Спецификация протокола свободной одноранговой системы маршрутизации

Автор: Гордопольцева Анна Дмитриевна (annruby@vendetti.ru)

Версия: 0.1-draft

Создан: 21.06.2025

Статус: черновик

Примечание: настоящая версия протокола является черновиком (Прошу обращаться с предложениями на почту выше). FP2PRS не предназначен для установления анонимных соединений.

1. Введение

Свободная одноранговая система маршрутизации (Free Peer-to-Peer Routing System; FP2PRS) — это прикладной протокол, предназначенный для организации децентрализованных сетей в условиях строгих NAT. FP2PRS использует гибридную систему идентификации узлов, сочетающую децентрализованные DHT-таблицы и криптографические идентификаторы, а также механизмы NAT-траверса для обеспечения устойчивого соединения между участниками.

Основные возможности протокола включают:

- Динамическое управление портами для установки прямых подключений;
- Выделение временных LAN-адресов участникам сети;
- Криптографическую аутентификацию узлов и защиту от атак;
- Полную независимость от централизованных серверов.

2. Требования к протоколу

Поддержка IPv4/IPv6:

Узел должен поддерживать протокол IPv4 или IPv6. Приоритет отдаётся IPv6-подключениям. Если IPv6 недоступен, протокол автоматически переключается на IPv4 с определением типа NAT. FP2PRS обеспечивает возможность взаимодействия между узлами с IPv4 и IPv6.

Автоматический обход NAT:

Протокол использует перебор различных методов, с целью обхода NAT. Предпочтение отдается наиболее быстрым решениям, таким как использование IPv6 или STUN. В проблемных сетях используется TURN.

Децентрализованная идентификация:

Протокол обеспечивает возможность прямой связи узлов, а также развертывание глобальных децентрализованных сетей (таких как мессенджеры, почтовые сервисы и тд). При прямой связи между маршрутизаторами рекомендуется использование криптографических идентификаторов без применения распределённой хеш-таблицы. Представление идентификатора, а также другой информации необходимой для подключения возможно посредством QR-кодов, magnet-ссылок, файлов «.fp2prs». В случаях, когда требуется подключиться к глобальной децентрализованной сети рекомендуется использование DHT. Распределять DHT следует между bootstrap-узлами и пользователями сети.

3. Архитектура FP2PRS

3.1. Определения

FP2PRS-сеть — совокупность узлов, взаимодействующих между собой с использованием протокола FP2PRS. Сеть может быть изолированной или глобальной, не требует наличия централизованной инфраструктуры и поддерживает как прямую одноранговую связь, так и маршрутизацию через виртуальные подсети.

FP2PRS-узел — логическая единица, обладающая уникальным криптографическим идентификатором и взаимодействующая с другими узлами через FP2PRS-маршрутизатор. Узел может инициировать соединения, принимать подключения, ретранслировать трафик и участвовать в распределённой инфраструктуре.

FP2PRS-маршрутизатор — программный агент, реализующий прикладной протокол FP2PRS. Выполняет NAT traversal, маршрутизацию, аутентификацию, организацию p2p-соединений и (опционально) участие в глобальной DHT.

Bootstrap-узел — FP2PRS-узел, участвующий в глобальной DHT и предоставляющий другим узлам первичную информацию о сети. Bootstrap-узлы не являются управляющими и могут быть заданы вручную, опубликованы в .fp2prs-файлах или обнаружены динамически.

Распределённая хеш-таблица (DHT) — это децентрализованное и отказоустойчивое хранилище пар "ключ-значение", используемое узлами FP2PRS для поиска других участников и поддержки глобальных сетей.

Криптографический идентификатор (Crypto-ID) — это глобально уникальный идентификатор узла, получаемый из его открытого ключа путём применения криптографической хеш-функции. Crypto-ID используется в качестве основной единицы адресации и аутентификации в сети FP2PRS.

3.2. Режимы работы маршрутизатора

Прямое подключение (Direct Peer Mode)

Маршрутизатор устанавливает защищённое p2p-соединение с другим узлом по криптографическому идентификатору. Используются NAT traversal (STUN/TURN) при необходимости. Соединение инициируется напрямую без участия инфраструктуры DHT.

Виртуальная подсеть (Virtual Subnet Mode)

Маршрутизатор принимает подключения от других узлов и назначает им временные IP-адреса. Такой узел действует как шлюз, обеспечивая маршрутизацию трафика и совместимость с IP-приложениями. Этот режим используется как вспомогательная мера для поддержки приложений, не работающих в p2p-режиме.

Подключение к глобальной сети (Global DHT Mode)

Узел участвует в распределённой хеш-таблице (DHT) и может использоваться для поиска и установления маршрутов к другим узлам. Инициализация возможна через bootstrap-узлы.

3.3. Расширяемость и мультиагентная архитектура

В текущей версии протокола FP2PRS предполагается, что маршрутизатор работает в одном активном режиме, соответствующем своей роли в сети. Однако архитектура не ограничивает реализацию одновременной работы в нескольких режимах. Возможны следующие подходы:

- **Комбинированный маршрутизатор:** единый экземпляр FP2PRS-маршрутизатора, способный обслуживать p2p-соединения, виртуальные IP-подсети и глобальную маршрутизацию одновременно;
- **Мультиагентная реализация:** запуск нескольких изолированных экземпляров маршрутизатора, каждый из которых работает в отдельном режиме и взаимодействует с приложениями через разные сокеты, интерфейсы или контейнеры.

Такое расширение может быть реализовано на уровне конкретной реализации и не входит в обязательные требования текущей спецификации. Формальное описание многорежимной архитектуры может быть включено в будущие версии протокола.

4. Идентификация узлов

4.1. Криптографическая идентификация

Каждому узлу, использующему протокол FP2PRS, присваивается криптографический идентификатор (далее — Crypto-ID), который представляет собой 256-битный хеш открытого ключа, сгенерированного по алгоритму Ed25519.

Crypto-ID служит глобально уникальным идентификатором узла в сети FP2PRS и используется в качестве:

- адреса в DHT и других структурах поиска;
- якоря доверия при аутентификации;
- идентификатора в интерфейсах пользователя.

Узел, устанавливающий соединение, раскрывает свой открытый ключ и предоставляет цифровую подпись. Принимающий узел выполняет следующие шаги:

- Проверяет, что 256-битный хеш публичного ключа совпадает с заявленным Crypto-ID.
- Проверяет корректность цифровой подписи с использованием переданного открытого ключа.

Это обеспечивает доказательство владения закрытым ключом и подтверждение подлинности узла, без необходимости предварительного распространения открытого ключа.

4.2. Временная адресация и NAT-информация

4.2.1. Виртуальные IP-адреса

В режиме виртуальной подсети FP2PRS-маршрутизатор динамически выделяет IP-адреса (например, из диапазона 10.0.0.0/16) подключённым узлам. Эти IP-адреса используются внутри FP2PRS-сети и являются временными.

Адресация применяется для:

- маршрутизации в виртуальной подсети;
- обеспечения совместимости с IP-приложениями;
- опционального NAT внутри FP2PRS-узла.

Эти IP-адреса не являются частью криптографической идентификации и не используются вне контекста текущего подключения.

4.2.2. NAT-тип и STUN-информация

Узел может предварительно определить возможность прямого подключения через NAT, используя STUN-протокол. Полученные данные могут включать:

- внешний IP-адрес и порт;
- тип NAT (например, Full-cone, Symmetric);
- доступность входящих подключений.

Данная информация может быть включена в файл «.fp2prs» или передана другой стороне в процессе установления соединения. Это позволяет принимающей стороне оценить возможность установления прямого соединения (например, исключить попытки STUN при наличии Symmetric NAT).

Внешняя NAT-информация считается временной и может изменяться в следующих случаях:

- смена точки подключения;
- перезапуск маршрутизатора/провайдера;
- истечение срока аренды IP.

Рекомендуется проверять STUN-информацию непосредственно перед установлением соединения или хранить её с указанием срока актуальности.

5. Формат файлов .fp2prs: дескрипторы узлов и сервисов

Файлы с расширением .fp2prs представляют собой дескрипторы узлов и сервисов FP2PRS, предназначенные для распространения информации об узле в децентрализованной сети. Формат разработан с целью обеспечить:

- безопасную идентификацию и аутентификацию узлов;
- начальную маршрутизацию соединений (bootstrapping);
- описание доступных сервисов и ролей узла;
- человекочитаемость и расширяемость.

Файлы .fp2prs представлены в формате YAML и подписаны владельцем узла с использованием ключа Ed25519. Перед использованием любой такой файл должен пройти процедуру криптографической верификации.

5.1 Структура файла

```
GAD_0.1
node:
  crypto_id: sha256:...
  public_key: Ed25519:...
connection_hints:
  protocol: ipv6
  address: 2001::db8::1
  port: 9999  full_cone
  nat_type: restricted_cone
bootstrap_peers:
  sha556:peer1hasr1hash...
  sha556:peer2hash...
services:
  id: main_site
  type: http
  port: Personal blog
  description: Personal blog
roles:
  type: relay
  policy: public_open
  name: Main Gateway
  description: Publi entry to
  FP2PRS community
signature:
  signer_id:sha556:...
  signature_data: base64:...
```

5.2 Верификация и безопасность

Каждый «.fp2prs» файл должен быть подписан владельцем соответствующего публичного ключа. Клиент при получении такого файла обязан:

- Вычислить хеш от public_key и убедиться, что он совпадает с crypto_id.
- Проверить цифровую подпись содержимого файла (все блоки, кроме signature) с помощью public_key.
- В случае несоответствия файл считается недействительным и отклоняется.

Цель этой схемы — исключить возможность подделки файла, MITM-атак, подмены адресов и маршрутов.

5.3 Расширяемость

Формат допускает добавление новых полей в будущем. Клиенты обязаны:

- Игнорировать незнакомые поля;
- Сохранять корректную валидацию и обработку известных блоков;
- Обращать внимание на поле spec_version при попытке прочитать файл.

5.4 Применение

Файлы .fp2prs применяются для:

- Распространения "визиток" узлов;
- Подключения к удалённым сервисам без централизованных DNS или API;
- Автоматической настройки клиентов при наличии только .fp2prs файла;
- Информирования клиентов о поддерживаемых сервисах и инфраструктурных ролях узла.

.....