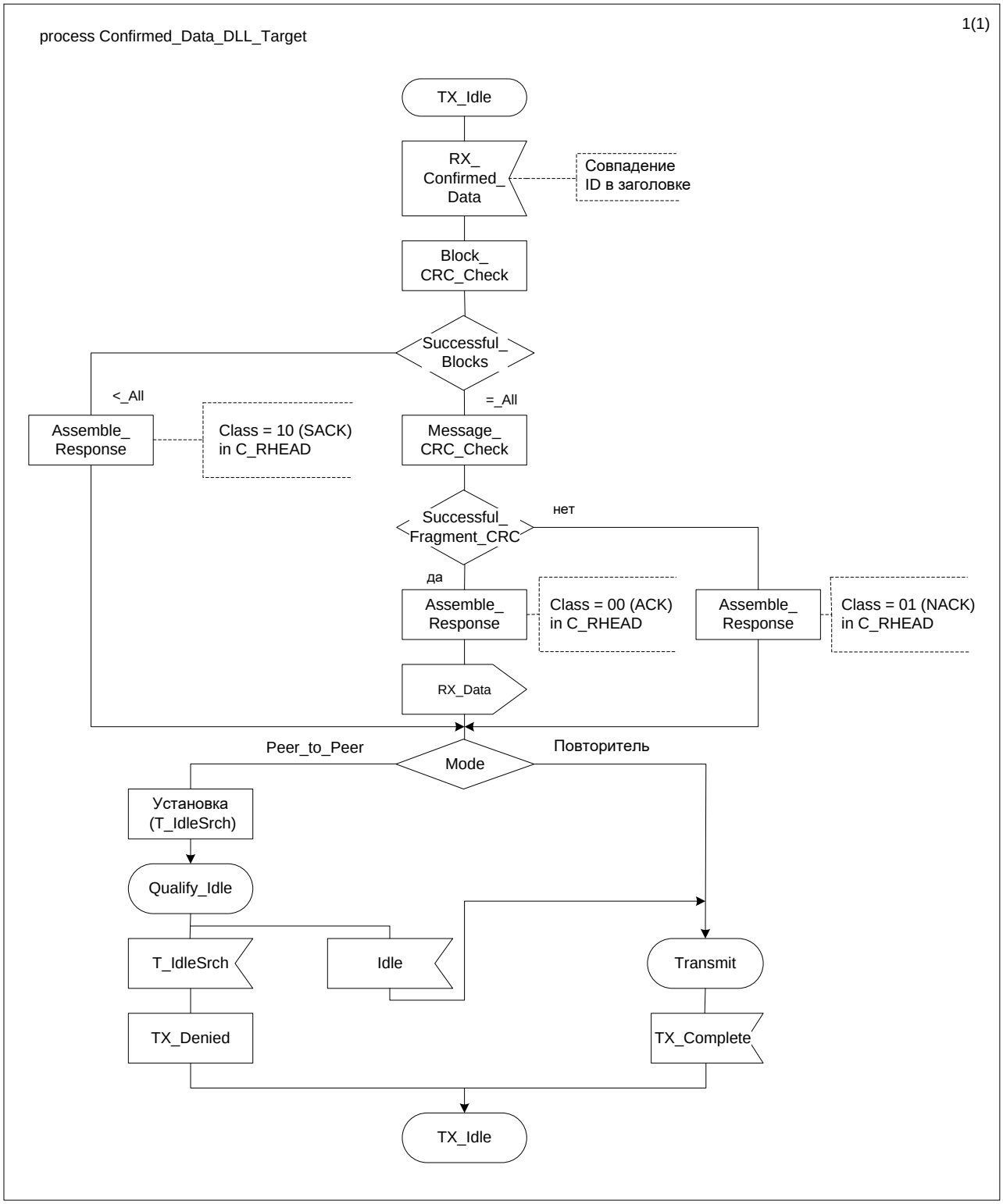

Рисунок 5.9 – SDL передача подтвержденных данных принимающей стороной (Target confirmed data transmission SDL)

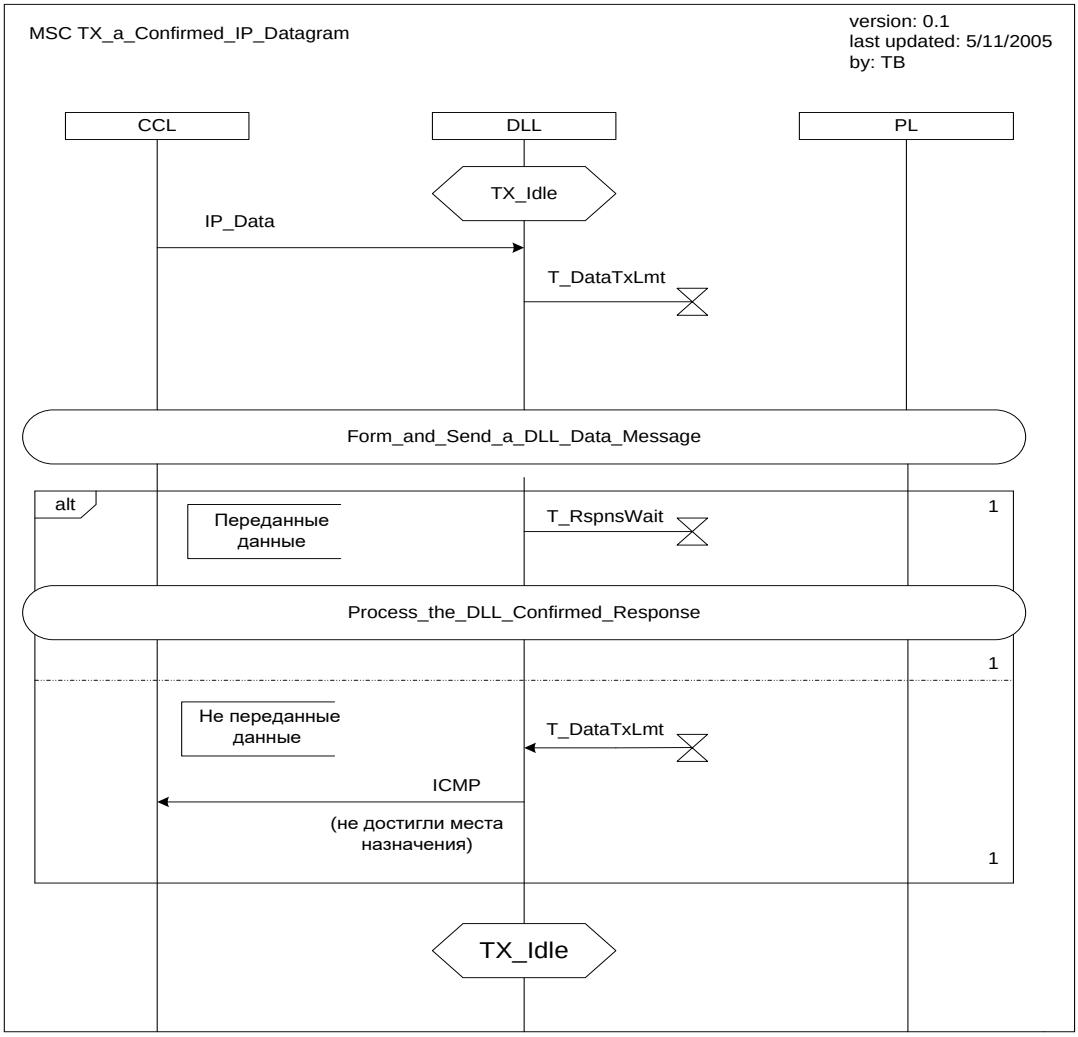

Рисунок 5.10 – MSC передачи подтвержденных IP данных

5.4.3.1.2 MSC формирования и отправки DLL сообщения с данными

MSC для формирования и отправки сообщений DLL подтвержденных данных идентичны MSC, определенных в пункте 5.3.3.2 для неподтвержденных данных.

5.4.3.1.3 MSC процесса DLL подтвержденных данных

Рисунок 5.11 иллюстрирует SDL определенного в пункте 5.4.2.1 с MSC показывающими момент ожидания источником приема заголовка подтвержденных данных. Если значение Class = 002 (ACK) все блоки данных были успешно приняты. Однако, если Class = 102 (SACK), то принимающая сторона уведомляет в ответе подтвержденных данных, какие блоки нужно повторить. Если заголовок ответа подтвержденных данных не дошел, DLL ведет себя также как если он был бы принят с Class = 012 (NACK). Если принимающая сторона запрашивает повторную передачу но значение счетчика повторов радиоинтерфейса равно N_RtryLmt, тогда DLL отправляет ICMP примитив к CCL демонстрируя тем самым, что хост был недоступен и число повторов радиоинтерфейса было исчерпано. Если принимающая сторона запрашивает повторную передачу и значение счетчика повторов радиоинтерфейса менее N_RtryLmt, тогда DLL формирует и отправляет соответствующее DLL сообщение с данными. После повторной передачи запускается таймер T_RspnsWait и DLL опять ждет заголовок ответа подтвержденных данных.

5.4.3.2 MSCs подтвержденных данных принимающей стороны

5.4.3.2.1 MSC приема подтвержденных данных

Рисунок 5.12 показывает действия принимающей стороны в момент приема подтвержденных данных в режиме контроля stop and wait вместо режима контроля sliding window и MS предназначенной для передачи вежливых ответов. После того, как подготовлен подходящий ответ, она запускает таймер T_IdleSrch. Если канал свободен, то передается ответ. Для подтвержденных данных режим idle

также применяется к времени задержки данных. В отдельных случаях, когда канал занят, сообщение не передается. Механизм передачи данных источника повторит передачу заново.

5.4.3.3 MSCs подтвержденных данных BS

5.4.3.3.1 MSC повторения подтвержденных данных

MSC повторения подтвержденных данных идентична MSC повторения неподтвержденных данных определенной в пункте 5.3.3.3 за исключением того, что U_HEAD PDU заменяется на заголовок подтвержденных данных PDU (C_HEAD).

5.4.3.3.1 MSC времени задержки подтвержденных данных

Рисунок 5.13 демонстрирует действия BS когда она подготовлена для работы во время зависания данных. Состояния CCL определены в пункте G.2 TS 102 361-1 [1] и состояние Call_Hangtime также применимо ко времени зависания данных. Во время приема последнего блока подтвержденных данных (C_LDATA) PDU в слоте 1, DLL повторяет блок и отсылает примитив Data_RX_LB_Slot_1 примитив процессу CCL_BS. Процесс CCL_BS отправляет примитив Data_RX_LB процессу CCL_1. Процесс CCL_1 отправляет Data_Terminator примитив процессу CCL_BS, запускает таймер T_DataHngtime и переходит в состояние Call_Hangtime. Таймер T_DataHngtime определяет длительность, в течении которой слот будет оставаться в состоянии зависания данных для данных. Во время приема Data_Terminator примитива, CCL_BS отправляет примитив Data_Terminator_Slot_1 к DLL, который непрерывно передает Terminator Data Link Control (TD_LC) PDUs. К моменту когда истекает таймер T_DataHngtime, процесс CCL_1 шлет примитив Generate_Idles процессу CCL_BS и переходит в состояние Channel_Hangtime. Процесс CCL_BS отсылает примитив Generate_Idles DLL который непрерывно передает Idle PDUs.

5.4.4 Формирование отправлений подтвержденных данных

Передача данных может использовать режим контроля sliding window используя DLL подтвержденных данных передачи данных. Источник постоянно отправляет пакеты данных к получателю для улучшения пропускной способности данных и запрашивает подтверждение по окончании постоянной передачи пакетов данных. Запрошенное подтверждение включает в себя все пакеты данных принятые во время постоянной передачи пакетов данных.

Во время использования режима контроля sliding window источник должен передавать не более чем 7 постоянных пакетов данных (смотри примечание) перед запросом о подтверждении передачи от принимающей стороны восьмого постоянного пакета данных. Каждый пакет данных за исключением последнего пакета должен начинаться с C_HEAD PDUs с информационным элементом Response Requested(A) установленным в значение 0_2. Последний пакет данных должен начинаться с C_HEAD PDU с информационным элементом Response Requested(A) установленным в значение 1_2. Это демонстрирует принимающей стороне, что источник запросил ответ с подтверждением для всех пакетов принятых во время передачи постоянных пакетов данных.

Примечание: Количество постоянных передач данных ограничено информационным элементом пакета Send Sequence Number(N(S)) в загаловке C_HEAD PDU.

Принимающая сторона, поддерживающая режим контроля sliding window должна хранить результаты CRC проверки блока и сообщения от всех пакетов данных непрерывной передачи пакетов данных. В момент приема Last Block PDU, который начинается заголовком C_HEAD PDU с информационным элементом Response Requested (A) установленным в значение 1_2 , принимающая сторона должна отправить соответствующий ответ источнику с заголовком C_RHEAD PDU. Ответу задаются значения информационных элементов Class, Type и Status как определено в TS 102 361-1 [1] (п. 8.2.2.3).

Принимающая сторона может подтвердить правильное получение множества пакетов в заголовке C_RHEAD PDU выставляя значения Send Sequence Number, N(R) последнего успешно принятого пакета в поле информационного элемента Status пакета ответа (Class = 002, Type = 001_2) . Sliding Window может также быть скомбинирован с механизмом SARQ. В этом случае заголовок C_RHEAD PDU от приемника со значениями информационных элементов Class = 10_2, Type = 000_2, and Status = N(R) показывает, что все пакеты до N(R)-1 приняты успешно.

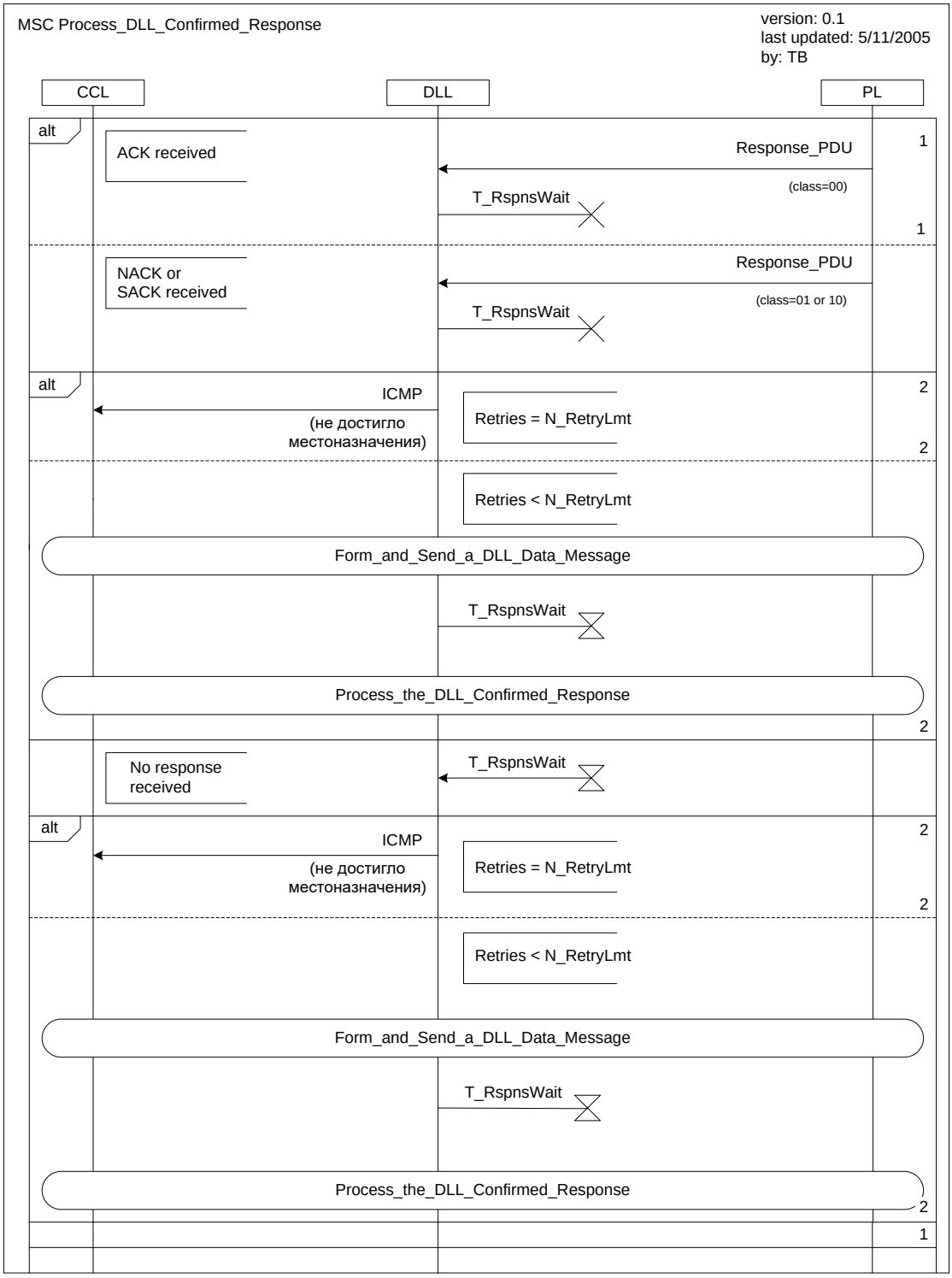

Рисунок 5.11 – MSC процесса ответа DLL подтверждения (Process the DLL confirmed response MSC)

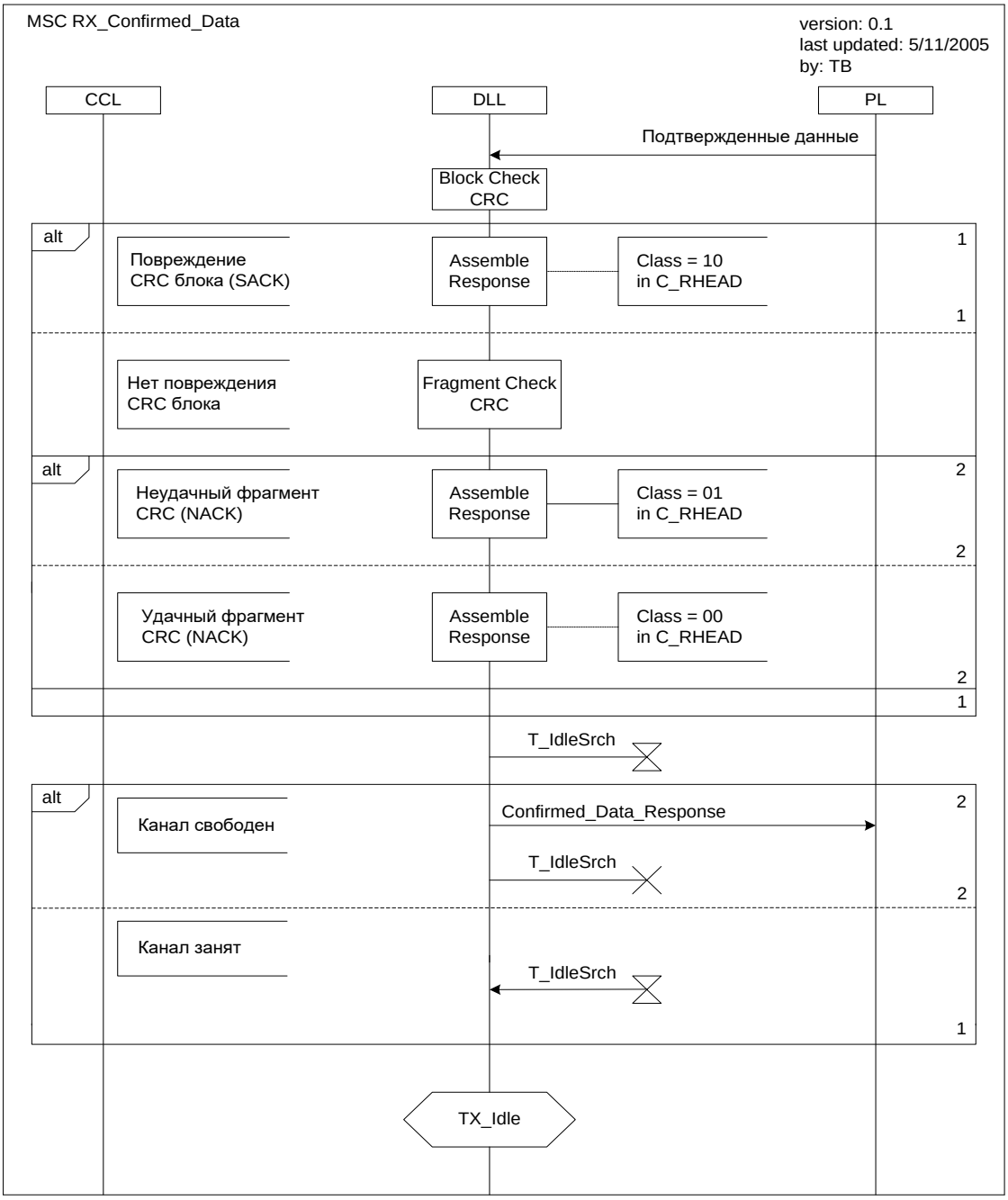

Рисунок 5.12 – MSC RX подтвержденных данных (RX confirmed data MSC)

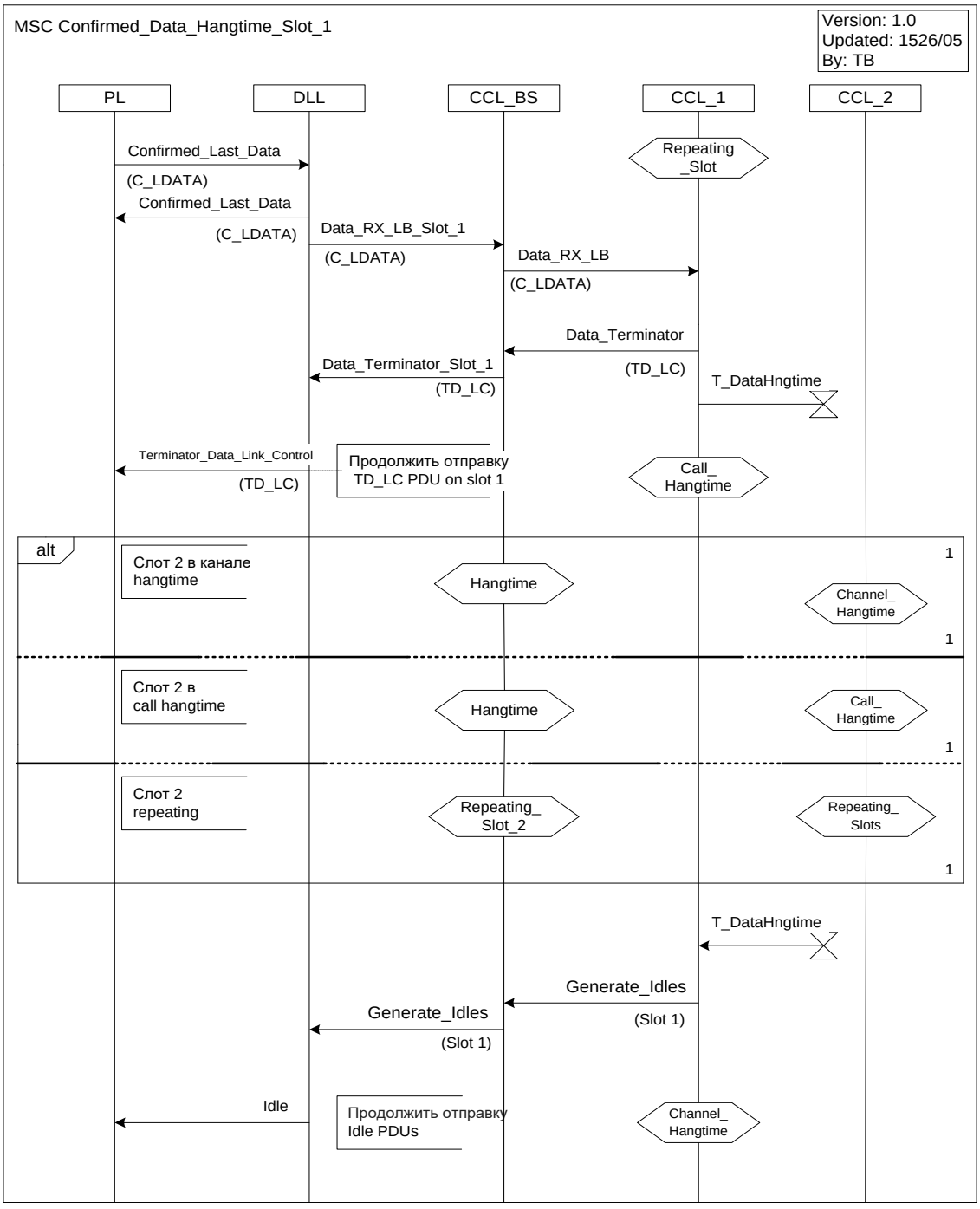

Рисунок 5.13 – MSC подтвержденных данных во время hangtime

5.5 Данные UDP/IPv4

Кроме приложений с полезными данными, пакеты данных UDP/IPv4 содержат UDP-заголовок (8 байт) и заголовок IPv4 (20 байт), когда необязательное поле IP Опция не используется, как показано на рисунках 5.14 и 5.15 соответственно.

Рисунок 5.14 – Заголовок UDP

Рисунок 5.15 – Заголовок IPv4

5.6 Сжатый заголовок UDP/IPv4

Кроме информационной нагрузки приложения, пакеты данных UDP/IPv4 также содержат и UDP заголовок(8 байт) и IPv4 заголовок(20 байт), в случае, когда опциональное поле IP Option не используется, как показано на рисунках 5.14 и 5.15 соответственно. Для дейтаграмм с малыми объемами полезной нагрузки приложения дополнительные 28 байт заголовков UDP/IPv4 могут оказаться значительной частью общего объема полезной нагрузки. Это увеличивает время передачи информации и в некоторых случаях может влиять на производительность системы. Сжатие заголовков UDP/IPv4 минимизирует дополнительную полезную нагрузку в то же самое время оставляя все положительные стороны передачи данных с использованием UDP/IPv4.

Механизм сжатия UDP/IPv4 поддерживает только IPv4 заголовки, которые не используют поле(я) IP Options. Если информационный элемент IP Options используется в заголовке IPv4, информация должна передаваться в несжатом UPD/IPv4 заголовке. Количество информационных элементов в UDP и IPv4 заголовках является или константой или может быть рассчитано без дополнительной информации заголовка переданной по приемному радиоканалу. Эти информационные элементы не отправляются по радиоэфиру когда осуществляется передача с использованием сжатия заголовков UDP/IPv4. Не передаются следующие информационные элементы UDP заголовка – UDP Length и UDP Checksum. Не передаются следующие информационные элементы IPv4 заголовка - IPv4 Version, IPv4 Internet Header Length (IHL), IPv4 Type of Service (TOS), IPv4 Total Length, IPv4 IP Flags, IPv4 Fragment Offset, IPv4 Time to Live, IPv4 Protocol и IPv4 Header Checksum.

Оставшиеся информационные элементы (UDP Source Port, UDP Destination Port, IPv4 Identification, IPv4 Source Address and IPv4 Destination Address) требуют механизма отправки по радиоэфиру. Информационный элемент IPv4 Identification, который поддерживает фрагментацию и во время передачи через MS и внутри IP сети, передается в полном объеме и дальнейшее уменьшение размера заголовка достигается с помощью индексирования UDP Source Port и UDP Destination Port актуальными номерами портов. Дальнейшее уменьшение заголовка достигается с помощью комбинирования Source LLID в информационном заголовке L2 с дополнительным значением Source Address Identifier(SAID) в сжатом заголовке для создания уникального IPv4 Source Address и с помощью комбинирования Destination LLID в информационном заголовке L2 с дополнительным значением Destionation Address Identifier(DAID) в сжатом заголовке для создания уникального IPv4 Destination Address. Дополнительно, если или один из UDP портов (источника или приемной стороны) или оба UDP порта не имеют назначенного индекса, тогда сжатый заголовок поддерживает механизм для передачи полного номера порта(ов).

Механизм сжатия в общем случае уменьшит размер заголовка UDP/IPv4 с 28 байт до 5, хотя варианты с 7 и 9 байтами также определены для поддержки некоторых случаях. Сжатый заголовок UDP/IPv4 должен быть передан в первом пакете Data Continuation и его наличие обозначается в заголовке Data (U_HEAD PDU или C_HEAD PDU) с помощью значения информационного элемента SAP сжатия заголовка UDP/IP, выставленного в 0011_2, как определено в TS 102 361-1 [1] (п. 9.3.18). В качестве примера, структура первого блока продолжения(?) данных для неподтвержденных данных со скоростью кодирования ½ и структура первого блока продолжения(?) данных для подтвержденных данных со скоростью кодирования ¾ показаны на рисунках 5.16 и 5.17 соответственно. Опциональные информационные элементы Extended Header 1 и Extended Header 2 передают полный номер UDP порта когда или один из UDP портов (источника или приемной стороны) или оба UDP порта не имеют назначенного индекса. Когда опциональные информационные элементы Extended Header не используются, эти поля заменяются Application Data. Подробности об использовании информационных элементов UDP Header и IPv4 Header при сжатии и декомпрессии смотри в пункте 7.2 настоящего стандарта.

Бит

	7	6	5	4	3	2	1	0
0	IP идентификация							
1								
2	SAID						DAID	
3	Op1	SPID						
4	Op2	DPID						
5	Расширенный заголовок 1 (опционально)							
6								
7	Расширенный заголовок 2 (опционально)							
8								

9	Приложенные (заявленные) данные
10	
11	

Рисунок 5.16 – Передача неподтвержденных данных со скоростью кодирования ½ с UDP/IPv4 сжатием заголовка

	Бит 7	6	5	4	3	2	1	0
0	Серийный номер блока данных							
1	9 битный CRC							
2	IP идентификация							
3								
4	SAID				DAID			
5	OP1	SPID						
6	OP2	DPID						
7	Расширенный заголовок 1 (опционально)							
8								
9	Расширенный заголовок 2 (опционально)							
10								
11	Приложенные (заявленные) данные							
12								
13								
14								
15								
16								
17								

Рисунок 5.17 – Передача подтвержденных данных со скоростью кодирования ¾ с UDP/IPv4 сжатием заголовка

5.7 Передача информационных данных по IP

UDP/IPv4 может передавать все типы информационных данных. Основные виды данных, поддерживающих передачу текстовых сообщений и данных местоположения определены далее в последующих пунктах.

5.7.1 Передача текстовых сообщений

Передача текстовых сообщений должна использовать кодировку UTF-16BE[15] в плоскости 0 или BMP(Basic Multilingual Plane). По умолчанию должен использоваться UDP порт радиосети 5016. Рекомендуется, чтобы UDP порт был настраиваемым для разрешения конфликтов адресов при включении в существующую работающую сеть.

5.7.2 Передача данных местоположения

Передача данных местоположения должна использовать Location Information Protocol [13]. По умолчанию должен использоваться UDP порт радиосети 5017. Рекомендуется чтобы UDP порт был настраеваемым для разрешения конфликтов адресов при включении в существующую работающую сеть.

6 Передача коротких данных

Этот раздел описывает механизм передачи сообщений коротких данных от одного DMR объекта на другой(гие) DMR объект(ы). Передача может быть подтвержденной или не подтвержденной. В зависимости от FEC и подтверждения/не подтверждения передачи данных, механизм способен передавать до 1 508 байт (24 байта/блок × 63 блока минус 4 байта).

Каждое сообщение состоит из заголовка данных и в большинстве случаев пакетов самих данных (скорости кодирования 1/2, 3/4 или 1). Последний блок пакетов данных должен включать 32 битное сообщение CRC.

Заголовок коротких данных содержит параметры, определяющие передачу данных и в частности количество и формат данных, передаваемых в сообщении.

В DLL передача неподтвержденных коротких данных должна соответствовать передаче неподтвержденных данных как определено в пункте 5.3 настоящего стандарта, хотя MS может использовать невежливый тип механизма доступа к каналу. Также в DLL передача подтвержденных коротких данных должна соответствовать передаче подтвержденных данных как определено в пункте 5.4 настоящего стандарта, хотя MS может использовать невежливый тип механизма доступа к каналу. Передача подтвержденных данных коротких сообщений должна поддерживать режим контроля stop and wait.

Примечание – Форматы заголовка не поддерживают режим контроля sliding window для коротких данных.

Передача коротких данных должна использовать вежливый тип (вежливый по отношению к собственному цветовому коду или вежливый ко всем) механизма доступа к каналу как определено в TS 102 361-1 [1] (п. 5.2.1). В системе ретрансляции когда BS находится в режиме BS_Hibernating (как определено в TS 102 361-1 [1] (п. G.2)), началу передачи должна предшествовать процедура BS Downlink Activation как описано в TS 102 361-2 [2] (п. 5.1.1.1).

6.1 Определенные данные

Определенные данные – это передача небольшого количества данных среди DMR объектов с заранее определенным форматом данных как определено информационным элементом “DD Format” в блоке Short Data Header. Информационный элемент DD Format должен быть таким же как определено в TS 102 361-1 [1].

6.1.1 Типы/PDUs определенных данных

Определенные данные могут использовать скорости кодирования 1/2, 3/4 или 1 как для подтвержденных, так и для неподтвержденных данных. Все типы данных/PDUs являются такими же, как описано в пункте 5 настоящего стандарта, за исключением заголовка данных как описано в таблице 6.1.

Таблица 6.1 – Особенности «Тип/PDUs» определенных данных

Тип данных	Значение	Назначение	PDU	DPF
Заголовок данных	0110_2	Адресация	DD_HEAD	1101_2

6.1.2 Значения информационного элемента определенных данных

Определенные данные должны использовать значение информационного элемента SAP Identifier коротких данных приведенное в TS 102 361-1 [1] (п. 9.3.18).

Значение информационного элемента Appended Blocks заголовка не должно быть равно 000000_2 так как вся информация передаются в блоках данных.

Значение информационного элемента Response Requested (A) заголовка должно быть равно 0_2 для неподтвержденных данных и 1_2 для подтвержденных.

6.2 Необработанные данные

Необработанные данные – это передача небольшого количества данных среди приложений, запущенных на DMR объектах которые предоставляют определение формата передаваемой информации самим приложениям. DMR DLL обеспечивает передачу данных между портами источника и местоназначения DMR объектов как определено в полях портов источника и местоназначения соответственно.

6.2.1 Типы/PDUs необработанных данных

Необработанные данные могут использовать скорости кодирования 1/2, 3/4 или 1 как для подтвержденных, так и для неподтвержденных данных. Все типы данных/PDUs являются такими же как описано в пункте 5 настоящего стандарта за исключением заголовка данных как описано в таблице 6.2.

Таблица 6.2 – Особенности «Тип/PDUs» необработанных данных

Тип данных	Значение	Назначение	PDU	DPF
Заголовок данных	0110_2	Адресация	R_HEAD	1110_2

6.2.2 Значения информационного элемента необработанных данных

Необработанные данные должны использовать значение информационного элемента SAP Identifier коротких данных приведенное в TS 102 361-1 [1] (п. 9.3.18).

Значение информационного элемента Appended Blocks заголовка не должно быть равно 000000_2 так как вся информация передаются в блоках данных.

Значение информационного элемента Response Requested (A) заголовка должно быть равно 0_2 для неподтвержденных данных и 1_2 для подтвержденных.

6.3 Статусная/прекодированные данные

Status/precoded – это передачи прекодированных и статусных сообщений от одного объекта DMR к другому(-им) объекту(-ам) DMR. Precoded/Status сообщение – это услуга, которая позволяет отправить код по радиоканалу, значение которого известно всем остальным участникам. Обычно в каждом объекте DMR хранится таблица соответствий определенных кодов определенным значениям(к примеру, код=0000000001_2 значение=”Принято”). Прекодированные и статусные сообщения содержат всю информацию в заголовке данных. Поэтому информационный элемент AB (appended blocks) заголовка данных должен быть выставлен в значение 000000_2.

Примечание: Статусные/прекодированные данные не поддерживают DLL SARQ.

6.3.1 Типы данных/PDUs статусных/прекодированных данных

Status/precoded данные передаются только в заголовке данных PDU. Могут использоваться как неподтвержденные так и подтвержденные данные. Типы данных/PDUs перечислены в таблице 6.3

Таблица 6.3 – Особенности «Тип/PDUs» статусных/прекодированных данных

Тип данных	Значение	Назначение	PDU	DPF
Заголовок данных	0110_2	Адресация	SP_HEAD	1110_2

6.3.2 Значения информационного элемента статусных/прекодированных данных

Status/precoded данные должны использовать значение информационного элемента SAP Identifier коротких данных приведенное в TS 102 361-1 [1] (п. 9.3.18).

Значение информационного элемента Appended Blocks заголовка должно быть равно 000000_2 так как вся информация передаются в заголовке данных. Комбинация значения 1110_2 информационного элемента Packet Data Format и значения 00_2 информационного элемента Appended Blocks идентифицирует заголовок коротких данных для работы со статусными/прекодированными короткими данными.

В заголовке информационного элемента Response Requested (A) значение должно выставлено в 0_2 для неподтвержденных данных и 1_2 для подтвержденных.

6.4 Ответ о подтверждении коротких данных Short data confirmed response

Ответ о подтверждении коротких данных для прямого режима и режима ретранслятора требует 2 типа данных и 2 PDUs. Они перечислены в таблице 6.4. Если поддерживается собственный заголовок, требуется третий блок PDU.

Таблица 6.4 – Типы/PDUs ответа подтвержденных данных

Тип данных	Значение	Назначение	PDU	DPF/FLCO
Заголовок данных	0110_2	Адресация	C_HEAD	0001_2
		Собственный заголовок	P_HEAD	1111_2
Данные, передаваемые со скоростью кодирования 1/2	0111_2	Блок данных пакета ответа	C_RDATA	NA

Комбинация информационных элементов A и SARQ, содержащихся в R_HEAD PDU или DD_HEAD PDU должна указать тип ответа, как показано в таблице 6.5.

Таблица 6.5 – Данные ответа

A	SARQ	Примечание
0	0	Сообщение не подтверждено (нет ответа)
0	1	Зарезервировано для будущего использования
1	0	Сообщение подтверждено (относится ко всему сообщению)
1	1	Сообщение подтверждено (SARQ на блок к основному блоку)

Информационный элемент F в R_HEAD PDU или DD_HEAD PDU должен быть 1_2, если SARQ не используется. Если SARQ используется, информационный элемент F должен быть 1_2 в первой попытке передачи и 0_2 в последующих попытках.

Ответное сообщение определяется информационными элементами «Класс», «Тип» и «Статус» в C_RHEAD, приведенном в таблице 6.6

Таблица 6.6 – Пакет ответа коротких данных с определением класса, типа и статуса

Класс	Тип	Статус	Сообщение	Комментарии
002	0012	N(S)	ACK	Все блоки всех пакетов N(S) успешно получены
012	0002	N(S)	NACK	Неправильный (несоответствующий) формат
012	0012	N(S)	NACK	Пакет с неверной CRC
012	0102	N(S)	NACK	Память получателя заполнена
012	1002	N(S)	NACK	Не подлежит доставке
102	0002	N(S)	SACK	Получатель запрашивает выборочный повтор блоков, указанных в блоке данных ответного пакета

Примечания:

1 Сообщение ответа коротких данных поддерживается только функцией «stop and wait flow control».

2 Таблица 6.6 представляет собой варианты возможных пакетов ответа, определенной таблицей находящейся в TS 102 361-1 [1] (пункт 8.2.2.3).

7 Описание PDU

Этот раздел описывает PDUs, которые применяются для передачи пакетных данных в протоколе DMR 3-го уровня, как описано в настоящем стандарте.

Ниже приведенные пункты содержат описания PDUs и информационных элементов, содержащихся в них. Структура определенных PDU, представленная в таблицах, выглядит следующим образом:

- в столбце «информационный элемент» приводится имя содержащегося элемента(ов);
- столбец «длина элемента» определяет длину элемента в битах;
- столбец «примечания» содержит другую информацию об информационном элементе;

Элементы должны быть переданы в порядке, указанном в TS 102 361-1 [1].

7.1 Пакеты и блоки данных (PDP PDUs) 3-го и 4-го уровня

Из-за характера DMR, при тесном взаимодействии между слоями 2 и 3, а также в связи с необходимостью иметь достоверную информацию о состоянии канала, PDUs слоя 3 подробно описаны в следующих разделах, и могут включать в себя два типа элементов:

- **зависимые элементы сообщения**. Эти элементы являются видимыми для слоя 2, и могут быть использованы любой MS (которая способна декодировать их), независимо от адресации. Эти элементы зависят от элемента тип сообщения. Некоторые генерируются слоем 2, когда он создает полное сообщение, тогда как другие генерируются слоем 3;
- **конкретные элементы.** Они являются "верными" для элементов слоя 3. Они обрабатываются только MSs которым они адресованы.

Там, где существуют оба типа в PDU, они показаны отдельно.

7.1.1 Полное управление соединением (FULL LC) PDUs

Этот раздел описывает FULL LC PDUs для PDP. Более подробное определение LC сообщений изложено в TS 102 361-1 [1] (раздел 7).

7.1.1.1 Терминатор управления соединением для передачи данных PDU

Нулевой (0) и первый октет (1) терминатора управления соединением для передачи данных (TD_LC) PDU соответствует структуре формата LC, как это определено в TS 102 361-1 [1] (пункт 7.1, рисунок 7.1). 2 – 8 октеты терминатора управления соединением для передачи данных содержат конкретную информацию. Содержание TD_LC PDU в таблице 7.1

Таблица 7.1 – Содержание TD_LC PDU

Информационный элемент	Длина	Примечания
зависимые элементы сообщения		
Защитный флаг (PF)	1	См. TS 102 361-1 [1] (пункт 9.3.10)
Зарезервированный	1	Этот бит должен быть установлен 0_2
конкретные элементы		
Opcode управления соединением	6	Должен быть установлен $110\ 000_2$

Full (FLCO)		
Признак ID (FID)	8	Должен быть установлен $00\ 000\ 000_2$
ID логического соединения (LLID)	24	Место назначения, см. TS 102 361-1 [1] (пункт 9.3.19)
ID логического соединения (LLID)	24	Источник, см. TS 102 361-1 [1] (пункт 9.3.19)
Группа или индивидуальный (G/I)	1	Он должен быть установлен для группы 1_2, см. TS 102 361-1 [1] (пункт 9.3.15)
Запрос ответа (A)	1	См. TS 102 361-1 [1] (пункт 9.3.16)
Флаг сообщения Full (FMF)	1	См. TS 102 361-1 [1] (пункт 9.3.20)
Зарезервированный	1	Этот бит должен быть установлен 0_2
Флаг ресинхронизации (S)	1	См. TS 102 361-1 [1] (пункт 9.3.23)
Отправить номер последовательности (N(S))	3	См. TS 102 361-1 [1] (пункт 9.3.24)

7.2 UDP/IPv4 сжатый заголовок

7.2.1 Информационные элементы UDP заголовка

UDP заголовок определен в RFC 768 [14]. Когда MS получает UDP/IPv4 сжатый заголовок, она должна распаковать UDP заголовок перед отправкой его на IP уровень. Данный пункт описывает, как информационные элементы заголовка UDP используются в процессах сжатия и распаковки UDP заголовка.

7.2.1.1 Номер порта источника UDP

Действия MS во время формирования сжатого заголовка UDP/IPv4 зависят от того, содержит или нет MS в заголовке UDP заранее определенный ID источника порта (SPID) связанный с номером порта источника UDP. Если в MS эта заранее определенная связь существует, соответствующий информационный элемент SPID должен быть передан в сжатом заголовке. Если эта заранее определенная связь не существует, информационный элемент SPID должен быть передан как $0\ 000\ 000_2$, а полный номер порта источника UDP должен быть передан как опциональный информационный элемент Расширенный Заголовок в сжатом заголовке. Когда номер источника порта отправляется в опциональном Расширенном Заголовке, он всегда отправляется в информационном элементе Расширенный Заголовок 1.

Действия MS во время распаковки принятого сжатого UDP/IPv4 заголовка зависят от принятого информационного элемента SPID. Если значение принятого SPID не равно $0\ 000\ 000_2$, тогда Номер Порта UDP Источника в Заголовке UDP является Номером Порта Источника связанного со значением SPID в приемной MS. Если значение принятого SPID равно $0\ 000\ 000_2$, тогда Номер Порта Источника UDP в заголовке UDP является опциональным информационным элементом Расширенный Заголовок. Когда номер источника порта отправляется в опциональном Расширенном Заголовке, он всегда отправляется в информационном элементе Расширенный Заголовок 1.

7.2.1.2 Номер порта назначения UDP

Действия MS во время формирования UDP/IPv4 сжатого заголовка зависят от того, содержит или нет MS в заголовке UDP заранее определенный ID назначения порта (DPID) связанный с номером порта назначения UDP. Если в MS эта заранее определенная связь существует соответствующий информационный элемент DPID должен быть передан в сжатом заголовке. Если эта заранее определенная связь не существует, информационный элемент DPID должен быть передан как $0\ 000\ 000_2$, а полный номер порта назначения UDP должен быть передан как опциональный информационный элемент Расширенный Заголовок в сжатом заголовке. Когда Номер Порта Назначения отправляется а опциональном Расширенном Заголовке, он может отправляться как в информационном элементе Расширенный Заголовок 1, так и в информационном элементе Расширенный Заголовок 2. Если значение Номера Порта Источника UDP в сжатом заголовке не равно $0\ 000\ 000_2$, тогда Номер Порта Назначения UDP отправляется в информационном элементе Расширенный Заголовок 1. Если значение Номера Порта Источника UDP в сжатом заголовке равно $0\ 000\ 000_2$, тогда Номер Порта Назначения UDP отправляется в информационном элементе Расширенный Заголовок 2.

Действия MS во время распаковки принятого сжатого заголовка UDP/IPv4 зависят от принятого информационного элемента DPID. Если значение принятого DPID не равно $0\ 000\ 000_2$, тогда Номер Порта UDP Назначения в Заголовке UDP является Номером Порта Назначения связанного со значением DPID в приемной MS. Если значение принятого DPID равно $0\ 000\ 000_2$, тогда Номер Порта Назначения UDP в заголовке UDP является опциональным информационным элементом Расширенный Заголовок. Когда Номер Порта Назначения отправляется как опциональный Расширенный Заголовок, он может отправляться и как информационный элемент Расширенный Заголовок 1 и как информационный элемент Расширенный Заголовок 2. Если значение Номера Порта Источника UDP в расширенном заголовке не равно $0\ 000\ 000_2$, тогда Номер Порта Назначения UDP отправляется как информационный элемент Расширенный Заголовок 1. Если значение Номера Порта Источника UDP в расширенном заголовке равно $0\ 000\ 000_2$, тогда Номер Порта Назначения UDP отправляется как информационный элемент Расширенный Заголовок 2.

7.2.1.3 Длина UDP

Информационный элемент «Длина UDP» - это длина в байтах пользовательской дейтаграммы, включая заголовок и прилагаемые данные. Значение этого поля не передается в сжатом заголовке UDP/IPv4 и принимающая MS рассчитывает значение этого поля, на основании принятой дейтаграммы, как показано в таблице 7.2.

Таблица 7.2 – Декомпрессия элемента Длина UDP

Информационный элемент	Длина	Значение	Примечание
Длина UDP	16		Расчет (см. Примечание)
Примечание – Длина UDP (в байтах) = длина заголовка UDP (8 байт) + пользовательские данные (в байтах) - сжатый заголовок UDP/IPv4 (в байтах).			

7.2.1.4 Контрольная сумма UDP

Информационный элемент «Контрольная сумма UDP» не передается и принимающая MS должна вычислять значение после восстановления заголовка UDP/IPv4. Принимающая MS должна использовать алгоритм контрольной суммы, как описано в таблице 7.3

Таблица 7.3 – Декомпрессия контрольной суммы UDP

Информационный элемент	Длина	Значение	Примечание
Контрольная сумма UDP	16		Расчет (см. Примечание)
Примечание – Алгоритм указан в RFC 768 [14].			

7.2.2 Информационные элементы заголовка IPv4

Заголовок IPv4 определен в RFC 791 [4]. Когда радиоприемник получает сжатый заголовок UDP/IPv4, он должен распаковать заголовок, перед отправкой заголовка IPv4 на уровень IP. В данном разделе описывается, как эти информационные элементы используются в сжатом заголовке IPv4 и процессы декомпрессии (распаковывания).

7.2.2.1 Версия IPv4

Информационный элемент версия IPv4 является постоянным, так как сжатый заголовок UDP/IPv4 поддерживает только IPv4. Значение этого поля не передается в сжатом заголовке UDP/IPv4 и MS, принимающая сжатый заголовок UDP/IPv4, должна установить это значение в заголовке IPv4, как описано в таблице 7.4.

Таблица 7.4 – Декомпрессия Версия IPv4

Информационный элемент	Длина	Значение	Примечание
Версия IPv4	4	0100_2	

7.2.2.2 Длина интернет заголовка IPv4 (IHL)

Информационный элемент Длина интернет заголовка IPv4 является постоянным, так как сжатый заголовок UDP/IPv4 не поддерживает IP-опции. Значение этого поля не передается в сжатом заголовке UDP/IPv4 и MS, принимающая сжатый заголовок UDP/IPv4, должна установить это значение в заголовке IPv4, как описано в таблице 7.5.

Таблица 7.5 – Декомпрессия Длина интернет заголовка IPv4

Информационный элемент	Длина	Значение	Примечание
Длина интернет заголовка IPv4	4	0101_2	

7.2.2.3 Тип обслуживания (TOS) IPv4

Информационный элемент «Тип обслуживания (TOS) IPv4» не поддерживается внутри радиосети (RAN). Значение этого поля не передается в сжатом заголовке UDP/IPv4 и MS, принимающая сжатый заголовок UDP/IPv4, должна установить это значение в заголовке IPv4, как описано в таблице 7.6.

Таблица 7.6 – Декомпрессия Тип обслуживания (TOS) IPv4

Информационный элемент	Длина	Значение	Примечание
Тип обслуживания (TOS) IPv4	8	$00\ 000\ 000_2$	

7.2.2.4 Информационный элемент «Общая длина IPv4» (IPv4 Total Length)

Информационный элемент «Общая длина IPv4» в IP дейтаграмме имеет длину в байтах. Значение этого поля не передается в сжатом заголовке UDP/IPv4 и MS, принимающая сжатый заголовок UDP/IPv4, должна вычислить значение этого поля, на основе принятой дейтаграммы, как описано в таблице 7.7.

Таблица 7.7 – Декомпрессия информационного элемента «Общая длина IPv4»

Информационный элемент	Длина	Значение	Примечание
Общая длина IPv4	16		Расчет (см. Примечание)
Примечание – Общая длина IPv4 (в байтах) = длина заголовка IPv4 (20 байт) + длина UDP (в байтах).			

7.2.2.5 Информационный элемент «идентификация IPv4» (IPv4 Identification)

Информационный элемент «идентификация IPv4», как описано в таблице 7.8, передается в сжатом заголовке UDP/IPv4 и MS, принимающая сжатый заголовок UDP/IPv4 должна использовать полученное значение в заголовке IPv4.

Таблица 7.8 – Информационный элемент «идентификация IPv4»

Информационный элемент	Длина	Значение	Примечание
идентификация IPv4	16		

7.2.2.6 Информационный элемент «флаги IPv4» (IPv4 Flags)

Информационный элемент «IPv4 Flags» не поддерживается внутри радиосети (RAN). Значение этого поля не передается в сжатом заголовке UDP/IPv4 и MS, принимающая сжатый заголовок UDP/IPv4, должна установить это значение в заголовке IPv4, как описано в таблице 7.9.

Таблица 7.9 – Декомпрессия информационного элемента «IPv4 Flags»

Информационный элемент	Длина	Значение	Примечание
IPv4 Flags	3	000_2	

7.2.2.7 Информационный элемент «смещение фрагмента IPv4» (IPv4 Fragment Offset)

Информационный элемент «IPv4 Fragment Offset» не поддерживается внутри радиосети (RAN). Значение этого поля не передается в сжатом заголовке UDP/IPv4 и MS, принимающая сжатый заголовок UDP/IPv4, должна установить это значение в заголовке IPv4, как описано в таблице 7.10.

Таблица 7.10 – Декомпрессия информационного элемента «IPv4 Fragment Offset»

Информационный элемент	Длина	Значение	Примечание
IPv4 Fragment Offset	13	$0\ 000\ 000\ 000\ 000_2$	

7.2.2.8 Информационный элемент «IPv4 время жизни» (IPv4 Time to Live)

Информационный элемент «IPv4 Time to Live» не поддерживается внутри радиосети (RAN). Значение этого поля не передается в сжатом заголовке UDP/IPv4 и MS, принимающая сжатый заголовок UDP/IPv4, должна установить это значение в заголовке IPv4, как описано в таблице 7.11.

Таблица 7.11 – Декомпрессия информационного элемента «IPv4 Time to Live»

Информационный элемент	Длина	Значение	Примечание
IPv4 Time to Live	8	$01\ 00\ 00\ 00_2$	

7.2.2.9 Информационный элемент «IPv4 протокол» (IPv4 Protocol)

Информационный элемент «IPv4 Protocol» указывает следующий протокол сетевого уровня, используемый в части данных интернет дейтаграммы. Он должен быть постоянным, так как UDP/IPv4 сжатый заголовок поддерживает только следующий уровень протокола UDP. Значение этого поля не передается в сжатом заголовке UDP/IPv4 и MS, принимающая сжатый заголовок UDP/IPv4, должна установить это значение в заголовке IPv4, как описано в таблице 7.12.

Таблица 7.12 – Декомпрессия информационного элемента «IPv4 Protocol»

Информационный элемент	Длина	Значение	Примечание
IPv4 Protocol	8	$00\ 01\ 00\ 01_2$	

7.2.2.10 Информационный элемент «IPv4 контрольная сумма заголовка» (IPv4 Header Checksum)

Информационный элемент «IPv4 Header Checksum» не передается и принимающая MS должна вычислить значение после того, как заголовок UDP/IPv4 повторно построен. Принимающая MS должна использовать алгоритм контрольной суммы, указанной в RFC 791 [4].

Таблица 7.13 – Декомпрессия информационного элемента «IPv4 Header Checksum»

Информационный элемент	Длина	Значение	Примечание
IPv4 Header Checksum	16		Расчет (см. Примечание)
Примечание – Алгоритм указан в RFC 791 [4].			

7.2.2.11 Информационный элемент «IPv4 адрес источника» (IPv4 Source Address)

Информационный элемент «IPv4 адрес источника» является источником IP-дейтаграммы, и он не передается в сжатом заголовке UDP/IPv4. Принимающая MS должна получить это значение из информационного элемента SAID в UDP/IPv4 сжатом заголовке и источника LLID либо в заголовке данных U_HEAD (неподтвержденные данные) либо в C_HEAD (подтвержденные данные).

Например, если система использует радиосеть класса A со значением 12, принятый информационный элемент SAID имеет значение 0000_2 (радиосеть) и принятое значение источника LLID равно 5, то полученный IPv4 адрес источника 12.0.0.5. Это следует из пункта 5.1.1 «DLL полученная IP-адресация», в настоящем стандарте.

7.2.2.12 Информационный элемент «IPv4 адрес назначения» (IPv4 Destination Address)

Информационный элемент «IPv4 адрес назначения» является пунктом назначения IP-дейтаграммы, и не передается в сжатом заголовке UDP/IPv4. Принимающая MS должна получить это значение из информационного элемента DAID в UDP/IPv4 сжатом заголовке и источника LLID либо в заголовке данных U_HEAD (неподтвержденные данные) либо в C_HEAD (подтвержденные данные).

Например, если система использует радиосеть класса A со значением 12, принятый информационный элемент DAID имеет значение 0000_2 (радиосеть) и принятое значение источника LLID равно 3, то полученный IPv4 адрес источника 12.0.0.3. Это следует из пункта 5.1.1 «DLL полученная IP-адресация», в настоящем стандарте.

7.2.3 UDP/IPv4 сжатый заголовок

UDP/IPv4 сжатый заголовок находится в первом блоке продолжения данных, а его структура приведена в таблице 7.14.

Таблица 7.14 – UDP/IPv4 сжатый заголовок

Информационный элемент	Длина	Примечание
IPv4 идентификация	16	Значение «IPv4 идентификация» в заголовке
ID IP-адреса источника (SAID)	4	Индекс IP-адреса источника
ID IP-адреса назначения (DAID)	4	Индекс IP-адреса назначения
Opcode 1 сжатого заголовка	1	MSB opcode сжатого заголовка
ID порта источника UDP (SPID)	7	Индекс порта источника UDP
Opcode 2 сжатого заголовка	1	LSB opcode сжатого заголовка
ID порта назначения UDP (DPID)	7	Индекс порта назначения UDP
Расширенный заголовок 1 (номер порта UDP)	16	Необязательное (см. примечание)
Расширенный заголовок 2 (номер порта UDP)	16	Необязательное (см. примечание)
Примечание – Если расширенные заголовки не используются, эти поля занимают данные полезной нагрузки.		

7.2.4 Информационные элементы UDP/IPv4 сжатого заголовка

7.2.4.1 ID IP-адреса источника (SAID) (Source IP Address ID)

Информационный элемент SAID является индексом к предварительно сконфигурированному IP-адресу источника ID сети, как описано в таблице 7.15.

Таблица 7.15 – Информационный элемент ID IP-адреса источника (SAID)

Информационный элемент	Длина	Значение	Примечание
Source IP Address ID	4	0000_2	Радиосеть
		0001_2	Сеть USB (Ethernet интерфейс)
		$0010_2 – 1011_2$	Зарезервированные
		$1100_2 – 1111_2$	Выбирается изготовителем (см. примечание)
Примечание – SAID, связанный с IP адресом источника, должен быть в настройках MS			

7.2.4.2 ID IP-адреса назначения (DAID) (Destination IP Address ID)

Информационный элемент DAID является индексом к предварительно сконфигурированному IP-адресу назначения ID сети, как описано в таблице 7.16.

Таблица 7.16 – Информационный элемент ID IP-адреса назначения (DAID)

Информационный элемент	Длина	Значение	Примечание
Destination IP Address ID	4	0000_2	Радиосеть
		0001_2	Сеть USB (Ethernet интерфейс)
		0010_2	Сеть группы
		$0011_2 – 1011_2$	Зарезервированные
		$1100_2 – 1111_2$	Выбирается изготовителем (см. примечание)
Примечание – DAID, связанный с IP адресом назначения, должен быть в настройках MS			

7.2.4.3 ID порта источника UDP (SPID) (UDP Source Port ID)

Информационный элемент SPID является индексом к предварительно сконфигурированному номеру порта источника UDP, как описано в таблице 7.17.

Таблица 7.17 – Информационный элемент UDP Source Port ID (SPID)

Информационный элемент	Длина	Значение	Номер порта UDP	Примечание
UDP Source Port ID	7	0000000_2	NA	В расширенном заголовке
		0000001_2	5016	Текстовое сообщение UTF-16BE (см. примечание 1)
		0000010_2	5017	Протокол локального интерфейса (см. примечание 1)
		$0000011_2 – 1011110_2$	NA	Зарезервированные
		$1011111_2 – 1111111_2$	настраиваемый	Выбирается изготовителем (см. примечание 2)
Примечания: 1 Номер порта UDP присваивается по умолчанию, при использовании внутри сети радиосвязи. 2 SPID связан с портом источника UDP и должен быть настраиваемым в MS.				

7.2.4.4 ID порта назначения UDP (UDP Destination Port ID)

Информационный элемент DPID является индексом в составе предварительно определенного IP адреса назначения, как описано в таблице 7.18.

Таблица 7.18 – Информационный элемент UDP Destination Port ID (DPID)

Информационный элемент	Длина	Значение	Номер порта UDP	Примечание
UDP Destination Port ID	7	0000000_2	NA	В расширенном заголовке
		0000001_2	5016	Текстовое сообщение UTF-16BE (см. примечание 1)
		0000010_2	5017	Протокол локального интерфейса (см. примечание 1)
		$0000011_2 – 1011110_2$	NA	Зарезервированные
		$1011111_2 – 1111111_2$	настраиваемый	Выбирается изготовителем (см. примечание 2)
Примечания: 1 Номер порта UDP присваивается по умолчанию, при использовании внутри сети радиосвязи. 2 SPID связан с портом источника UDP и должен быть настраиваемым в MS.				

7.2.4.5 Опкод сжатого заголовка (Header Compression Opcode)

Информационный элемент Опкод Сжатого Заголовка идентифицирует формат сжатого заголовка, как описано в таблице 7.19.

Таблица 7.19 – Информационный элемент «Header Compression Opcode»

Информационный элемент	Длина	Значение	Примечание
Header Compression Opcode	2	00_2	UDP/IPv4 сжатый заголовок
		Все другие	Зарезервированные

7.2.4.6 Расширенный заголовок 1 (Extended Header 1)

Информационный элемент Extended Header 1 должен быть включен только в UDP/IPv4 сжатый заголовок, как описано в таблице 7.20.

Таблица 7.20 – Информационный элемент «Extended Header 1»

Информационный элемент	Длина	Значение	Примечание
Extended Header 1	16	Все значения	Номер порта UDP (см. прим.)
Примечания: 1 Если SPID = 0000000_2, то расширенный заголовок 1 является номером порта источника UDP. 2 Если SPID ≠ 0000000_2, а DPID = 0000000_2, то расширенный заголовок 1 является номером порта назначения UDP. 3 Если SPID ≠ 0000000_2, и DPID ≠ 0000000_2, то информационный элемент расширенный заголовок 1 не используется и он заменяется приложенными данными.			

7.2.4.7 Расширенный заголовок 2 (Extended Header 2)

Информационный элемент Extended Header 2 должен быть включен только в UDP/IPv4 сжатый заголовок, как описано в таблице 7.21.

Таблица 7.21 – Информационный элемент «Extended Header 2»

Информационный элемент	Длина	Значение	Примечание
Extended Header 2	16	Все значения	Номер порта UDP (см. прим.)
Примечания: 1 Если SPID = 0000000_2 и DPID = 0000000_2, то поле «расширенный заголовок 2» является номером порта назначения UDP. 2 Если условие в примечании 1 не выполняется, то информационный элемент расширенный заголовок 2 не используется и он заменяется приложенными данными.			

Приложение А
(обязательное)

Таймеры и константы PDP в DMR

В настоящем приложении перечислены таймеры, применяемые в MS DMR при передаче PDP.

Там, где указано, значение должно быть выбрано по модели MS/BS из диапазона ее внутренних значений. Для других таймеров и констант, значение может быть задано по умолчанию и значение этих таймеров и констант должны быть настраиваемыми внутри объекта DMR (MS или BS).

А.1 Таймеры уровня 2

T_DataTxLmt – Data Transmission Limit. Таймер устанавливает предел времени, отведенный для передачи данных.

Значение выбирается в зависимости от модели MS.

Рекомендуемое максимальное значение – 60 с.

Примечание – T_Data xLmt устанавливает время, в течение которого MS будет пытаться передать сообщение с неподтвержденными данными, или передать сообщение с подтвержденными данными и получить ответ.

T_RspnsWait – Confirmed Data Response Wait Limit. Таймер устанавливает предел времени ожидания ответа о получении подтвержденных данных.

Значение выбирается в зависимости от модели MS.

Рекомендуемое значение – 180 мс.

Рекомендуемое минимальное значение (для simulcast systems?) – 2 с.

Примечание – T_RspnsWait устанавливает время, в течение которого MS будет ждать приема ответа заголовка пакета с подтверждением передачи данных.

T_Holdoff – Random Holdoff Time. Таймер устанавливает предел «отложенного» времени, значение которого выбирается случайным образом.

Диапазон выбирается в зависимости от модели MS.

MS случайным образом генерирует длительность таймера в диапазоне

Минимальное значение = TBD.

Рекомендуемое максимальное значение – 2 с. (для неподтвержденных данных).

Рекомендуемое максимальное значение – 2 с. (для подтвержденных данных).

Примечание – T_Holdoff используется для минимизации коллизий, когда сообщения с данными стоят в очереди, и канал становится свободным.

T_DataHngtime – Data Hangtime.

Значение выбирается в зависимости от модели BS.

Рекомендуемое значение – 180 мс (3 трафиковых пакета)

Примечание – T_DataHngtime устанавливает время, в течение которого BS будет передавать Терминатор установления соединения для передачи данных (TD_LC) PDUs с целью резервирования канала для ответа подтвержденных данных.

А.2 Константы уровня 2

N_RtryLmt – Data Air Interface Retry Limit. Предел числа повторов передачи данных по радиоинтерфейсу.

Значение выбирается в зависимости от модели MS.

Рекомендуемое максимальное значение – 8.

Примечание – N_RtryLmt это максимальное число повторов, когда DLL будет передавать и пытаться получить ответ о передаче подтвержденных данных от принимающей MS.

Приложение В
(обязательное)

Списки ссылочного опкода

В настоящем приложении перечислены следующие опкоды, используемые в PDP DMR:
- опкоды полного управления соединением.

В.1 Опкод полного управления соединением PDP

В таблице В.1 показан код FLCO

Таблица В.1

FLCO	Описание	Обозначение
110000_2	Terminator Data Link Control Терминатор управления соединением для передачи данных	TD_LC

Приложение С
(справочное)

Передача IPv6 данных по PDP

Данное приложение показывает некоторые стратегии и дает некоторые ссылки на то, как IPv6 пакеты могут быть переданы в Протоколе Пакетных Данных DMR, который разработан для передачи IPv4 пакетов.

С.1 IPv6 адресация

IPv6 – это новое поколение протокола Интернет. Детальное описание протокола IPv6 представлено в RFC 2460 [8], «Internet Protocol, Version 6 (IPv6) Specification».

В IPv6 IP адрес имеет длину 128 бит. Существует три типа адресов:

- Unicast (юникаст). Идентификатор единичного сетевого интерфейса. Пакет, отправленный на unicast адрес, доставляется интерфейсу, идентифицированному как этот адрес;
- Anycast (эникаст). Идентификатор для набора сетевых интерфейсов (обычно принадлежащих разным оконечным узлам). Пакет, отправленный на anycast адрес, доставляется одному из интерфейсов, идентифицированных как этот адрес (ближайшему первому в соответствии с протоколом маршрутизации как мера от расстояния);
- Multicast (мультикаст). Идентификатор для набора сетевых интерфейсов (обычно принадлежащих разным узлам). Пакет, отправленный на multicast адрес, доставляется всем интерфейсам идентифицированным как этот адрес.

В рамках этого приложения рассматриваются только Unicast адреса. Unicast адрес имеет длину 128 бит и может быть разбит на несколько полей. IPv6 адреса записываются в шестнадцатеричном формате, как показано ниже.

Неопределенный адрес: 00000000_{16}.

Примечание – Неопределенный адрес обозначает отсутствие адреса.

Петлевой адрес: 00000001_{16}.

Примечание – петлевой адрес может использоваться узлом для отправки IPv6 пакетов самому себе.

Общая схема адресации Global Unicast представлена в таблице С.1.

Таблица С.1 – Схема адресации Global Unicast

n bits	m bits	128-n-m bits
Приставка глобальной маршрутизации	ID подсети	ID интерфейса

Механизмы передачи IPv6 включают в себя технологию для узлов и маршрутизаторов для динамического тунеллирования IPv6 пакетов в инфраструктуре маршрутизаторов IPv4 сети. Узлам IPv6 которые используют данную технологию присваиваются специальные IPv6 Unicast адреса, которые несут в себе глобальные IPv4 32-битные адреса в нижних разрядах. Данный тип адресов называется термином «IPv4-совместимые с IPv6 адреса» и представлены в таблице С.2.

Таблица С.2 – IPv4 совместимые с IPv6 адреса

80 bits (10 bytes)					**16 bits**	**32 bits**
00 00	00 00	00 00	00 00	00 00	00 00	IPv4 адрес

Также определен второй тип IPv6 адресов, который содержит встроенный IPv4 адрес. Этот тип адреса используется для представления IPv4 адресов узлов в виде IPv6. Данный тип адреса называется термином «IPv4-сопоставимый с IPv6 адресом» и представлен в таблице С.3.

Таблица С.3 – IPv4 сопоставимый с IPv6 адресом

80 bits (10 bytes)					16 bits	32 bits
00 00	00 00	00 00	00 00	00 00	FF FF	IPv4 адрес

С.2 Сопоставление адресов передаваемых по PDP

Существует две возможные стратегии, позволяющие передавать IPv6 пакеты по Протоколу Передачи Пакетов PDP DMR:

- прямое сопоставление IPv6 пакета внутри пакета подтвержденных или неподтвержденных данных протокола DMR;
- передача IPv6 пакета с использованием одной из технологий туннелирования IPv6 в IPv4.

Прямое сопоставление IPv6 пакетов на пакеты одного из двух сервисов «bearer services» передачи данных может быть возможно с использованием специального значения SAP в Data Fragment Header (Заголовке Фрагмента Данных). При использовании данного подхода излишние сложности сведены к минимуму, а разница между IPv4 и IPv6 пакетами в заголовке IPv6 больше на 20 байт. В IPv6 не требуется процедура ARP, потому что IPv6 адреса включают в себя MAC адрес. Данный подход не описан в этом справочном приложении настоящего стандарта.

С.3 Технологии туннелирования IPv6

Описаны различные технологии туннелирования IPv6 в IPv4. Подробности описания могут быть найдены в следующих документах:

- RFC 2529 [9] "Transmission of IPv6 over IPv4 Domains without Explicit Tunnels";
- RFC 3056 [10] "Connection of IPv6 Domains via IPv4 Clouds";
- RFC 3142 [11] "An IPv6-to-IPv4 Transport Relay Translator";
- RFC 4213 [12] "Transition Mechanisms for IPv6 Hosts and Routers".

Данные различные решения используют некоторое сопоставление между IPv4 и IPv6 адресами. В частности хорошее описание данных различных сценариев (случаи использования) представлено в RFC 4213 [12].

Механизмы, описанные в RFC 4213 [12] включают:

- двойной IP слой (Dual IP layer), также известный как Двойной Стэк (Dual Stack). Технология, предоставляющая полную поддержку для обоих интернет протоколов (IPv4 и IPv6) для хостов и маршрутизаторов;
- настраиваемое туннелирование IPv6 через IPv4 (Configured tunnelling of IPv6 over IPv4). Туннели «точка-точка» созданные с помощью вложения IPv6 пакетов внутри IPv4 заголовков для передачи их по маршрутной инфраструктуре IPv4;
- IPv4 совместимый с IPv6 адрес (IPv4-compatible IPv6 addresses). Формат IPv6 адреса, который использует встроенный в себя IPv4 адрес;
- автоматическое туннелирование IPv6 через IPv4 (Automatic tunnelling of IPv6 over IPv4). Механизм для использования IPv4-совместимых IPv6 адресов для автоматического туннелирования IPv6 пакетов по IPv4 сетям.

Возможны две различных конфигурации MS DMR, как показано на рисунках С.1 и С.2.

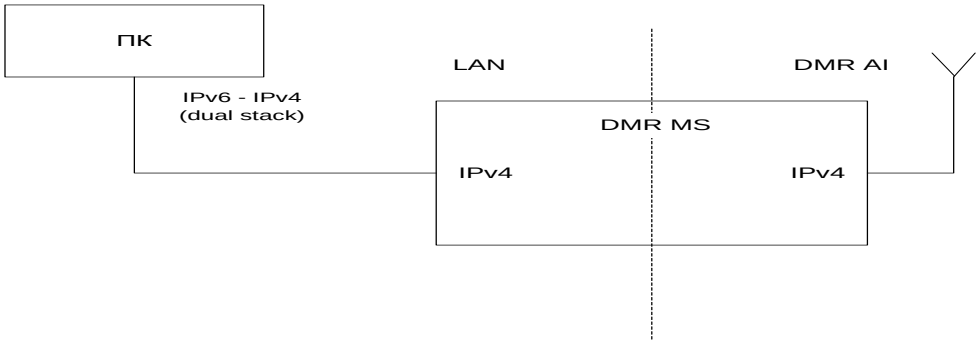

Рисунок С.1 – DMR соединение по IPv4

На рисунке С.1 показана конфигурация подключения MS DMR к интерфейсу LAN IPv4.

При использовании данной конфигурации, туннелирование управляется напрямую хостом (ПК), соединенным с MS DMR. Данный хост может использовать как автоматическое туннелирование так и настраиваемое туннелирование, как описано ниже.

Случай 1а. Если источник и хост назначения имеют IPv4-совместимые через IPv6 адреса, автоматическое туннелирование изначально передается в IPv4 сетевой DMR интерфейс и маршрутизация

пакета выполняется ARP по DMR процедуре. На практике, автоматическое туннелирование разрешает прямую связь мобильного хоста с другим мобильным хостом внутри IPv6 хоста по маршрутизационной инфраструктуре IPv4.

Случай 1б. Если хост источника или хост назначения не имеют IPv4-совместимых через IPv6 адресов, тогда единственная возможность это использовать настраиваемое туннелирование. В этом случае хост источника знает, что существует IPv4 тунель между его сетевым интерфейсом и другим сетевым интерфейсом другого устройства, которое может маршрутизировать IPv6 пакет на хост назначения. На практике данный настроенный тунель прокладывается от мобильного хоста к центру переключения, где есть IPv6 маршрутизатор. В данном случае не существует возможности иметь прямую связь мобильного хоста с мобильным хостом внутри IPv6 хоста.

На рисунке С.2 показана конфигурация соединения MS DMR с IPv6 LAN интерфейсом.

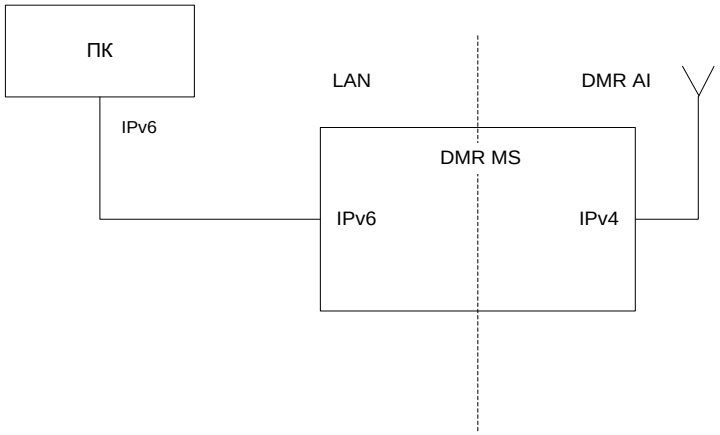

Рисунок С.2 – DMR соединение по IPv6

При использовании данной конфигурации, туннелированием управляет каждая MS DMR, которая имеет подключенное IPv6-совместимое устройство. MS DMR может использовать как автоматическое, так и настаиваемое туннелирование, в зависимости от типа IPv6 адресов, используемых хостами источника и назначения.

Случай 2а. Если источник и хост назначения обладают IPv4-совместимыми через IPv6 адресами, автоматическое туннелирование изначально передается в IPv4 сетевой DMR интерфейс и маршрутизация пакета выполняется ARP по DMR процедуре. На практике автоматическое туннелирование разрешает прямую связь мобильного хоста с другим мобильным хостом внутри IPv6 хоста по маршрутизационной инфраструктуре IPv4.

Случай 2б Если хост источника или хост назначения не имеют IPv4-совместимых через IPv6 адресов, тогда единственная возможность это использовать настраиваемое туннелирование. В этом случае MS DMR знает что существует IPv4 туннель между ее IPv4 сетевым интерфейсом и другим сетевым интерфейсом другого устройства, которое может маршрутизировать IPv6 пакет на хост назначения. На практике данный настроенный туннель прокладывается от MS DMR к центру переключения, где есть IPv6 маршрутизатор. В данном случае не существует возможности иметь прямую связь мобильного хоста с мобильным хостом внутри IPv6 хоста.

Приложение D
(справочное)

Запросы на изменение

Запросы на изменение изложены в ETSI TS 102 361-3 (таблица D.1).

Приложение Д.А

(справочное)

Таблица Д.А.1 – сведения о соответствии государственных стандартов ссылочным международным стандартам (международным документам)

Обозначение и наименование международного стандарта (международного документа)	Степень соответствия	Обозначение и наименование государственного стандарта
ETSI TS 102 361-1:2016 Электромагнитная совместимость и спектр радиочастот (ERM). Системы цифровой подвижной радиосвязи (DMR). Часть 1. DMR протокол радиоинтерфейса	IDT	СТБ ETSI TS 102 361-1 Электромагнитная совместимость и спектр радиочастот (ERM). Системы цифровой подвижной радиосвязи (DMR). Часть 1. DMR протокол радиоинтерфейса
ETSI TS 102 361-2:2016 Электромагнитная совместимость и спектр радиочастот (ERM). Системы цифровой подвижной радиосвязи (DMR). Часть 2. Речевые и общие услуги и функциональные возможности DMR. Основные услуги и возможности	IDT	СТБ ETSI TS 102 361-2 Электромагнитная совместимость и спектр радиочастот (ERM). Системы цифровой подвижной радиосвязи (DMR). Часть 2. Речевые и общие услуги и функциональные возможности DMR.
ETSI TS 102 361-4:2016 «Электромагнитная совместимость и спектр радиочастот (ERM). Системы цифровой подвижной радиосвязи (DMR). Часть 4. DMR протокол транкинговый	IDT	СТБ ETSI TS 102 361-4 «Электромагнитная совместимость и спектр радиочастот (ERM). Системы цифровой подвижной радиосвязи (DMR). Часть 4. DMR протокол транкинговый

Приложение Е
(справочное)

Библиография

[1] ETSI TR 102 335-1 "Electromagnetic compatibility and Radio spectrum Matters (ERM); System reference document for harmonized use of Digital Mobile Radio (DMR); Part 1: Tier 1 DMR#, expected to be for general authorization with no individual rights operation"
(Электромагнитная совместимость и спектр радиочастот (ERM). Справочная система документов для гармонизированного использования цифрового подвижного радио (DMR). Часть 1. Уровень1. DMR #, как ожидается, будет для общего разрешения, без каких-либо операций по индивидуальным правам.)

[2] ETSI TR 102 335-2 "Electromagnetic compatibility and Radio spectrum Matters (ERM); System reference document for harmonized use of Digital Mobile Radio (DMR); Part 2: Systems operating under individual licences in the existing land mobile service spectrum bands"
(Электромагнитная совместимость и спектр радиочастот (ERM). Справочная система документов для гармонизированного использования цифрового подвижного радио (DMR). Часть 2. Системы, работающие по индивидуальным лицензиям в существующих полосах спектра сухопутной подвижной службы.)

Исполнители

Директор ОАО «Гипросвязь»	С.В.Новиков
Заместитель директора по науке и развитию ОАО «Гипросвязь»	В.М.Ивашко
Начальник НИИЛ ЭМИ НИИЦ ОАО «Гипросвязь»	О.Е.Смолярко
Заведующий сектором НИИЛ СУС НИИЦ ОАО «Гипросвязь»	С.Н.Бендь