Internet Engineering Task Force (IETF) M. Thomson
Request for Comments: 8999 Mozilla
Category: Standards Track May 2021
ISSN: 2070-1721

Version-Independent Properties of QUIC

Независимые от версии свойства QUIC

Аннотация

Этот документ определяет свойства транспортного протокола QUIC, общие для всех версий протокола.

Статус документа

Документ относится к категории Internet Standards Track.

окумент является результатом работы IETF[1] и представляет согласованный взгляд сообщества IETF. Документ прошёл открытое обсуждение и был одобрен для публикации IESG[2]. 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/rfc8999.

Оглавление

1. Абстрактное описание QUIC

QUIC - это ориентированный на соединения протокол взаимодействия двух конечных точек. Эти точки обмениваются дейтаграммами UDP. дейтаграммы UDP содержат пакеты QUIC. Конечные точки QUIC используют пакеты QUIC для организации соединения QUIC, которое является общим состоянием для этих конечных точек.

2. Фиксированные свойства всех версий QUIC

В дополнение к защищённому мультиплексируемому транспорту QUIC [QUIC-TRANSPORT] протокол позволяет согласовать версию. Это позволяет протоколу меняться с течением времени в соответствии с новыми требованиями. Многие характеристики протокола могут меняться в разных версиях. В этом документе описано подмножество QUIC, которое предназначено оставаться стабильным в новых версиях по мере их разработки и развёртывания. Все эти инварианты не зависят от версии IP. Основной целью этого документа является обеспечение возможности развёртывания новых версий QUIC. Описывая неизменные свойства, этот документ направлен на сохранение возможности ключевых точек QUIC согласовать изменения любого другого аспекта протокола. В результате это гарантирует минимальный объем информации, доступной кому-либо кроме конечных точек. Если это явно не запрещено данным документом, любые аспекты протокола могут меняться в разных версиях.

В Приложении A приведён список некоторых некорректных допущения, которые могут быть сделаны на основе сведений о QUIC версии. Это не относится к другим версиям QUIC.

[1]Internet Engineering Task Force - комиссия по решению инженерных задач Internet.
[2]Internet Engineering Steering Group - комиссия по инженерным разработкам Internet.

3. Соглашения и определения

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.

Этот документ определяет требования к будущим версиям QUIC, хотя нормативный язык здесь не применяется. В документе используются термины и соглашения о нотации из [QUIC-TRANSPORT].

4. Соглашения о нотации

Формат пакетов описывается с использованием определённой здесь нотации, которая совпадает с применяемой в [QUIC-TRANSPORT].

Составные поля указываются именем, а затем следует список полей в фигурных скобках через запятые. Отдельные поля включают сведения о размере, а также указания о фиксированном значении, необязательности или повторах. Для полей применяются указанные ниже обозначения (размеры задаются в битах).

x (A)
: Поле x размером A битов.

x (A..B)
: Указывает, что x может иметь любой размер от A до B, если A не указано, поле может иметь размер 0, отсутствие B говорит, что размер поля не ограничен. Значения в этом формате всегда завершаются на границе байта.

x (L) = C
: Указывает, что x имеет фиксированное значение C, размером L в одной из приведённых выше форм.

x (L) …
: Указывает повторение x (возможно пустой набор), где каждый экземпляр имеет размер L.

В документе применяется сетевой порядок байтов (big endian), поля указываются со старшего бита в каждом байте.

Отдельные поля составного поля указываются с именем составного поля. На рисунке 1 представлен пример.

```
Example Structure {
  One-bit Field (1),
  7-bit Field with Fixed Value (7) = 61,
  Arbitrary-Length Field (..),
  Variable-Length Field (8..24),
  Repeated Field (8) ...,
}
```

Рисунок 1. Пример формата.

5. Пакеты QUIC

Конечные точки QUIC обмениваются дейтаграммами UDP, содержащими один или несколько пакетов QUIC. В этом разделе описаны инвариантные характеристики пакетов QUIC. Версия QUIC может разрешать включение множества пакетов QUIC в одну дейтаграмму UDP, но инвариантные свойства описывают лишь первый пакет в дейтаграмме.

QUIC определяет два типа заголовка в пакетах - длинный и короткий. Пакеты с длинным заголовком указываются установкой (1) старшего бита в первом байте пакета, в коротких заголовках этот бит сброшен (0).

В пакетах QUIC может применяться защита целостности пакета, включая заголовок. Однако для пакетов QUIC Version Negotiation защита целостности не применяется (см. раздел 6).

Помимо описанных здесь значений содержимое (payload) пакетов QUIC зависит от версии и имеет произвольный размер.

5.1. Длинный заголовок

Формат длинного заголовка показан на рисунке 2.

```
Long Header Packet {
  Header Form (1) = 1,
  Version-Specific Bits (7),
  Version (32),
  Destination Connection ID Length (8),
  Destination Connection ID (0..2040),
  Source Connection ID Length (8),
  Source Connection ID (0..2040),
  Version-Specific Data (..),
}
```

Рисунок 2. Длинный заголовок QUIC.

В пакете QUIC с длинным заголовком старший бит первого байта имеет значение 1. Остальные биты этого байта зависят от версии. Следующие 4 байта образуют 32-битовое поле Version, описанное в параграфе 5.4. Следующий байт указывает размер следующего за ним поля Destination Connection ID (в байтах). Размер представлен 8-битовым целым числом без знака. Поле Destination Connection ID следует за Destination Connection ID Length и имеет размер от 0 до 255 байтов. Идентификаторы соединений описаны в параграфе 5.3. В следующем байте указан размер поля Source Connection ID, расположенного вслед за ним. Размер представлен 8-битовым целым числом без знака. Поле Source Connection ID следует за Source Connection ID Length и имеет размер от 0 до 255 байтов.

Остальная часть пакета зависит от версии.

5.2. Короткий заголовок

Формат короткого заголовка показан на рисунке 3.

```
Short Header Packet {
  Header Form (1) = 0,
  Version-Specific Bits (7),
  Destination Connection ID (..),
  Version-Specific Data (..),
}
```

Рисунок 3. Короткий заголовок QUIC.

В пакетах QUIC с коротким заголовком старший бит первого байта имеет значение 0. Пакет QUIC с коротким заголовком включает Destination Connection ID сразу за первым байтом. Короткий заголовок не содержит полей Destination Connection ID Length, Source Connection ID Length, Source Connection ID, Version. Размер Destination Connection ID не указывается в пакетах с коротким заголовком и не ограничивается этой спецификацией.

Остальная часть пакета зависит от версии.

5.3. Идентификатор соединения

Идентификатор соединения представляет собой неанализируемое (opaque) поле произвольного размера. Основным назначением идентификаторов соединения является предотвращение доставки пакетов в соединении QUIC не той конечной точке в случае смены адреса на нижележащих уровнях (UDP, IP и ниже). Идентификаторы соединения используются конечными точками и промежуточными узлами для гарантированной доставки каждого пакета QUIC корректному экземпляру конечной точки. В конечной точке идентификатор соединения служит для указания соединения QUIC, которому предназначен пакет.

Каждая конечная точка выбирает идентификаторы соединения с использованием зависящих от версии методов. Пакеты одного соединения QUIC могут использовать разные значения идентификаторов соединения.

5.4. Версия

Поле Version содержит 4-байтовый идентификатор, который может применяться конечными точками для указания версии QUIC. Поле Version = 0x00000000 зарезервировано для согласования версии (см. раздел 6), все остальные значения могут быть действительными.

Описанные в этом документе свойства применимы ко всем версиям QUIC. Протокол, не соответствующий описанным в этом документе свойствам, не является QUIC. В будущих документах могут описываться другие свойства, применимые к конкретной версии или диапазону версий QUIC.

6. Согласование версий

Конечная точка QUIC, получившая пакет с длинным заголовком и версией, которую она не понимает или не поддерживает, может передать в ответ пакет Version Negotiation. Пакеты с коротким заголовком не вызывают согласования версии.

В пакете Version Negotiation установлен (1) старший бит первого байта, задающий длинный заголовок, как описано в параграфе 5.1. Пакет Version Negotiation идентифицируется в качестве такового по полю Version = 0x00000000.

```
Version Negotiation Packet {
  Header Form (1) = 1,
  Unused (7),
  Version (32) = 0,
  Destination Connection ID Length (8),
  Destination Connection ID (0..2040),
  Source Connection ID Length (8),
  Source Connection ID (0..2040),
  Supported Version (32) ...,
}
```

Рисунок 4. Пакет согласования версии.

В первом байте пакета Version Negotiation определено значение лишь старшего бита (1), а остальные 7 битов, помеченные как Unused, могут иметь любые значения при передаче и **должны** игнорироваться получателем.

После поля Source Connection ID в пакете Version Negotiation содержатся пола Supported Version, каждое из которых указывает версию, поддерживаемую отправившей пакет конечной точкой. Других полей пакет Version Negotiation не содержит. Конечная точка **должна** игнорировать пакет без поля Supported Version или с усечённым полем. Для пакетов Version Negotiation не обеспечивается защиты целостности и конфиденциальности. Конкретные версии QUIC могут включать элементы протокола, позволяющие конечным точкам обнаруживать изменение или повреждения списка поддерживаемых версий.

Конечная точка **должна** включать значение Source Connection ID из полученного пакета в поле Destination Connection ID. Значение Source Connection ID **должно** копироваться из поля Destination Connection ID в полученном пакете, которое исходно клиент задаёт случайным. Указание обоих идентификаторов соединения даёт клиенту некоторую уверенность в том, что сервер получил пакет, а пакет Version Negotiation не создан злоумышленником, способным наблюдать пакеты.

Получившая пакет Version Negotiation конечная точка может сменить версию для последующих пакетов. Условия смены конечной точкой версии QUIC зависят от выбираемой версии.

В документе [QUIC-TRANSPORT] приведено более подробное описание генерации и использования пакетов Version Negotiation конечной точкой, поддерживающей QUIC версии 1.

7. Вопросы безопасности и приватности

Возможны ситуации, когда промежуточные устройства способны видеть черты конкретной версии QUIC и предполагать ту же семантику, когда другая версия QUIC демонстрирует аналогичные черты. Таких черт может быть много, см.

Приложение A. Были предприняты попытки устранить или скрыть наблюдаемые черты в QUIC версии 1, но многие из них остались. В других версиях QUIC могут применяться иные решения и проявляться другие черты.

Номер версии QUIC не указывается в пакетах QUIC, что означает необходимость сохранение на промежуточных устройствах состояния для каждого видимого идентификатора соединения, чтобы надёжно извлечь информацию из потока на основе наблюдаемых черт версии.

Описанный в этом документе пакет Version Negotiation не имеет защиты целостности и лишь слегка защищён от злоумышленников. Конечная точка **должна** проверять подлинность смыслового содержимого Version Negotiation, если она пытается в результате сменить версию QUIC.

8. Литература

8.1. Нормативные документы

[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>.

[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>.

8.2. Дополнительная литература

[QUIC-TLS] Thomson, M., Ed. and S. Turner, Ed., "Using TLS to Secure QUIC", RFC 9001, DOI 10.17487/RFC9001, May 2021, <https://www.rfc-editor.org/info/rfc9001>.

[QUIC-TRANSPORT] Iyengar, J., Ed. and M. Thomson, Ed., "QUIC: A UDP-Based Multiplexed and Secure Transport", RFC 9000, DOI 10.17487/RFC9000, May 2021, <https://www.rfc-editor.org/info/rfc9000>.

[RFC5116] McGrew, D., "An Interface and Algorithms for Authenticated Encryption", RFC 5116, DOI 10.17487/RFC5116, January 2008, <https://www.rfc-editor.org/info/rfc5116>.

Приложение A. Некорректные допущения

Имеются некоторые черты QUIC версии 1 [QUIC-TRANSPORT], не защищённые от наблюдения, но тем не менее, считающиеся изменяемыми в новых версиях. В этом приложении приведены примеры некорректных допущений, которые могут быть приняты на основе сведений о QUIC версии 1. Некоторые из приведённый утверждений неверны даже для QUIC версии 1. Список не является полным и служит лишь иллюстрацией. **Любое из приведённых ниже утверждений может быть ошибочным для конкретной версии QUIC.**

- QUIC использует TLS [QUIC-TLS] и некоторые сообщения TLS видимы в линии.
- Длинные заголовки QUIC передаются лишь при организации соединения.
- Каждый поток данного квинтета (5-tuple) включает фазу организации соединения.
- Первые пакеты в потоке используют длинный заголовок.
- Можно предположить, что последний поток перед долгим бездействием содержит лишь подтверждение.
- QUIC использует функцию аутентифицированного шифрования со связанными данными (Authenticated Encryption with Associated Data или AEAD) AEAD_AES_128_GCM [RFC5116] для защиты пакетов в процессе организации соединения.
- Номера пакетов QUIC шифруются и указываются в первых шифрованных байтах.
- Номера пакетов QUIC увеличиваются на 1 в каждом передаваемом пакете.
- QUIC устанавливает минимальный размер для первого пакета согласования, передаваемого клиентом.
- QUIC требует, чтобы соединение инициировал (начинал «говорить») клиент.
- В пакетах QUIC второй бит первого байта (0x40) всегда установлен (1).
- Пакеты QUIC Version Negotiation передаёт только сервер.
- Идентификаторы соединения QUIC меняются нечасто.
- Конечные точки QUIC меняют применяемую версию, если передан пакет Version Negotiation.
- Поле Version в пакетах QUIC с длинным заголовком одинаково для обоих направлений.
- Пакет QUIC с определенным значением поля Version означает использование соответствующей версии QUIC.
- Между парой взаимодействующих конечных точек QUIC в каждый момент имеется лишь одно соединение.

Адрес автора

Martin Thomson
Mozilla
Email: mt@lowentropy.net

Перевод на русский язык

Николай Малых

nmalykh@protokols.ru