Internet Engineering Task Force (IETF)
Request for Comments: 8928
Updates: 8505
Category: Standards Track
ISSN: 2070-1721

P. Thubert, Ed.
Cisco
B. Sarikaya

M. Sethi
Ericsson
R. Struik
Struik Security Consultancy

November 2020

# Address-Protected Neighbor Discovery for Low-Power and Lossy Networks

Обнаружение соседей с защитой адресов в сетях LLN

**Аннотация**

Этот документ обновляет протокол обнаружения соседей 6LoWPAN[1] ND (Neighbor Discovery), определённый в RFC 6775 и RFC 8505. Новое расширение названо обнаружением соседей с защитой адресов (Address-Protected Neighbor Discovery или AP-ND) и обеспечивает владельцев адресов от их кражи и атак с подменой (impersonation) в сетях LLN[2]. Узлы, поддерживающие это расширение рассчитывают криптографический идентификатор (Crypto-ID) и применяют его с одним или несколькими зарегистрированными адресами (RA). Crypto-ID указывает владельца RA и может служить доказательством владения адресами. Когда адрес зарегистрирован с Crypto-ID и владение подтверждено, регистрационные данные может менять лишь владелец адреса, что обеспечивает проверку адресов отправителей (Source Address Validation).

**Статус документа**

Документ относится к категории Internet Standards Track.

Документ является результатом работы IETF[3] и представляет согласованный взгляд сообщества IETF. Документ прошёл открытое обсуждение и был одобрен для публикации IESG[4]. Дополнительную информацию о стандартах Internet можно найти в разделе 2 в RFC 7841.

Информацию о текущем статусе документа, ошибках и способах обратной связи можно найти по ссылке https://www.rfc-editor.org/info/rfc8928.



# Оглавление



[1] IPv6 over Low-Power Wireless Personal Area Network - IPv6 в персональных беспроводных сетях со слабым питанием.
[2] Low-Power and Lossy Network - сеть со слабым питанием и потерями.
[3] Internet Engineering Task Force - комиссия по решению инженерных задач Internet.
[4] Internet Engineering Steering Group - комиссия по инженерным разработкам Internet.

# *1. Введение*

Оптимизация обнаружения соседей для сетей 6LoWPAN (6LoWPAN ND) [RFC6775] приспосабливает исходные протоколы обнаружения соседей IPv6, определённые в [RFC4861] и [RFC4862], к сетям LLN. В частности, 6LoWPAN ND добавляет механизм регистрации адреса хоста с использованием индивидуальной адресации, снижающий уровень группового трафика по сравнению с механизмом DAD[1] в IPv6 ND. 6LoWPAN ND определяет новую опцию регистрации адресов (Address Registration Option или ARO), передаваемую в индивидуальных сообщениях предложения соседства (Neighbor Solicitation или NS) и анонсирования соседа (Neighbor Advertisement или NA), передаваемых между узлом 6LoWPAN Node (6LN) и маршрутизатором 6LoWPAN Router (6LR). Определены также сообщения запроса о дубликатах адресов (Duplicate Address Request или DAR) и подтверждения дубликатов (Duplicate Address Confirmation или DAC) между 6LR и граничным маршрутизатором 6LoWPAN (6LBR). В сетях LLN маршрутизатор 6LBR является центральным хранилищем всех зарегистрированных адресов своего домена.

Механизм регистрации в «Neighbor Discovery Optimization for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)» [RFC6775] предотвращает использование адресов, уже зарегистрированных в подсети (первым пришел - первого обслужили). Для проверки владения адресами в «Registration Extensions for IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) Neighbor Discovery» [RFC8505] задано поле Registration Ownership Verifier (ROVR). [RFC8505] позволяет узлам 6LR и 6LBR проверять связь между RA узла и его ROVR. Значение ROVR может выводиться из адреса устройства на канальном уровне (с использованием 64-битового формата адресов EUI-64[2], заданного IEEE). Однако адрес EUI-64 можно подменить, поэтому узел, подключенный к подсети и знающий сопоставления зарегистрированного адреса с ROVR может подделать ROVR. Это позволяет атакующему украсть адрес и перенаправить трафик для него. В [RFC8505] определена опция расширенной регистрации адресов (Extended Address Registration Option или EARO), доставляющая другую форму ROVR и являющуюся обязательным условием для использования этой спецификации.

В соответствии с этой спецификацией 6LN генерирует криптографический идентификатор (Crypto-ID) и помещает его в поле ROVR в процессе регистрации одного или нескольких своих адресов на маршрутизаторах 6LR. Подтверждение владения Crypto-ID передаётся в первом регистрационном обмене с новым 6LR и навязывает его 6LR. Узел 6LR проверяет владение Crypto-ID до создания нового состояния регистрации или изменения имеющихся данных.

Предложенный в этом документе протокол защищённой регистрации адресов обеспечивает такие же концептуальные преимущества как улучшенная проверка адреса отправителя (Source Address Validation Improvement или SAVI) [RFC7039] в том, что лишь владелец адреса IPv6 может передавать пакеты с этого адреса. В отличие от [RFC7039], основанного на протоколах слежки (snooping), предлагаемая этим документом защита основана на состоянии, которое устанавливается и поддерживается в сети владельцем адреса. На основе этой спецификации 6LN может использовать 6LR для пересылки пакета IPv6 лишь в том случае, когда он зарегистрировал адрес, используемый в поле отправителя пакета, на данном маршрутизаторе 6LR.

С уровнем адаптации 6LoWPAN [RFC4944] и [RFC6282] узел 6LN может обеспечить лучшее сжатие адреса IPv6, используя идентификатор Interface ID (IID), выводимый из адреса L2. Такое сжатие не совместимо с «SEcure Neighbor Discovery (SEND)» [RFC3971] и «Cryptographically Generated Addresses (CGAs)» [RFC3972], поскольку они выводят IID из криптографического ключа. Эта спецификация отделяет создание IID от криптографических расчётов и обеспечивает большее сжатие.

# *2. Терминология*

## 2.1. Уровни требований

Ключевые слова **необходимо** (MUST), **недопустимо** (MUST NOT), **требуется** (REQUIRED), **нужно** (SHALL), **не следует** (SHALL NOT), **следует** (SHOULD), **не нужно** (SHOULD NOT), **рекомендуется** (RECOMMENDED), **не рекомендуется** (NOT RECOMMENDED), **возможно** (MAY), **необязательно** (OPTIONAL) в данном документе интерпретируются в соответствии с BCP 14 [RFC2119] [RFC8174] тогда и только тогда, когда они выделены шрифтом, как показано здесь.

[1]Duplicate Address Detection - обнаружение дубликатов адресов.
[2]Extended Unique Identifier - расширенный уникальный идентификатор.

## 2.2. Основы

Читателю будет полезно ознакомиться с перечисленными ниже документами для лучшего понимания спецификации.

- «SEcure Neighbor Discovery (SEND)» [RFC3971].
- «Cryptographically Generated Addresses (CGA)» [RFC3972].
- «Neighbor Discovery for IP version 6 (IPv6)» [RFC4861].
- «IPv6 Stateless Address Autoconfiguration» [RFC4862].
- «IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals» [RFC4919].

## 2.3. Сокращения

***6BBR***
6LoWPAN Backbone Router – магистральный маршрутизатор 6LoWPAN.

***6LBR***
6LoWPAN Border Router - граничный маршрутизатор 6LoWPAN.

***6LN***
6LoWPAN Node - узел 6LoWPAN (хост или маршрутизатор с ограниченным питанием).

***6LR***
6LoWPAN Router - маршрутизатор 6LoWPAN.

***AP-ND***
Address-Protected Neighbor Discovery - обнаружение соседей с защитой адреса.

***CGA***
Cryptographically Generated Address - криптографически сгенерированный адрес.

***DAD***
Duplicate Address Detection - обнаружение дубликатов адресов.

***EARO***
Extended Address Registration Option - расширенная опция регистрации адреса.

***ECC***
Elliptic Curve Cryptography - криптография на основе эллиптических кривых.

***ECDH***
Elliptic Curve Diffie-Hellman - алгоритм Diffie-Hellman с эллиптическими кривыми.

***ECDSA***
Elliptic Curve Digital Signature Algorithm - алгоритм цифровой подписи с эллиптическими кривыми.

***EDAC***
Extended Duplicate Address Confirmation - расширенное подтверждение дубликата адреса.

***EDAR***
Extended Duplicate Address Request - расширенный запрос о дубликатах адреса.

***CIPO***
Crypto-ID Parameters Option - опция параметров Crypto-ID.

***LLN***
Low-Power and Lossy Network - сеть со слабым питанием и потерями.

***NA***
Neighbor Advertisement - анонсирование соседа.

***ND***
Neighbor Discovery - обнаружение соседей.

***NDP***
Neighbor Discovery Protocol - протокол обнаружения соседей.

***NDPSO***
Neighbor Discovery Protocol Signature Option - опция подписи протокола обнаружения соседей.

***NS***
Neighbor Solicitation - предложение соседства.

***ROVR***
Registration Ownership Verifier - проверка регистрации владения.

***RA***
Router Advertisement - анонсирование маршрутизатора.

***RS***
Router Solicitation - предложение маршрутизатора.

***RSAO***
RSA Signature Option - опция подписи RSA.

***SHA***
Secure Hash Algorithm - алгоритм защищённого хэширования.

***SLAAC***
Stateless Address Autoconfiguration - автоматическая настройка адреса без учёта состояния.

***TID***
Transaction ID - идентификатор транзакции (счётчик в EARO).

# *3. Обновление RFC 8505*

В параграфе 5.3 [RFC8505] введён элемент проверки владения адресом ROVR, служащий для обнаружения и отклонения дублирующих регистраций в процессе DAD. ROVR является базовым элементом, разработанным с учётом совместимости с имеющимися механизмами и поддержки в будущем новых методов расчёта. Данная спецификация **рекомендует** применять метод Crypto-ID. В параграфе 7.5 описаны конфликты, которые могут возникать при использовании в сети разнородных полей ROVR.

Эта спецификация вводит новый идентификатор Crypto-ID, передаваемый в поле ROVR и служащий для косвенного доказательства владения адресом, которое зарегистрировано с помощью [RFC8505]. Crypto-ID выводится из открытого криптографического ключа и дополнительных параметров.

Общий механизм требует поддержки криптографии с эллиптическими кривыми (Elliptic Curve Cryptography или ECC) и хэш-функции, как описано в параграфе 6.2. Для включения проверки владения регистрирующий узел должен предоставить некоторые параметры, включающие одноразовое значение (nonce) и подпись, подтверждающую владение узла секретным ключом, соответствующим открытому ключу, использованному для создания Crypto-ID.

Эта спецификация использует эллиптические кривые и хэш-функции, указанные в таблице 1, а в будущем могут быть добавлены новые с соответствующей регистрацией в IANA. Криптографические алгоритмы (включая кривые и соглашения о представлении) указываются полем Crypto-Type в новой опции криптопараметров (IPv6 ND Crypto-ID Parameters Option или CIPO), описанной в параграфе 4.3 и включающей параметры, требуемые для проверки адреса. Документ также задаёт новую опцию NDP Signature (параграф 4.4) для передачи результирующей подписи. Опция Nonce [RFC3971] добавляется в NA(EARO) для запроса проверки и все три опции нужны в NS(EARO) для проверки.

# *4. Новые поля и опции*

## 4.1. Crypto-ID

Значение Crypto-ID передаётся в поле ROVR опции EARO и запросе расширенной проверки дубликатов (Extended Duplicate Address Request или EDAR) и связано с зарегистрированным адресом (RA) на 6LR и 6LBR. Владение Crypto-ID может быть продемонстрировано с помощью криптографических механизмов и путём связывания может подтверждать владение RA.

Узлу с требуемыми криптографическими примитивами **следует** по умолчанию применять Crypto-ID в качестве ROVR для своих регистрация. Использование в ROVR идентификатора Crypto-ID указывается новым флагом C в опции EARO сообщения NS(EARO).

Crypto-ID выводится из открытого ключа и модификатора, как показано ниже.

1. К CIPO применяется хэш-функция используемая схемой подписи и указанная Crypto-Type (таблица 1). Все резервные поля и поля заполнения **должны** иметь значение 0.
2. В качестве Crypto-ID используется нужное число битов полученного хэш-значения, начиная слева.

В момент создания этого документа **рекомендовался** минимальный размер Crypto-ID 128 битов, если не нужна совместимость с [RFC8505] (в этом случае не меньше 64 битов). Размер Crypto-ID очевидно вырастет в будущем.

## 4.2. Обновлённая опция EARO

Эта спецификация обновляет опцию EARO для передачи в поле ROVR значения Crypto-ID (рисунок 1).

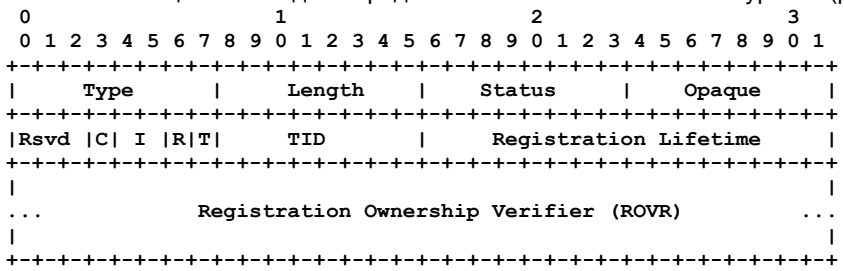


*Рисунок 1. Опция расширенной регистрации адреса.*

***Type***
33

***Length***
Определено в [RFC8505] и копируется в поле EARO Length связанной опции CIPO.

***Status***
Определено в [RFC8505].

***Opaque***
Определено в [RFC8505].

***Rsvd (Reserved)***
3-битовое целое число без знака. При передаче **должно** устанавливаться в 0, а при получении **должно** игнорироваться.

***C***
Флаг, указывающий размещение в поле ROVR идентификатора Crypto-ID и то, что для 6LN **может** быть проверено владение адресом, как описано в этом документе.

***I, R, T***
Определено в [RFC8505].

***TID and Registration Lifetime***
Определено в [RFC8505].

***Registration Ownership Verifier (ROVR)***
При установленном флаге C это поле содержит Crypto-ID.

В этой спецификации используются коды состояния Validation Requested (запрошена проверка) и Validation Failed (отказ при проверке), определённые в [RFC8505]. Новых кодов состояния эта спецификация не определяет.

## 4.3. Опция параметров Crypto-ID

Эта спецификация определяет опцию CIPO, содержащую параметры, используемые для создания Crypto-ID.

Для обеспечения криптографической гибкости [BCP201], спецификация поддерживает различные схемы подписи на основе эллиптических кривых, указываемые в поле Crypto-Type:

- ECDSA256 использует ECDSA с кривой NIST P-256 [FIPS186-4] и хэш-функцию SHA-256 [RFC6234]; схема **должна** поддерживаться всеми реализациями;
- Ed25519 использует алгоритм Pure Edwards-Curve Digital Signature (PureEdDSA) [RFC8032] со скрученной кривой Эдвардса Edwards25519 [RFC7748] и хэш-функцию SHA-512 [RFC6234]; реализации **могут** поддерживать эту схему как вариант;
- ECDSA25519 использует ECDSA [FIPS186-4] с кривой Вейерштрасса Wei25519 (Приложение B.4) и хэш-функцию SHA-256 [RFC6234]; реализации **могут** поддерживать эту схему.

Используемые в спецификации схемы подписи имеют близкие параметры криптостойкости, но основаны на разных кривых, хэш-функциях, алгоритмах подписи и соглашениях о представлении. В будущих спецификациях могут быть добавлены другие криптоалгоритмы и размеры ключей, например, для улучшения защитных свойств или упрощения реализации.

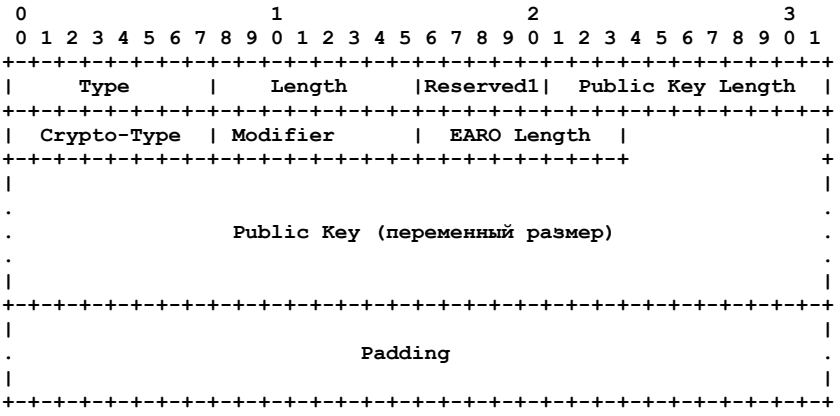


*Рисунок 2. Опция параметров Crypto-ID.*

***Type***
8-битовое целое число без знака, для которого агентство IANA выделило значение 39 (таблица 2).

***Length***
8-битовое целое число без знака, указывающее размер опции в 8-октетных блоках.

***Reserved1***
5-битовое целое число без знака. При передаче **должно** устанавливаться в 0, а при получении **должно** игнорироваться.

***Public Key Length***
11-битовое целое число без знака, указывающее размер поля Public Key в байтах. Фактический размер зависит от значения Crypto-Type и способа представления открытого ключа. Выделенные значения приведены в таблице 1).

***Crypto-Type***
8-битовое целое число без знака, указывающее криптоалгоритм для расчёта Crypto-ID индексом из субреестра IANA Crypto-Types в реестре Internet Control Message Protocol version 6 (ICMPv6) Parameters (параграф 8.2).

***Modifier***
8-битовое целое число без знака, указывающее произвольное значение, выбранное создателем Crypto-ID. Роль модификатора заключается в возможности создания нескольких Crypto-ID из одной пары ключей. Это снижает отслеживаемость, за счёт чего повышается приватность узла с ограничениями без наличия нескольких пар ключей.

***EARO Length***
8-битовое целое число без знака, указывающее размер опции EARO, содержащей идентификатор Crypto-ID, связанный с CIPO.

***Public Key***
Поле переменного размера, указанного в поле Public Key Length.

***Padding***
Поле переменного размера, дополняющее поле Public Key для выравнивания по 8-байтовой границе. Отправитель **должен** заполнять поле нулями, а получатель **должен** игнорировать это поле.

Реализация нескольких хэш-функций на устройстве с ограничениями может потребовать слишком много памяти. Эта спецификация разрешает применять одну хэш-функцию SHA-256 [RFC6234] для двух или трёх поддерживаемых схем подписи на основе ECC. При расчёте ECC возможна некоторая факторизация кода.

В [CURVE-REPR] приведены сведения о представлении кривых Монтгомери и скрученных кривых Эдвардса в краткой форме Вейерштрасса и показано, как это можно применить для реализации расчёта эллиптических кривых на основе имеющихся реализаций, которые уже представляют, например, ECDSA и ECDH с использованием простых кривых NIST [FIPS186-4]. Соглашения о представлении более подробно описаны в Приложении B.

## 4.4. Опция подписи NDP

Эта спецификация определяет опцию подписи NDP (NDP Signature Option или NDPSO). NDPSO содержит подпись, подтверждающую владение Crypto-ID и регистрацию адреса. Формат NDPSO показан на рисунке 3.

В отличие от опции RSA Signature (RSAO), определённой в параграфе 5.2 документа SEND [RFC3971], NDPSO не включает поле хэшированного ключа. Вместо этого используется 128 битов левой части поля ROVR опции EARO в качестве хэш-значения для отыскания опции CIPO, содержащей ключевой материал, используемый для проверки подписи, с заполнением слева при необходимости. Другим отличием является то, что NDPSO подписывает фиксированный набор полей, а не все опции, размещённые до неё в сообщении ND с подписью. Это позволяет опустить опцию CIPO, которая уже получена маршрутизатором 6LR, за счёт способности добавлять произвольные опции, которые будут подписаны с помощью RSAO.

Сообщение ND с опцией NDPSO **должно** иметь единственную опцию EARO, которая **должна** содержать Crypto-ID в поле ROVR, а значение Crypto-ID **должно** быть связано с ключевой парой, используемой для цифровой подписи в NDPSO.

Опция CIPO может включаться в одно сообщение с NDPSO. Если опция не указана там, её можно найти в абстрактной таблице, созданной предыдущим сообщением и индексированной хэшем.

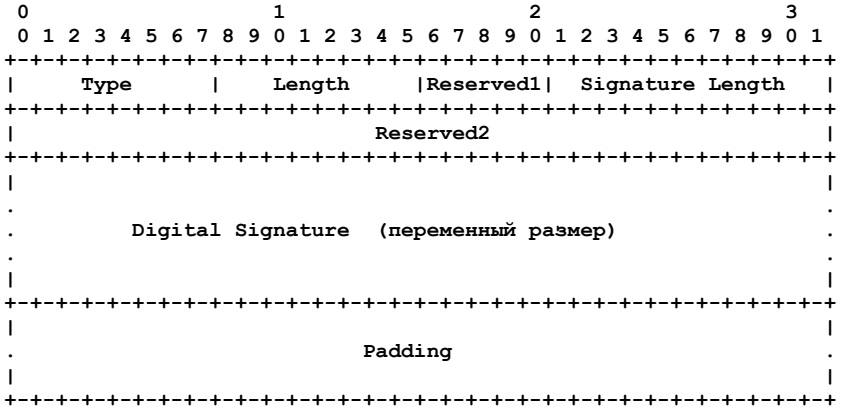


*Рисунок 3. Опция NDP Signature.*

***Type***
Выделенное IANA значение 40 (таблица 2).

***Length***
8-битовое целое число без знака, указывающее размер опции в 8-октетных блоках.

***Reserved1***
5-битовое целое число без знака. При передаче **должно** устанавливаться в 0, а при получении **должно** игнорироваться.

***Digital Signature Length***
11-битовое целое число без знака, указывающее размер поля Digital Signature в байтах.

***Reserved2***
32-битовое целое число без знака. При передаче **должно** устанавливаться в 0, а при получении **должно** игнорироваться.

***Digital Signature***
Поле переменного размера, содержащее цифровую подпись. Размер и способ расчёта цифровой подписи зависит от Crypto-Type, значение которого можно найти в опции CIPO (приложение B). Для значения Crypto-Type, заданный этой спецификацией и будущих значений Crypto-Type подпись рассчитывается в соответствии с параграфом 6.2, если явно не указано иное.

***Padding***
Поле переменного размера, дополняющее поле Digital Signature для выравнивания по 8-байтовой границе. Отправитель **должен** заполнять поле нулями, а получатель **должен** игнорировать это поле.

## 4.5. Расширения опции Capability Indication

Эта спецификация определяет новый бит возможности в опции 6LoWPAN Capability Indication (6CIO), определённой в [RFC7400], для использования маршрутизаторами 6LR и 6LBR в сообщениях IPv6 ND RA.

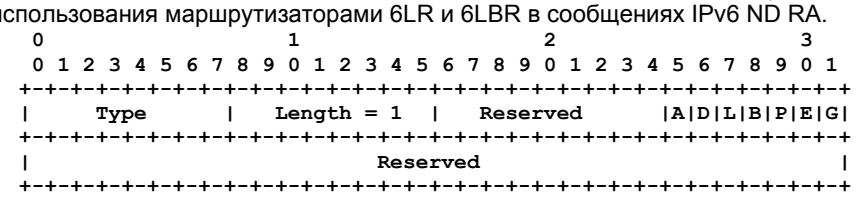


*Рисунок 4. Новый бит возможности в 6CIO.*

Новое поле обозначается символом A.

***A***
Флаг, указывающий глобальную активацию AP-ND в сети.

Флагом A управляет маршрутизатор 6LBR, обслуживающий сеть, и флаг распространяется маршрутизаторами 6LR. Флаг обычно устанавливается, если все 6LR перешли на поддержку этой спецификации.

# *5. Область действия протокола*

Описанный здесь протокол работает в 6LoWPAN LLN, которая обычно является оконечной сетью, подключённой к более крупной сети IP через граничный маршрутизатор 6LBR в соответствии с [RFC6775]. 6LBR имеет возможности выполнения требований DAD.

6LBR поддерживает состояние регистрации для всех устройств в подключённой сети LLN. Вместе с маршрутизатором первого интервала пересылки (6LR), узел 6LBR обеспечивает уникальность адресов и предоставляет право владения адресом IPv6 до начала его использования в LLN. Это отличается от традиционных сетей, основанных на автоматической настройке адресов IPv6 [RFC4862], где нет гарантии владения адресами от сети и каждый пакет IPv6 Neighbor Discovery должен защищаться индивидуально [RFC3971].

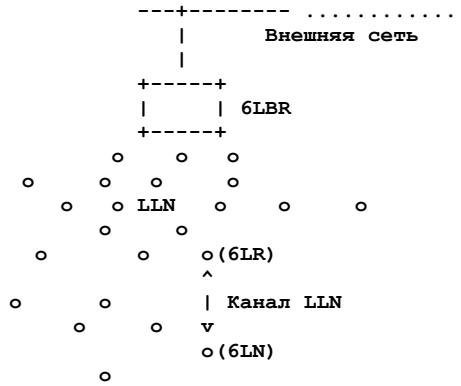


*Рисунок 5. Базовая конфигурация.*

В многосвязной (mesh) сети маршрутизаторы 6LR напрямую соединены с хостами. Эта спецификация требует развёртывания защиты на уровне L2, чтобы все пакеты от конкретного хоста были защищены. 6LR может быть отделён от 6LBR несколькими узлами пересылки. Пакеты маршрутизируются между 6LR и 6LBR через другие 6LR.

Эта спецификация требует защиты всех каналов LLN между 6LR и 6LBR, чтобы пакеты, проверенные первым 6LR, можно было безопасно маршрутизировать другим 6LR на пути к 6LBR.

# 6. Потоки протокола

Маршрутизаторы 6LR и 6LBR реализуют модель обслуживания в порядке очереди (first come, first served) путём сохранения значения ROVR, связанного с регистрируемым адресом при первой регистрации, и отвергая регистрацию с другим значением ROVR. Узел 6LN может заявить любой адрес, если он первым запросил этот адрес. После успешной регистрации узел 6LN становится владельцем RA и этот адрес привязывается к значению ROVR в реестре 6LR/6LBR.

Эта спецификация защищает владение адресом на первом узле пересылки (hop). Использование защиты указывается флагом A в 6CIO, который устанавливается маршрутизатором 6LBR и распространяется в неизменном виде маршрутизаторами 6LR. После обновления всех узлов сети для поддержки этой спецификации флаг A может быть установлен для глобального включения защиты.

6LN помещает криптографический идентификатор Crypto-ID в поле ROVR, связанное с адресом при первой регистрации, позволяя 6LR запрашивать его для последующей проверки регистрации. Вызов для проверки 6LR или 6LBR может сделать в любой момент по своему усмотрению. Действительную регистрацию в 6LR или 6LBR **недопустимо** менять до завершения обработки вызова.

Когда флаг A в подсети установлен, маршрутизатор 6LR **должен** сделать запрос к 6LN, прежде чем создать привязку с установленным флагом C в EARO. 6LR **должен** также запрашивать 6LN при новой попытке регистрации для смены параметров уже имеющейся привязки для этого 6LN, например, с иным адресом источника на канальном уровне. Такая проверка защищает от атак с попыткой кражи адреса узла.

6LR **должен** сообщить маршрутизатору 6LBR об успешной проверке путём установки кода состояния 5 (Validation Requested) в EDAR. При последующем EDAR от нового 6LR с кодом состояния, отличным от 5, для проверенной привязки маршрутизатор 6LBR **должен** указать новому 6LR, что ему необходимо обратиться к 6LN, используя код состояния 5 в расширенном подтверждении дубликата адреса (Extended Duplicate Address Confirmation или EDAC).

6LR **должен** запросить 6LN, когда 6LBR просит сделать это с помощью сообщения EDAC с кодом состояния 5. EDAC возвращается маршрутизатором 6LR в NA(EARO) для регистрирующего узла. Маршрутизатору 6LR **следует** также обратиться ко всем подключённым 6LN в тот момент, когда 6LBR установил флаг A в 6CIO для незамедлительного обнаружения проблемы.

Если маршрутизатор 6LR не поддерживает Crypto-Type, он **должен** ответить EARO с кодом состояния 10 (Validation Failed) без вызова. В этом случае 6LN может попытаться использовать другое значение Crypto-Type до возврата к значению Crypto-Type = 0, которое **должны** поддерживать все 6LR.

Узел может использовать одновременно несколько адресов IPv6. Разделение адреса и криптографического материала устраняет для устройств с ограничениями необходимость создания множества ключей для разных адресов. 6LN **может** использовать одно значение Crypto-ID для подтверждения владения несколькими адресами IPv6. 6LN **может** также вывести несколько Crypto-ID для одной пары ключей, просто меняя модификатор.

## 6.1. Первый обмен с 6LR

6LN регистрируется в 6LR, расположенном через один интервал от него, с установленным в EARO флагом C, указывающим, что поле ROVR содержит Crypto-ID. Target Address в сообщении NS указывает адрес IPv6, который 6LN пытается зарегистрировать [RFC8505]. Взаимодействия на (локальном) канале показаны на рисунке 6. Если у 6LR нет состояния для 6LN, соответствующего NS(EARO), он отвечает вызовом NA(EARO, status=Validation Requested) с опцией Nonce Option (NonceLR на рисунке 6).

Nonce Option содержит значение, которое, насколько это возможно для реализации, ранее не использовалось. Эта спецификация наследует идею [RFC3971] о том, что значение nonce является случайным. В идеале реализация использует непредсказуемое криптографически случайное значение [BCP106]. Однако в некоторых сетях LLN это может оказаться непрактичным для устройств с ограниченными возможностями. Как вариант, устройство может использовать возрастающее значение, хранящееся в одном стабильном хранилище с ключом, что они терялись вместе и инициализировались возможным случайным значением nonce или «заготовки» для его расчёта.

6LN отвечает на запрос сообщением NS(EARO) с опцией Nonce (NonceLN на рисунке 6), CIPO (параграф 4.3) и NDPSO с подписью. Оба значения nonce включаются в подписанные данные для «содействия», обеспечивающего лучшую защиту даже при создании одной из сторон «слабого» значения nonce.

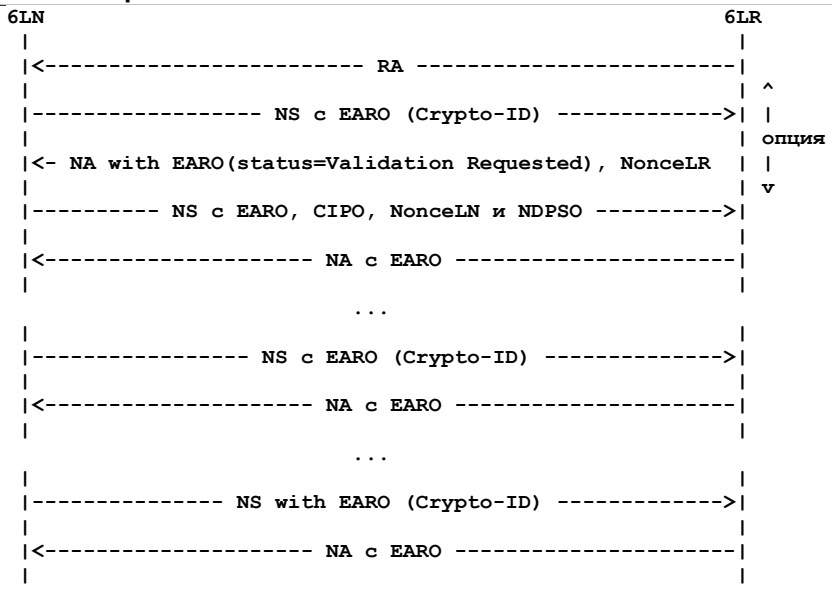


*Рисунок 6. Операции протокола на канале.*

6LR **должен** сохранять информацию, связанную с Crypto-ID в первом обмене NS, где эти данные указаны так, что параметры CIPO могут быть извлечены из Crypto-ID.

Этапы регистрации в 6LR указаны ниже.

При первом обмене с 6LR у узла 6LN запрашивается подтверждение владения Crypto-ID и Target Address зарегистрированный в Neighbor Solicitation. Когда 6LR получает регистрацию NS(EARO) с новым Crypto-ID в поле ROVR и эта регистрация не отвергнута по какой-либо иной причине, маршрутизатор **должен** передать вызов в сообщении NA(EARO) с кодом состояния Validation Requested.

При получении первого NA(EARO) со статусом Validation Requested от 6LR регистрирующему узлу **следует** повторить свою регистрацию с CIPO (параграф 4.3), содержащим весь материал, требуемый для создания Crypto-ID, созданное значение NonceLN и опцию NDP Signature (параграф 4.4), подтверждающую владение Crypto-ID и намерения зарегистрировать Target Address. При последующей (пере)проверке на том же 6LR узел 6LN **может** опустить опцию CIPO в целях экономии полосы канала, надеясь, что 6LR хранит её. Если проверка не проходит и узел получает новый вызов, ему **следует** снова включить CIPO.

Для подтверждения владения 6LR выполняет те же шаги, что и 6LN, заново создавая Crypto-ID на основе параметров из CIPO. Если созданное заново значение Crypto-ID соответствует полю ROVR, 6LN проверяет подпись, содержащуюся в NDPSO. При соответствии подписи в NDPSO проверка считается успешной, в противном случае завершается отказом.

Если 6LR получает отказ при проверке подписанного NS(EARO), он отвечает кодом состояния Validation Failed. После получения NA(EARO) с кодом Validation Failed регистрирующему узлу **следует** попытаться сменить Crypto-Type. Даже при отказе для Crypto-Type 0 можно попытаться зарегистрировать другой адрес в сообщении NS.

## 6.2. Генерация и проверка NDPSO

Подпись, создаваемая 6LN для доказательства владения секретным ключом, передаётся в опции NDPSO. Создание подписи узлом 6LN зависит от выбора Crypto-Type (таблица 1), выполняемого 6LN, как показано ниже.

- Создание сообщения, которое будет подписано, путём конкатенации приведённых ниже строковых значений в указанном порядке:
  1. 128-битовый тег Message Type [RFC3972] с сетевым порядком байтов (используемый в данной спецификации тег представлен в параграфе 8.1, значение было создано редактором спецификации с помощью службы https://www.random.org);
  2. опция CIPO;
  3. 16-байтовый Target Address (сетевой порядок байтов), переданный в сообщении NS (адрес, регистрируемый 6LN в маршрутизаторах 6LR и 6LBR);
  4. значение NonceLR, полученное от 6LR (сетевой порядок байтов) в сообщении NA (nonce имеет размер не менее 6 байтов в соответствии с [RFC3971]);
  5. значение NonceLN от 6LN (сетевой порядок байтов, размер nonce не менее 6 в соответствии с [RFC3971];
  6. 1-байтовое значение размера опции в EARO с Crypto-ID.
- Применение алгоритма подписи, заданного Crypto-Type, с использованием секретного ключа.

При получении опция NDPSO и CIPO маршрутизатор 6LR сначала проверяет соответствие EARO Length в CIPO размеру EARO. Если значения совпадают, восстанавливается Crypto-ID на основе CIPO, чтобы убедиться в соответствии ROVR битов слева. При положительном результате проверки маршрутизатор пытается проверить подпись в NDPSO, выполняя указанные ниже действия.

- Формирование сообщения для проверки путём конкатенации байтовых строк в указанном порядке:
  1. 128-битовый тег Message Type [RFC3972], описанный в параграфе 8.1 (сетевой порядок байтов);

2. опция CIPO;
3. 16-байтовый Target Address (сетевой порядок байтов), полученный в сообщении NS (адрес, регистрируемый 6LN в маршрутизаторах 6LR и 6LBR);
4. NonceLR из сообщения NA (nonce имеет размер не менее 6 байтов в соответствии с [RFC3971]);
5. значение NonceLN, полученное от 6LN в сообщении NS (сетевой порядок байтов, размер nonce не менее 6 в соответствии с [RFC3971];
6. 1-байтовое значение EARO Length, полученное в CIPO.

- Проверка подписи в сообщении с использованием открытого ключа из CIPO и рассчитанных локально значений с алгоритмом, заданным Crypto-Type. Если подпись соответствует, 6LR распространяет информацию 6LBR, используя поток EDAR/EDAC.
- Поскольку регистрация выполняется в порядке запросов (first-come, first-served), для адреса, который ещё не зарегистрирован на 6LBR, поток завершается успехом и оба маршрутизатора 6LR и 6LBR добавляют состояние для регистрируемых Crypto-ID и Target Address в свои абстрактные базы данных.

## 6.3. Работа через несколько узлов пересылки

Новый узел 6LN, присоединяющийся к сети, автоматически получает адрес и регистрируется на соседнем 6LR с помощью сообщения NS, передаваемого в опции EARO [RFC8505]. В сети 6LoWPAN с множеством пересылок (multihop) регистрация Crypto-ID распространяется маршрутизатору 6LBR, как показано на рисунке 7 для потока регистрации на всем пути к магистральному маршрутизатору 6LoWPAN (6BBR) [RFC8929].

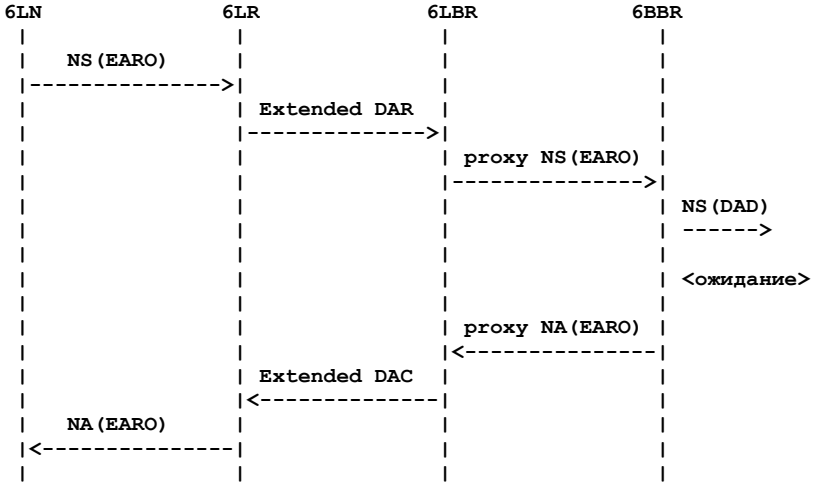


*Рисунок 7. Поток (повторной) регистрации.*

6LR и 6LBR взаимодействуют с помощью сообщения ICMPv6 EDAR и EDAC [RFC8505], как показано на рисунке 7. Эта спецификация расширяет сообщения EDAR и EDAC для передачи созданных криптографически ROVR.

Предполагается наличие между 6LR и 6LBR защищённой связи для контроля целостности и проверки подлинности сообщений EDAR и EDAC, поэтому не требуется распространять подтверждение владения 6LBR. Маршрутизатор 6LBR неявно полагает, что 6LR выполняет проверку, когда это нужно 6LBR, и при отсутствии дополнительных сведений от 6LR для удаления состояния проверка считается завершённой успешно.

# *7. Вопросы безопасности*

## 7.1. Смешанные сети

Оспорить регистрацию и избежать атак на адреса способны лишь маршрутизаторы 6LR, обновлённые в соответствии с этой спецификацией. В смешанной (brown) сети атакующий может подключиться к традиционному (не обновлённому) маршрутизатору 6LR и обмануть 6LBR. Поэтому даже при возможности установить флаг A в любой момент для проверки работы протокола защита будет эффективна лишь после обновления всех 6LR.

## 7.2. Угрозы, отмеченные в RFC 3971

Наблюдения для перечисленных ниже угроз в локальной сети [RFC3971] применимы и к данной спецификации.

***Обманные анонсы и запросы соседства***

Применимы угрозы, отмеченные в параграфе 9.2.1 [RFC3971]. AP-ND противостоит угрозам для сообщений NS(EARO) за счёт требования NDPSO и CIPO в предложениях соседства.

***DoS-атаки с дубликатами адресов***

Внутри LLN дубликаты адресов отбираются с помощью ROVR. Другое значение ROVR для того же зарегистрированного адреса влечёт отказ при второй регистрации [RFC8505]. DAD из опорной сети не пересылаются через LLN для обеспечения некой защиты от DoS в части сети с ограниченными ресурсами. Однако опции EARO из сообщений NS и NA передаются через опорную сеть. Это защищает от ошибочной интерпретации перемещения узлов как дублирования и позволяет магистральным маршрутизаторам определять подсеть с наиболее свежей регистрацией [RFC8505], которая больше всего подходит для проверки регистрации [RFC8929].

***Атаки с предложениями и анонсами маршрутизаторов***

Эта спецификация не меняет защиту RS и RA, остающихся защищёнными с помощью SEND.

***Атаки с воспроизведением***

Одноразовым значениям nonce следует быть неповторяющимися, но для безопасной работы их непредсказуемость не требуется. Использование NonceLR и NonceLN, создаваемых 6LR и 6LN, обеспечивает

согласованное поведение, которое обеспечивает эффективную защиту от атак с повторным использованием (replay) потока запросов и откликов. Качество защиты с применением случайных значений nonce зависит от генератора случайных чисел.

***DoS-атаки с ND***

Мошеннический узел с доступом к сети L2 может формировать множество адресов и регистрировать их с помощью AP-ND. Фронтом таких атак являются все 6LR в зоне досягаемости атакующего. 6LR **должен** защищать себя от переполнения и отвергать избыточные регистрации с кодом 2 (Neighbor Cache Full). Это будет препятствовать и регистрациям легитимных 6LN на том же 6LR, но 6LN может зарегистрироваться на других 6LR, доступных ему, но не атакующему.

## 7.3. Связь с 6LoWPAN ND

Угрозы и пути их устранения, описанные для 6LoWPAN ND [RFC6775] [RFC8505], применимы и здесь, в частности, к атакам на службы (denial-of-service или DoS), направленным на регистрацию в 6LR или 6LBR.

Secure ND [RFC3971] делает адрес IPv6 «криптографическим» за счёт объединения CGA как IID в адресе IPv6. Данная спецификация в отличие от упомянутого документа экономит около 1 Кбайт в каждом сообщении NS и NA, а также отделяет криптографический идентификатор от регистрируемого адреса IPv6, чтобы узел мог использовать несколько адресов IPv6, защищённых одним криптографическим идентификатором.

В соответствии с этой спецификацией 6LN может создавать свои адреса IPv6 любым способом, что обеспечивает возможность сжатия 6LoWPAN для адресов IPv6, выведенных из адресов L2 или использования временных адресов, не подверженных сжатию, например, псевдослучайных или краткосрочных в целях приватности [RFC8064][RFC8065].

Эта спецификация обеспечивает дополнительную защиту адресов, полученных по процедуре [RFC8505], но не ограничивает способ формирования или число адресов, одновременной используемых одним объектом. Атакующий по-прежнему может организовать DoS-атаку на регистрацию в 6LR или 6LBR, а также пытаться исчерпать пул адресов L2 или L3.

## 7.4. Взломанный 6LR

Эта спецификация распределяет запрос и его проверку на краю сети между 6LN и 6LR, что обеспечивает защиту от DoS-атак на центральный маршрутизатор 6LBR, а также снижает объем обмена данными в больших сетях и сетях с ограничениями.

Обратной стороной этого является необходимость для 6LBR доверять маршрутизаторам 6LR при проверке, а взаимодействие между 6LR и 6LBR должно быть защищено, чтобы результаты проверки не искажались.

Если маршрутизатор 6LR взломан и ему известно поле ROVR, применяемое реальным владельцем адреса, 6LR может заявить о том, что владелец адреса переместился и присоединён к нему, успешно пройдя проверку Crypto-ID. После этого 6LR может привлекать и внедрять трафик с этого адреса или позволить атакующему завладеть адресом.

## 7.5. Конфликты ROVR

Конфликт ROVR (т. е. Crypto-ID в этой спецификации) является редким, но возможным событием. В предположении, что хэш, применяемый для расчёта Crypto-ID, является достаточно строгим криптографически и возможны лишь случайные конфликты, при максимальном числе хэш-значений $n = 2^{(k)}$ (k битов в хэш-значении) и числе узлов p, выражение $1 - e^{(-p^{(2)}/(2n))}$ обеспечивает достаточно точную оценку вероятности конфликта (при одном Crypto-ID на узел), как в «парадоксе дней рождения».

Если Crypto-ID имеет размер 64 бита (минимальный разрешенный), вероятность конфликта составит 0,01% для сети в 66 миллионов узлов. Более того, конфликты актуальны лишь при их возникновении в одной оконечной сети (6LBR). В случае такого конфликта легитимный узел может случайно запросить адрес, зарегистрированный другим легитимным узлом (с тем же Crypto-ID). Для предотвращения таких конфликтов узлам **рекомендуется** не выводить адрес для регистрации из поля ROVR.

## 7.6. Атаки на реализацию

Упоминаемые в документе схемы подписи соответствуют стандартам NIST [FIPS186-4] или CFRG (Crypto Forum Research Group) [RFC8032] и обеспечивает строгую алгоритмическую защиту с уровнем примерно 128 битов. Эти схемы используют эллиптические кривые, которые специально разработаны с учётом арифметики без исключений и с постоянным временем (constant-time) [RFC7748], или для них имеется обширный опыт развёртывания с устойчивостью к timing-атакам [FIPS186-4].

Однако неосторожное выполнение операций подписи может приводить к утечке сведений о секретных ключах. Например, имеются атаки через побочные каналы на уровне микро-архитектуры, которые разработчикам следует учитывать [breaking-ed25519]. Разработчикам следует твердо помнить, что для защищённой реализации Ed25519 требуется надёжная реализация хэш-функции SHA-512, но этого не требуется для функции SHA-256, применяемой с ECDSA256 и ECDSA25519.

## 7.7. Атаки на ключи и протоколы

Пары ключей, используемые в этой спецификации, могут создаваться самостоятельно[1] и обмен открытыми ключами (например, через сертификаты от третьей стороны) не требуется. Новые пары ключей узел по желанию может создавать для новой регистрации, однако один секретный ключ **недопустимо** использовать более чем с одним экземпляром схемы подписи. **Недопустимо** также использовать тот секретный ключ для целей, отличающихся от создания подписей NDPSO.

ECDSA нужно применять строго в соответствии с [FIPS186-4]. В частности, каждая операция подписывания ECDSA **должна** использовать эфемерные секретные ключи k. Это исключает возникновение детерминированных ECDSA без

[1] Без удостоверяющего центра. *Прим. перев.*

ввода случайного значения для определения k, что считается опасным для предусмотренных этим документом приложений.

## 7.8. Проверка открытого ключа

Корректность формата открытых ключей, содержащихся в поле CIPO (служат для проверки подписей), нужно проверять на предмет того, что ключ действительно является точкой эллиптической кривой, указанной Crypto-Type, и эта точка имеет верный порядок.

Для точек, используемых со схемой подписи Ed25519, **должна** выполняться проверка того, что точка не входит в небольшую подгруппу (приложение B.1 в [CURVE-REPR]), для точек со схемой подписи ECDSA (т. е. ECDSA256 и ECDSA25519) **должна** выполняться проверка того, что точка имеет тот же порядок, что и базовая точка рассматриваемой кривой. Это обычно называют полной проверкой открытого ключа (приложение B.1 в [CURVE-REPR]).

## 7.9. Связанные регистрации

Поле ROVR в опции EARO, введённое в [RFC8505], расширяет поле EUI-64 опции ARO, заданной в [RFC6775]. Одним из недостатков применения EUI-64 в качестве ROVR является возможность атакующего, который знает о регистрации, сопоставить трафик одного узла 6LN с разными адресами. В разделе 3 [RFC8505] указано, что ROVR и регистрируемый адрес не связаны и 6LN может применять одно значение ROVR для нескольких регистраций или разные ROVR в каждой регистрации, а значение IID недопустимо выводить из ROVR. Теоретически, разные узлы 6LN могут использовать одно значение ROVR, пока они не пытаются зарегистрировать один адрес.

Используемый при расчёте Crypto-ID модификатор позволяет 6LN создавать разные Crypto-ID для разных адресов с одной парой ключей. Это повышает уровень приватности 6LN за счёт увеличения хранилища в 6LR, где приходится записывать множество CIPO с одним открытым ключом. Если атакующий получит доступ к 6LR, модификатор не сможет обеспечить защиту и узлу 6LN потребуется создавать разные пары ключей и адреса канального уровня для сокрытия владения множеством адресов.

# *8. Взаимодействие с IANA*

## 8.1. Тип сообщения CGA

В этом документе определён новый тег типа расширения (128-bit CGA Extension Type Tag) в субреестре CGA Extension Type Tags реестра Cryptographically Generated Addresses (CGA) Message Type Name Space, созданном [RFC3972]. Тег имеет значение 0x8701 55c8 0cca dd32 6ab7 e415 f148 84d0.

## 8.2. Субреестр Crypto-Type

Агентство IANA создало субреестр Crypto-Types в реестре Internet Control Message Protocol version 6 (ICMPv6) Parameters. Реестр индексируется целым числом от 0 до 255 и указывает эллиптическую кривую, хэш-функцию, алгоритм подписи, соглашение о представлении, размер открытого ключа и размер подписи, как показано в таблице 1, совместно задающие схему подписи. Подробные разъяснения приведены в Приложении B.

*Таблица 1. Параметры Crypto-Type.*

| **Значение Crypto-Type** | 0 (ECDSA256) | 1 (Ed25519) | 2 (ECDSA25519) |
|---|---|---|---|
| **Эллиптическая кривая** | NIST P-256 [FIPS186-4] | Curve25519 [RFC7748] | Curve25519 [RFC7748] |
| **Хэш-функция** | SHA-256 [RFC6234] | SHA-512 [RFC6234] | SHA-256 [RFC6234] |
| **Алгоритм подписи** | ECDSA [FIPS186-4] | Ed25519 [RFC8032] | ECDSA [FIPS186-4] |
| **Соглашения о представлении** | Вейерштрасс, (не)сжатое, порядок MSB/msb, [SEC1] | Эдвардс, сжатое, порядок LSB/lsb, [RFC8032] | Вейерштрасс, (не)сжатое, порядок MSB/msb, [CURVE-REPR] |
| **Размер открытого ключа** | 33 байта (сжатый), 65 байтов (несжатый) | 32 байта (сжатый) | 33 байта (сжатый), 65 байтов (несжатый) |
| **Размер подписи** | 64 байта | 64 байта | 64 байта |
| **Документ** | RFC 8928 | RFC 8928 | RFC 8928 |

В будущем могут быть определены новые значения Crypto-Type, обеспечивающие такую же или лучшую защиту. Выделение новых значений Crypto-Type **должно** выполняться через IANA по процедуре Specification Required или IESG Approval в соответствии с BCP 26 [RFC8126].

## 8.3. Типы IPv6 ND Option

Этот документ регистрирует два новых типа опций ND в субреестре IPv6 Neighbor Discovery Option Formats.

*Таблица 2. Новые опции ND.*

| ***Описание*** | ***Тип*** | ***Документ*** |
|---|---|---|
| Crypto-ID Parameters Option (CIPO) | 39 | RFC 8928 |
| NDP Signature Option (NDPSO) | 40 | RFC 8928 |

## 8.4. Новый бит возможностей 6LoWPAN

Агентство IANA добавило запись в субреестр 6LoWPAN Capability Bits, созданный в [RFC7400].

*Таблица 3. Новый бит 6LoWPAN Capability.*

| ***Бит*** | ***Описание*** | ***Документ*** |
|---|---|---|
| 9 | AP-ND Enabled (1 бит) | RFC 8928 |

# 9. Литература

## 9.1. Нормативные документы


[FIPS186-4] National Institute of Standards and Technology, "Digital Signature Standard (DSS)", FIPS 186-4, DOI 10.6028/NIST.FIPS.186-4, July 2013, <https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.186-4.pdf>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC3971] Arkko, J., Ed., Kempf, J., Zill, B., and P. Nikander, "SEcure Neighbor Discovery (SEND)", RFC 3971, DOI 10.17487/RFC3971, March 2005, <https://www.rfc-editor.org/info/rfc3971>.

[RFC6234] Eastlake 3rd, D. and T. Hansen, "US Secure Hash Algorithms (SHA and SHA-based HMAC and HKDF)", RFC 6234, DOI 10.17487/RFC6234, May 2011, <https://www.rfc-editor.org/info/rfc6234>.

[RFC6775] Shelby, Z., Ed., Chakrabarti, S., Nordmark, E., and C. Bormann, "Neighbor Discovery Optimization for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)", RFC 6775, DOI 10.17487/RFC6775, November 2012, <https://www.rfc-editor.org/info/rfc6775>.

[RFC7400] Bormann, C., "6LoWPAN-GHC: Generic Header Compression for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)", RFC 7400, DOI 10.17487/RFC7400, November 2014, <https://www.rfc-editor.org/info/rfc7400>.

[RFC7748] Langley, A., Hamburg, M., and S. Turner, "Elliptic Curves for Security", RFC 7748, DOI 10.17487/RFC7748, January 2016, <https://www.rfc-editor.org/info/rfc7748>.

[RFC8032] Josefsson, S. and I. Liusvaara, "Edwards-Curve Digital Signature Algorithm (EdDSA)", RFC 8032, DOI 10.17487/RFC8032, January 2017, <https://www.rfc-editor.org/info/rfc8032>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC8505] Thubert, P., Ed., Nordmark, E., Chakrabarti, S., and C. Perkins, "Registration Extensions for IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) Neighbor Discovery", RFC 8505, DOI 10.17487/RFC8505, November 2018, <https://www.rfc-editor.org/info/rfc8505>.

[SEC1] Standards for Efficient Cryptography, "SEC 1: Elliptic Curve Cryptography", Version 2, May 2009, <https://www.secg.org/sec1-v2.pdf>.


## 9.2. Дополнительная литература


[BCP106] Eastlake 3rd, D., Schiller, J., and S. Crocker, "Randomness Requirements for Security", BCP 106, RFC 4086, DOI 10.17487/RFC4086, June 2005, <https://www.rfc-editor.org/info/rfc4086>.

[BCP201] Housley, R., "Guidelines for Cryptographic Algorithm Agility and Selecting Mandatory-to-Implement Algorithms", BCP 201, RFC 7696, DOI 10.17487/RFC7696, November 2015, <https://www.rfc-editor.org/info/rfc7696>.

[breaking-ed25519] Samwel, N., Batina, L., Bertoni, G., Daemen, J., and R. Susella, "Breaking Ed25519 in WolfSSL", Topics in Cryptology - CT-RSA, pp. 1-20, March 2018, <https://link.springer.com/chapter/10.1007/978-3-319-76953-0_1>.

[CURVE-REPR] Struik, R., "Alternative Elliptic Curve Representations", Work in Progress, Internet-Draft, draft-ietf-lwig-curve-representations-14, 15 November 2020, <https://tools.ietf.org/html/draft-ietf-lwig-curve-representations-14>.

[RFC3972] Aura, T., "Cryptographically Generated Addresses (CGA)", RFC 3972, DOI 10.17487/RFC3972, March 2005, <https://www.rfc-editor.org/info/rfc3972>.

[RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", RFC 4861, DOI 10.17487/RFC4861, September 2007, <https://www.rfc-editor.org/info/rfc4861>.

[RFC4862] Thomson, S., Narten, T., and T. Jinmei, "IPv6 Stateless Address Autoconfiguration", RFC 4862, DOI 10.17487/RFC4862, September 2007, <https://www.rfc-editor.org/info/rfc4862>.

[RFC4919] Kushalnagar, N., Montenegro, G., and C. Schumacher, "IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals", RFC 4919, DOI 10.17487/RFC4919, August 2007, <https://www.rfc-editor.org/info/rfc4919>.

[RFC4944] Montenegro, G., Kushalnagar, N., Hui, J., and D. Culler, "Transmission of IPv6 Packets over IEEE 802.15.4 Networks", RFC 4944, DOI 10.17487/RFC4944, September 2007, <https://www.rfc-editor.org/info/rfc4944>.

[RFC6282] Hui, J., Ed. and P. Thubert, "Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks", RFC 6282, DOI 10.17487/RFC6282, September 2011, <https://www.rfc-editor.org/info/rfc6282>.

[RFC7039] Wu, J., Bi, J., Bagnulo, M., Baker, F., and C. Vogt, Ed., "Source Address Validation Improvement (SAVI) Framework", RFC 7039, DOI 10.17487/RFC7039, October 2013, <https://www.rfc-editor.org/info/rfc7039>.

[RFC7217] Gont, F., "A Method for Generating Semantically Opaque Interface Identifiers with IPv6 Stateless Address Autoconfiguration (SLAAC)", RFC 7217, DOI 10.17487/RFC7217, April 2014, <https://www.rfc-editor.org/info/rfc7217>.

[RFC8064] Gont, F., Cooper, A., Thaler, D., and W. Liu, "Recommendation on Stable IPv6 Interface Identifiers", RFC 8064, DOI 10.17487/RFC8064, February 2017, <https://www.rfc-editor.org/info/rfc8064>.

[RFC8065] Thaler, D., "Privacy Considerations for IPv6 Adaptation-Layer Mechanisms", RFC 8065, DOI 10.17487/RFC8065, February 2017, <https://www.rfc-editor.org/info/rfc8065>.

[RFC8126] Cotton, M., Leiba, B., and T. Narten, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 8126, DOI 10.17487/RFC8126, June 2017, <https://www.rfc-editor.org/info/rfc8126>.

[RFC8929] Thubert, P., Ed., Perkins, C.E., and E. Levy-Abegnoli, "IPv6 Backbone Router", RFC 8929, DOI 10.17487/RFC8929, November 2020, <https://www.rfc-editor.org/info/rfc8929>.

# *Приложение A. Требования, выполняемые этим документом*

В этом приложении указаны требования к защищённому протоколу обнаружения соседей (ND) для сетей LLN.

- Протокол **должен** базироваться на оптимизации обнаружения соседей для LLN, определённой в [RFC6775]. RFC 6775 задаёт оптимизацию путём инициируемого хостом взаимодействия для «спящих» хостов с ограниченными ресурсами и устранения распознавания групповых адресов.
- Новые опции, добавляемые в сообщения Neighbor Solicitation, **должны** обеспечивать небольшой размер пакетов, особенно по сравнению с такими протоколами как SEND. Уменьшение размера пакетов снижает энергопотребления на узлах с ограниченными возможностями в сетях с потерями.
- Механизму регистрации **следует** быть расширяемым для других каналов LLN и не ограничиваться лишь IEEE 802.15.4. **Следует** поддерживать каналы LLN, для которых имеется спецификация 6lo (IPv6 over foo), такие как Wi-Fi со слабым питанием.
- В рамках протокола следует обеспечивать механизм расчёта уникальных идентификаторов с возможностью формирования адреса Link-Local, уникального по меньшей мере в LLN, подключённой к 6LBR.
- Опции Address Registration в регистрации ND **следует** быть расширяемой для передачи соответствующих форм уникальных идентификаторов.
- Механизму обнаружения соседей следует задавать формирование локального адреса сайта в соответствии с рекомендациями по безопасности [RFC7217].

# *Приложение B. Соглашения о представлении*

## B.1. Схемы подписей

Схема подписи ECDSA256 для Crypto-Type=0 - это ECDSA [FIPS186-4], созданная с кривой NIST P-256, как указано в Приложении D.1.2 к [FIPS186-4] и хэш-функцией SHA-256 [RFC6234], где точки кривой NIST представлены как точки сокращённой кривой Вейерштрасса (см. [FIPS186-4]) строками октетов с порядков битов и байтов от старшего к младшему (msb и MSB). Сама подпись состоит из двух целых чисел (r и s), каждое из которых представляется строкой октетов фиксированного размера с порядком MSB и msb. Другие детали приведены в [FIPS186-4] для ECDSA, приложение B.3 описывает кодирование открытых ключей, а приложение B.2 - кодирование подписи.

Схема подписи Ed25519 для Crypto-Type=1 - это EdDSA [RFC8032], созданная с кривой Монтгомери Curve25519, как указано в [RFC7748] и хэш-функцией SHA-512 [RFC6234], где точки кривой Монтгомери представлены как точки соответствующей скрученной кривой Эдвардса Edwards25519 (см. Приложение B.4) строками октетов с порядков битов и байтов от младшего к старшему (lsb и LSB). Сама подпись является строкой битов, представляющей точку этой скрученной кривой Эдвардса с сжатом формате, и целым числом с порядком LSB и lsb. Детали EdDSA, а также кодирование открытых ключей и подписей представлены в спецификации Ed25519 [RFC8032].

Схема подписи ECDSA25519 для Crypto-Type=2 - это ECDSA [FIPS186-4], созданная с кривой Монтгомери Curve25519, как указано в [RFC7748] и хэш-функцией SHA-256 [RFC6234], где точки кривой Монтгомери представлены как точки сокращённой кривой Вейерштрасса Wei25519 (см. Приложение B.4) строками октетов с порядков битов и байтов от старшего к младшему (msb и MSB). Сама подпись состоит из двух целых чисел (r и s), каждое из которых представляется строкой октетов фиксированного размера с порядком MSB и msb. Другие детали приведены в [FIPS186-4] для ECDSA, приложение B.3 описывает кодирование открытых ключей, а приложение B.2 - кодирование подписи.

## B.2. Представление подписей ECDSA

В ECDSA каждая подпись является упорядоченной парой целых чисел (r, s) [FIPS186-4], где каждая число задано строкой из 32 октетов в соответствии с правилами преобразования FieldElement-to-OctetString [SEC1], а сама пара представлена конкатенацией этих строк (строка из 64 октетов). Обратная операция проверяет, что подпись имеет размер 64 октета и представляет левую и правую половину (каждая по 32 октета) как целые числа r и s, соответственно, используя правила OctetString-to-FieldElement [SEC1]. В обоих случаях поля представляются набором чисел по модулю n, где n - (простой) порядок базовой точки соответствующей кривой. Номенклатура эллиптических кривых представлена в Приложении B.1 к [CURVE-REPR].

## B.3. Представление открытых ключей, применяемых с ECDSA

Алгоритм ECDSA предназначен для использования с эллиптическими кривыми в сокращённой форме Вейерштрасса. Каждая точка такой кривой представляет строкой октетов по правилам Elliptic-Curve-Point-to-Octet-String [SEC1], где может быть включено сжатие точек (указывается левым октетом представления). Обратное преобразование строки октетов в точку кривой выполняется по правилам Octet-String-to-Elliptic-Curve-Point [SEC1], которые задают отклонение точек, уходящих в бесконечность (этот случай возникает при подаче на вход преобразования строки октетов размером 1).

## B.4. Дополнительные представления Curve25519

Эллиптическая кривая Curve25519 [RFC7748] является кривой Монтгомери и каждая её точка может быть представлена как точка скрученной кривой Эдвардса или кривой в сокращённой форме Вейерштрасса путём

преобразования координат (изоморфное отображение). Параметры кривой Монтгомери и соответствующей изоморфной кривой в виде скрученной кривой Эдвардса или сокращённой формы Вейерштрасса показаны ниже. Параметры области кривой Монтгомери Curve25519 и кривой Эдвардса Edwards25519 заданы в [RFC7748], а эллиптической кривой Wei25519 в сокращённой форме Вейерштрасса - в параграфе 6.1.1 [FIPS186-4]. Дополнительные сведения об этих кривых и преобразовании координат приведены в [CURVE-REPR].

Общие параметры (все кривые):

```
p  2^(255)-19
   (=0x7fffffff ffffffff ffffffff ffffffff ffffffff ffffffff ffffffff
   ffffffed)
h  8
n
   72370055773322622139731865630429942408571163593799076060019509382 8
   5454250989
   (=2^(252) +  0x14def9de a2f79cd6 5812631a 5cf5d3ed)
```

Параметры кривой Монтгомери (Curve25519):

```
A  486662
B  1
Gu 9 (=0x9)
Gv
   14781619447589544791020593568409986887264606134616475288964881837 7
   55586237401
   (=0x20ae19a1 b8a086b4 e01edd2c 7748d14c 923d4d7e 6d7c61b2 29e9c5a2
   7eced3d9)
```

Параметры скрученной кривой Эдвардса (Edwards25519):

```
a  -1 (-0x01)
d  -121665/121666
   (=3709570593466943934313808350875456518954211387984321901638878553
   3085940283555)
   (=0x52036cee 2b6ffe73 8cc74079 7779e898 00700a4d 4141d8ab 75eb4dca
   135978a3)
Gx
   15112221349535400772501151409588531511454012693041857206046113283 9
   49847762202
   (=0x216936d3 cd6e53fe c0a4e231 fdd6dc5c 692cc760 9525a7b2 c9562d60
   8f25d51a)
Gy  4/5
   (=4631683569492647816942839400347516314130799386625622561578303360
   3165251855960)
   (=0x66666666 66666666 66666666 66666666 66666666 66666666 66666666
   66666658)
```

Параметры кривой Вейерштрасса (Wei25519):

```
a
   19298681539552699237261830834781317975544997444273427337399095973345
   73241639236
   (=0x2aaaaaaa aaaaaaaa aaaaaaaa aaaaaaaa aaaaaaaa aaaaaaaa aaaaaa98
   4914a144)
b
   55751746669818908907645289078257140818241103727901012315294400837 9
   56729358436
   (=0x7b425ed0 97b425ed 097b425e d097b425 ed097b42 5ed097b4 260b5e9c
   7710c864)
GX
   19298681539552699237261830834781317975544997444273427337399095973346
   52188435546
   (=0x2aaaaaaa aaaaaaaa aaaaaaaa aaaaaaaa aaaaaaaa aaaaaaaa aaaaaaaa
   aaad245a)
GY
   14781619447589544791020593568409986887264606134616475288964881837 7
   55586237401
   (=0x20ae19a1 b8a086b4 e01edd2c 7748d14c 923d4d7e 6d7c61b2 29e9c5a2
   7eced3d9)
```

## *Благодарности*

Большое спасибо Charlie Perkins за подробную рецензию и конструктивные замечания. Авторы также признательны Robert Moskowitz и Benjamin Kaduk за комментарии и предложения, которые привели ко многим улучшениям. Спасибо Shwetha Bhandari за активное руководство проектом, а также Roman Danyliw, Alissa Cooper, Mirja Kühlewind, Éric Vyncke, Vijay Gurbani, Al Morton и Adam Montville за конструктивные рецензии в процессе IESG. Большое спасибо руководителям направления INT Suresh Krishnan и Erik Kline за поддержку на протяжении работы.

## *Адреса авторов*

**Pascal Thubert** (редактор)

Cisco Systems, Inc.

Building D

45 Allee des Ormes - BP1200

06254 MOUGINS - Sophia Antipolis

France

Phone: +33 497 23 26 34

Email: pthubert@cisco.com

**Behcet Sarikaya**

Email: sarikaya@ieee.org

**Mohit Sethi**

Ericsson

FI-02420 Jorvas

Finland

Email: mohit@piuha.net

**Rene Struik**

Struik Security Consultancy

Email: rstruik.ext@gmail.com

**Перевод на русский язык**

Николай Малых

nmalykh@protokols.ru