Internet Engineering Task Force (IETF)
Request for Comments: 9462
Category: Standards Track
ISSN: 2070-1721

T. Pauly
E. Kinnear
Apple Inc.
C. A. Wood
Cloudflare
P. McManus
Fastly
T. Jensen
Microsoft

November 2023

Discovery of Designated Resolvers

Обнаружение назначенных распознавателей

Аннотация

Этот документ задаёт для клиентов DNS набор механизмов обнаружения назначенных распознавателей (Discovery of Designated Resolvers или DDR) путём использования записей DNS для обнаружения шифрованной конфигурации распознавателя DNS. Распознаватели с шифрованием (Encrypted DNS Resolver), найденные таким способом, называются назначенными распознавателями (Designated Resolver). Эти механизмы могут служить для перехода от DNS без шифрования к шифрованной системе DNS, когда известен лишь IP-адрес распознавателя. Механизмы предназначены лишь для случаев, когда распознаватели DNS без шифрования и соответствующие назначенные распознаватели работают на одном или согласованных объектах (сущностях). Они могут также применяться для обнаружения поддержки протоколов DNS с шифрованием, когда известно имя распознавателя DNS с шифрованием.

Статус документа

Документ относится к категории Internet Standards Track.

Документ 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/rfc9462.

Оглавление

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

1. Ведение

Клиентам DNS, желающим использовать шифрованные протоколы DNS, такие как DNS over TLS (DoT) [RFC7858], DNS over QUIC (DoQ) [RFC9250], DNS over HTTPS (DoH) [RFC8484], может потребоваться дополнительная информация о сервере DNS (не только адрес IP), такая как имя хоста распознавателя, дополнительные адреса IP, нестандартные порты, шаблоны URI. Обнако базовые механизмы конфигурации предоставляют для настройки лишь IP-адрес распознавателя. К таким механизмам относятся протокол поддержки DHCP [RFC2132] [RFC8415] опции анонсирования маршрутизаторов (IPv6 Router Advertisement или RA) [RFC8106], а также настройка вручную.

Этот документ определяет два механизма обнаружения клиентами назначенных маршрутизаторов, поддерживающих протоколы с шифрованием, на основе записей о привязке серверов DNS (server Service Binding или SVCB) [RFC9460].

1. Если известен лишь IP-адрес распознавателя DNS без шифрования, клиент запрашивает специальное доменное имя (Special-Use Domain Name или SUDN) [RFC6761] для нахождения записей DNS SVCB, связанных связанных с одним или несколькими распознавателями DNS с шифрованием, которые распознаватель без шифрования назначил для использования при запросе шифрования DNS (раздел 4).

2. Если известно имя хоста распознавателя DNS с шифрованием, клиент узнаёт детали, передавая запрос для записи DNS SVCB. Это может служить для обнаружения дополнительных шифрованных протоколов DNS, поддерживаемых известным сервером, или для получения подробностей, если имя распознавателя предоставляется сетью (раздел 5).

Оба подхода позволяют клиенту подтвердить, что обнаруженный распознаватель DNS с шифрованием назначен исходно предоставленным распознавателем. Назначение в этом контексте говорит о том, что распознаватели контролирует один субъект или сотрудничающие субъекты. Например, распознаватели доступны по одному адресу IP или имеется сертификат, содержащий IP-адрес исходно назначенного распознавателя.

1.1. Уровни требований

Ключевые слова **необходимо** (MUST), **недопустимо** (MUST NOT), **требуется** (REQUIRED), **нужно** (SHALL), **не нужно** (SHALL NOT), **следует** (SHOULD), **не следует** (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.

2. Терминология

DDR
: Обнаружение назначенных распознавателей (Discovery of Designated Resolver) - механизм, заданный здесь.

Designated Resolver - назначенный распознаватель
: Распознаватель (предположительно с шифрованием), назначенный другим распознавателем для использования вместо себя. Назначение можно проверить с помощью сертификатов TLS.

Encrypted DNS Resolver - распознаватель DNS с шифрованием
: Распознаватель, использующий шифрованный транспорт DNS, включая DoH, DoT, DoQ и будущие механизмы.

Unencrypted DNS Resolver - распознаватель DNS без шифрования
: Распознаватель DNS, использующий транспорт без шифрования (исторически это TCP или UDP через порт 53).

3. Записи о привязке служб DNS

Распознаватели DNS могут анонсировать один или несколько назначенных распознавателей, которые могут предлагать поддержку через шифрованные каналы и контролироваться той же стороной.

Когда клиент обнаруживает назначенные распознаватели, он получает такие сведения, как поддерживаемые протоколы и порты. Эта информация предоставляется в записях SVCB ServiceMode для серверов DNS, хотя могут использоваться и записи SVCB AliasMode для направления клиента к нужной записи SVCB ServiceMode в соответствии с [RFC9460]. Формат этих записей, включая уникальные для DNS параметры, такие как dohpath, задан в [RFC9461].

Ниже приведён пример записи SVCB, описывающей сервер DoH, найденный по запросу _dns.example.net

```
_dns.example.net.  7200  IN SVCB 1 example.net. (
      alpn=h2 dohpath=/dns-query{?dns} )
```

Следующий пример показывает запись SVCB, описывающую сервер DoT, найденный по запросу _dns.example.net

```
_dns.example.net.  7200  IN SVCB 1 dot.example.net (
      alpn=dot port=8530 )
```

В следующем примере указана запись SVCB, описывающая сервер DoQ, найденный по запросу _dns.example.net

```
_dns.example.net.  7200  IN SVCB 1 doq.example.net (
      alpn=doq port=8530 )
```

Если найдено несколько назначенных распознавателей, поддерживающих один или несколько протоколов DNS с шифрованием, могут быть указаны предпочтения с помощью полей приоритета в каждой записи SVCB [RFC9460].

Если клиент встречает в записи SVCB непонятный ему обязательный параметр, ему **недопустимо** использовать эту запись для обнаружения распознавателя в соответствии с разделом 8 в [RFC9460]. Клиент может использовать другие записи из того же отклика, если ему понятны обязательные параметры в них. Это позволяет будущим системам с шифрованием одновременно поддерживать протоколы, даже если конкретный клиент не знает всех этих протоколов. Например, если распознаватель DNS без шифрования возвращает 3 записи SVCB - одну для DoH, одну для DoT и одну для ещё несуществующего протокола, - клиент, поддерживающий только DoH и DoT сможет использовать две записи, игнорируя третью.

Для предотвращения тупиковых ситуаций, использующему назначенные распознаватели клиенту нужно убедиться, что конкретный распознаватель DNS с шифрованием не используется для каких-либо запросов, требуемых для распознавания имени самого распознавателя, или проверить статус отзыва сертификата распознавателя, как описано в разделе 10 [RFC8484]. Назначенные распознаватели должны предотвращать такие тупиковые ситуации, как описано в разделе 10 [RFC8484].

Этот документ сосредоточен на обнаружении назначенных распознавателей DoH, DoT и DoQ. Другие протоколы также могут применять формат, заданный в [RFC9461]. Однако, если такой протокол не включает какой-либо проверки сертификатов, потребуется определить новые механизмы проверки назначения, как описано в параграфе 4.2.

4. Обнаружение с использованием IP-адресов распознавателей

Когда на клиенте DNS настроен IP-адрес распознавателя DNS без шифрования, ему **следует** запросить у распознавателя записи SVCB службы со схемой dns и основанием (authority) resolver.arpa до выполнения других запросов. Это позволит клиенту перейти на использование DNS с шифрованием для всех других запросов, если это возможно. Клиент передаёт запрос для _dns.resolver.arpa. С типом записи SVCB (64) [RFC9460].

Отклики на запрос SVCB для SUDN resolver.arpa описывают назначенные распознаватели. Чтобы можно гарантированно различить конфигурации назначенных распознавателей и связать их с записями A и AAAA, в откликах SVCB ServiceMode на эти запросы **недопустимо** использовать значение . или resolver.arpa для TargetName. Клиентам **недопустимо** выполнять запросы A и AAAA для resolver.arpa.

Ниже приведён пример записи SVCB, описывающей сервер DoH, найденный по запросу _dns.resolver.arpa.

```
_dns.resolver.arpa.  7200  IN SVCB 1 doh.example.net (
      alpn=h2 dohpath=/dns-query{?dns} )
```

В следующем примере показана запись SVCB, описывающая сервер DoT, найденный по запросу _dns.resolver.arpa.

```
_dns.resolver.arpa.  7200  IN SVCB 1 dot.example.net (
      alpn=dot port=8530 )
```

Следующий пример показывает запись SVCB, описывающую сервер DoQ, найденный по запросу _dns.resolver.arpa.

```
_dns.resolver.arpa.  7200  IN SVCB 1 doq.example.net (
      alpn=doq port=8530 )
```

Если получивший такой запрос рекурсивных распознаватель имеет один или несколько назначенных распознавателей, он возвращает соответствующие записи SVCB. При ответе на специальные запросы для resolver.arpa распознавателю **следует** включать записи A и AAAA для имени назначенного распознавателя в раздел Additional Answers. Это избавит сервер DNS от лишнего кругового обхода для извлечения адреса назначенного распознавателя (раздел 5 [RFC9460]).

Назначенным распознавателям **следует** быть доступными с использованием семейств адресов IP, поддерживаемых связанными с ними распознавателями DNS без шифрования. Если распознаватель DNS без шифрования доступен по адресу IPv4, он должен предоставлять запись A с адресом IPv4 назначенного распознавателя, а при доступности по адресу IPv6 - запись AAAA с адресом IPv6 назначенного распознавателя. Назначенный распознаватель **может** поддерживать больше семейств адресов, чем распознаватель DNS без шифрования, но ему **не следует** поддерживать меньше. Если это не сделать, клиенты со связностью лишь по одному семейству адресов могут остаться без доступа к назначенному распознавателю.

Если у получившего такой запрос рекурсивного распознавателя нет назначенных распознавателей, ему **следует** возвращать NODATA для запросов зоны resolver.arpa, чтобы клиент получил чёткий сигнал отсутствия назначенных распознавателей.

4.1. Использование назначенных распознавателей

При получении клиентом назначенных распознавателей по адресу IP распознавателя DNS без шифрования, он может использовать эти распознаватели (1) автоматически, (2) на основе эвристических правил или по выбору пользователя. Этот документ задаёт два предпочтительных метода автоматического применения назначенных распознавателей.

- Проверяемое обнаружение (параграф 4.2), когда может использоваться сертификат TLS для проверки отождествления распознавателя.
- Гибкое обнаружение (параграф 4.3), когда IP-адрес распознавателя является приватным или локальным.

Клиент также **может** использовать найденные назначенные распознаватели без применения этих методов, на основе связанных с реализацией правил или по воле пользователя. Детали такого применения выходят за рамки документа. Клиентам **недопустимо** автоматически применять назначенные распознаватели без той или иной проверки, такой как указанные выше методы или будущие механизмы. Использование без проверки может позволить злоумышленнику направить трафик на распознаватель DNS с шифрованием, который не связан с исходным распознавателем DNS без шифрования, как описано в разделе 7. Клиенту **недопустимо** использовать назначение, обнаруженные по IP-адресу одного распознавателя DNS без шифрования, вместо другого распознавателя DNS без шифрования. Вместо этого клиенту нужно повторить процесс обнаружения для получения назначенных распознавателей от другого распознавателя DNS без шифрования. Иными словами, назначения привязаны к распознавателю и **недопустимо** использовать их для универсального поведения клиента DNS. Это гарантирует отправку всех запросов стороне, назначенной используемым распознавателем.

4.1.1. Использование назначенных распознавателей при смене сети

Если у клиента настроен один IP-адрес распознавателя DNS без шифрования для нескольких разных сетей, назначенные распознаватели, найденные для одной сети, **не следует** использовать в других сетях без повторения процесса обнаружения в каждой сети, поскольку адрес IP может применяться для разных серверах в разных сетях.

4.2. Проверяемое обнаружение

Механизм обнаружения с проверкой (Verified Discovery) позволяет автоматически применять назначенный распознаватель с шифрованием DNS, поддерживающий согласование TLS.

Чтобы назначенный распознаватель был сочтён действительным, представленный им сертификат TLS должен пройти у клиента указанные ниже проверки.

1. Клиент **должен** проверить цепочку сертификатов до корня доверия, как описано в разделе 6 [RFC5280]. Клиенту **следует** использовать принятые в системе или приложении привязки доверия, если не задано иное.

2. Клиент **должен** проверить наличие в сертификате IP-адреса назначающего распознавателя DNS без шифрования (запись iPAddress расширения subjectAltName), как описано в параграфе 4.2.1.6 [RFC5280].

Если эти проверки прошли, клиенту **следует** использовать обнаруженный назначенный распознаватель во всех случаях, где он использовал бы распознаватель DNS без шифрования, чтобы, по возможности, работать с шифрованным DNS.

Если проверки не прошли, клиенту **недопустимо** применять автоматически обнаруженный назначенный распознаватель, если назначение было обнаружено только через запрос _dns.resolver.arpa. (объявленное сетью напрямую назначение можно использовать, как описано в параграфе 6.5). Кроме того, клиенту **следует** запретить любые последующие запросы к назначенным распознавателям, использующим этот распознаватель DNS без шифрования, на время, указанное в записи SVCB полем Time to Live (TTL), чтобы избежать избыточных запросов, которые приведут к отрицательному результату проверки. Клиент **может** выдавать новые запросы, если значение SVCB TTL слишком велико (по правилам клиента) для минимизации времени, на которое злоумышленник может остановить использование DNS с шифрованием.

Если назначенный распознаватель и распознаватель DNS без шифрования имеют один адрес IP, клиент **может** выбрать гибкое применение назначенного распознавателя даже без проверки сертификата (параграф 4.3). Если адреса IP различаются, гибкий подход к использованию opportunistic позволит злоумышленникам перенаправить запросы на сторонний распознаватель DNS с шифрованием, как описано в разделе 7.

В соединениях с назначенным распознавателем могут применяться адреса IP, отличные от адреса распознавателя DNS без шифрования, например, при получении дополнительных адресов в процессе распознавания сервиса SVCB. Даже при использовании для соединения другого адреса IP описанная выше проверка сертификата TLS применяется к исходному IP-адресу распознавателя DNS без шифрования.

4.3. Гибкое обнаружение

В некоторых случаях распознавание с проверкой для конфигурации DNS с шифрованием через DNS без шифрования невозможно. Например, распознаватели DNS без шифрования с приватными адресами IP [RFC1918], уникальными локальными адресами (Unique Local Addresses или ULA) [RFC4193] и адресами Link-Local [RFC3927] [RFC4291] в большинстве случаев невозможно надёжно проверить с использованием сертификатов TLS.

Гибкий (opportunistic) профиль приватности определён для DoT в параграфе 4.1 of [RFC7858] как режим, в котором клиенты не проверяют имя распознавателя, представленное в сертификате. Такой профиль применим и к DoQ [RFC9250]. Для этого профиля в параграфе 4.1 [RFC7858] сказано, что клиенты могут (но не обязаны) проверить распознаватель. Однако даже при выборе клиентом проверки он не сможет проверить имена, представленные в поле SubjectAltName (SAN) для приватных и локальных адресов IP.

Клиент **может** использовать сведения из записи SVCB для _dns.resolver.arpa. с этим гибким профилем, пока IP-адрес распознавателя DNS с шифрованием не отличается от адреса распознавателя DNS без шифрования. Клиентам **следует** применять этот режим только для распознавателей с приватными или локальными адресами IP, поскольку распознаватели с другими адресами могут предоставлять сертификаты TLS для своих адресов.

5. Обнаружение по имени распознавателя

Клиент DNS, уже знающий имя распознавателя DNS с шифрованием, может использовать DDR для получения сведений обо всех поддерживаемых протоколах DNS с шифрованием. Такая ситуация может возникать, когда клиент настроен на использование данного распознавателя DNS с шифрованием или протокол поддержки (например, DHCP или IPv6 RA) предоставляет имя распознавателя DNS с шифрованием вместе с его адресов IP, как при обнаружении назначенных сетью распознавателей с шифрованием (Discovery of Network-designated Resolvers или DNR) [RFC9463]. В таких случаях клиент просто отправляет запрос DNS SVCB, используя известное имя распознавателя. Запрос может быть отправлен самому распознавателю DNS с шифрованием или любому другому распознавателю. В отличие от случая загрузки с распознавателя DNS без шифрования (раздел 4), этим записям **следует** быть доступными в DNS общего пользования, если записи A или AAAA для того же имени доступны в DNS общего пользования, чтобы любой распознаватель мог обнаружить назначенные распознаватели. Когда имя распознаётся лишь в частном пространстве имён, эти записи **следует** делать доступными тем же, кто имеет доступ к записям A и AAAA. Например, если клиент уже знает о сервере DoT resolver.example.com, он может отправить запрос SVCB для _dns.resolver.example.com, чтобы узнать, доступны ли другие протоколы DNS с шифрованием. Ниже приведены отклики SVCB, указывающие, что resolver.example.com поддерживает DoH и DoT, а сервер DoH имеет более высокий приоритет, нежели сервер DoT.

```
_dns.resolver.example.com.  7200  IN SVCB 1 resolver.example.com. (
     alpn=h2 dohpath=/dns-query{?dns} )
_dns.resolver.example.com.  7200  IN SVCB 2 resolver.example.com. (
     alpn=dot )
```

Клиент **должен** убедиться, что для любого распознавателя DNS с шифрованием, обнаруженного по известному имени распознавателя, сертификат TLS содержит известное имя в расширении subjectAltName. В приведённом выше примере это означает, что оба сервера должны иметь сертификаты, охватывающие имя resolver.example.com. Поддерживаемые протоколы DNS с шифрованием часто задаются так, что SVCB TargetName соответствует известному имени, как в примере выше. Однако даже при разных TargetName (например, если сервер DoH имеет TargetName doh.example.com) клиенты всё равно проверяют наличие в сертификате известного имени исходного распознавателя. Отметим, что такая проверка не относится к распознавателю DNS из отклика SVCB. Ещё одним примером является возможность найти назначенный распознаватель для известного распознавателя DNS с шифрованием, которая полезна при наличии у клиента конфигурации DoT для foo.resolver.example.com в сочетании с блокировкой в сети трафика DoT. Клиент всё равно может отправить запрос любому доступному распознавателю (например, локальному или доступному серверу DoH), чтобы найти назначенный сервер DoH для foo.resolver.example.com.

6. Вопросы внедрения

При внедрении распознавателей с поддержкой DDR рекомендуется рассмотреть отмеченные ниже аспекты.

6.1. Пересылающие узлы с кэшированием

Пересылающему элементу DNS (forwarder) **не следует** пересылать наверх запросы для resolver.arpa (и субдоменов). Это предотвратит получение клиентом записей SVCB, которые не пройдут проверку подлинности, поскольку IP-адрес пересылающего не указан в поле SubjectAltName (SAN) сертификата TLS назначенного распознавателя у восходящего распознавателя. Пересылающий узел DNS, который уже действует как совершенно прозрачный, **может** пересылать такие запросы, когда оператор считает, что это ограничение не применимо, поскольку ему известно, что поле SAN в сертификате TLS содержит IP-адрес пересылающего или он предполагает проверку соединений клиентами с помощью каких-либо будущих механизмов. Операторам, решившим пересылать наверх запросы для resolver.arpa, следует помнить, что поведение должное клиентов не гарантируется, а использование DDR распознавателей не означает требования к клиентам использовать запись SVCB, если её невозможно проверить.

6.2. Управление сертификатами

Владельцы распознавателей, поддерживающих обнаружение с проверкой, должны указывать действительные ссылочные адреса IP в своих сертификатах TLS. Это может вызывать проблемы для распознавателей с большим число таких адресов.

6.3. Обработка имени сервера

Клиенту **недопустимо** использовать resolver.arpa в качестве имени сервера ни в (1) индикации имени сервера TLS (Server Name Indication или SNI) [RFC8446] для соединений DoT, DoQ, DoH, ни в (2) URI хоста для запросов DoH.

При обнаружении с использованием IP-адреса распознавателя клиенты **должны** использовать исходный адрес IP распознавателя DNS без шифрования в качестве URI хоста для запросов DoH.

Поскольку адреса IP по умолчанию не поддерживаются в TLS SNI, распознаватели, поддерживающие обнаружение по адресу IP, должны быть настроены на предоставление соответствующего сертификата TLS при отсутствии SNI для DoT, DoQ, DoH.

6.4. Обработка отличных от DDR запросов для resolver.arpa

Распознаватели DNS, которые поддерживают DDR, отвечая на запросы для _dns.resolver.arpa., **должны** считать resolver.arpa локально обслуживаемой зоной в соответствии с [RFC6303]. На практике это означает, что распознавателю **следует** отвечать NODATA на запросы любого типа, кроме SVCB, для _dns.resolver.arpa. и на запросы любого типа для доменных имён в дереве resolver.arpa.

6.5. Взаимодействие с назначенными сетью распознавателями

DNR [RFC9463] позволяет сети напрямую назначать распознаватели через DHCP [RFC2132] [RFC8415] и опции IPv6 RA [RFC8106]. При наличии таких указаний клиенты могут сдерживать запросы для resolver.arpa к серверу DNS без шифрования, указанному сетью через DHCP или RA, а указаниям DNR **следует** предоставлять более высокий приоритет по сравнению с обнаруженными с использованием resolver.arpa для того же распознавателя в случае возникновения конфликта, поскольку DNR считается более надёжным источником.

Сведения о назначенном распознавателе в DNR могут не содержать всех SvcParam, требуемых для подключения к распознавателю DNS с шифрованием. В таких случаях клиент может использовать запрос SVCB с именем распознавателя (см. раздел 5) для имени домена аутентификации (Authentication Domain Name или ADN).

7. Вопросы безопасности

Поскольку клиенты могут получать отклики DNS SVCB через DNS без шифрования, злоумышленники на пути могут препятствовать обнаружению, отбрасывая запросы или отклики SVCB и мешая переходу клиентов на использование DNS с шифрованием. Клиентам следует понимать, что может оказаться невозможным отличить распознаватели без назначенного распознавателя от такой активной атаки. Чтобы ограничить последствия вредоносного и непреднамеренного отбрасывания запросов обнаружения, клиенты могут периодически повторять запросы SVCB.

В параграфе 8.2 [RFC9461] описан другой тип атак с понижением, где злоумышленник может блокировать соединения с шифрованным DNS. В DDR клиенты должны проверять назначенный распознаватель до того, как доверять ему, используя соединение с сервером, поэтому атакующие, способные блокировать такие соединения могут помешать переходу клиента на использование DNS с шифрованием.

Распознавателям DNS с шифрованием, поддерживающим обнаружение с использованием откликов DNS SVCB через DNS без шифрования, **недопустимо** дифференцировать поведение лишь на основе метаданных в записи SVCB, таких как путь HTTP или альтернативный номер порта, которые злоумышленник может изменить. Например, если распознаватель DoH поддерживает службу с фильтрацией для одного пути URI и без фильтрации - для другого, атакующий может выбрать, какая из служб будет использоваться, путём изменения параметра dohpath. Такие атаки можно смягчить за счёт предоставляения распознавателям отдельных адресов IP или имён хостов.

Хотя IP-адрес распознавателя DNS без шифрования часто предоставляется через механизмы без защиты, его можно предоставлять и с защитой, например, через ручную настройку, VPN или сеть с защитой, вроде RA-Guard [RFC6105]. Атакующий может пытаться направить нешифрованный трафик DNS к себе, заставляя клиента думать, что найденный назначенный распознаватель использует не тот адрес IP, как у распознавателя DNS без шифрования. Такое назначенный распознаватель может иметь действительный сертификат, но находиться под управлением атакующего, который пытается отслеживать или изменять запросы пользователей без ведома их или сети.

Если IP-адрес назначенного распознавателя отличается от адреса распознавателя DNS без шифрования, клиенты, применяющие обнаружение с проверкой (параграф 4.2), **должны** убедиться, что IP-адрес распознавателя DNS без

шифрования охватывается полем SAN из сертификата TLS назначенного распознавателя. Если проверка не прошла, клиенту **недопусимо** автоматически использовать обнаруженный назначенный распознаватель.

Клиенты, использующие гибкое обнаружение (параграф 4.3), **должны** ограничиваться случаями, где у распознавателя DNS без шифрования и назначенного распознавателя совпадает IP-адрес, которому **следует** быть приватным или локальным. Клиентам, которые не следуют гибкому обнаружению (параграф 4.3) и пытаются соединиться без предварительной проверки адресата, подвергаются риску перехвата злоумышленником, поместившим распознаватель DNS с шифрованием по адресу IP распознавателя DNS без шифрования, если ему не удалось получить контроль над распознавателем DNS без шифрования.

Указанные здесь ограничения на использование назначенных распознавателей применимы к механизмам автоматического обнаружения, заданным в этом документе как Verified Discovery и Opportunistic Discovery. Клиенты **могут** применять иные механизмы для проверки и использования назначенных распознавателей, обнаруженным с помощью записей DNS SVCB. Однако при использовании таких механизмов требуется учитывать описанные здесь варианты атак.

8. Взаимодействие с IANA

8.1. Специальный домен resolver.arpa

Агентство IANA зарегистрировало имя resolver.arpa в реестре Special-Use Domain Names, заданном [RFC6761].

Агентство IANA добавило в реестр Transport-Independent Locally-Served DNS Zone Registry запись для resolver.arpa. с описанием DNS Resolver Special-Use Domain (специальный домен для распознавателей) и ссылкой на этот документ.

8.2. Вопросы резервирования доменных имён

В соответствви с разделом 5 в [RFC6761] ниже приведены ответы на вопросы, связанные с этим документом.

1. Предполагается ли, что пользователи (люди) будут считать эти имена особыми и использовать их по-особому? Каким образом?

   Нет. Это имя автоматически используется конечным (stub) распознавателем DNS на клиентском устройстве от имени пользователей, которые не видят само имя.

2. Должны ли создатели прикладных программ требовать от них считать эти имена особыми и использовать их по-особому? Каким образом?

   Нет. Не существует ни одного варианта применения, где не относящемуся к DNS приложению (см. следующий вопрос) требуется использовать это имя.

3. Должны ли авторы API и библиотек для распознавания имён требовать от них считать эти имена особыми и использовать их по-особому? Если да, то как?

   Да. Предполагается, что реализации клиентов DNS будут использовать эти имена при запросе свойств распознавателя вместо записей для самого имени. Ожидается, что серверы DNS будут отвечать на запросы для этих имён своими свойствами, а не проверять соответствующую зону как для обычных доменных имен.

4. Должны ли разработчики кэширующих серверов доменных имён требовать от них считать эти имена особыми и использовать их по-особому? Если да, то как?

   Да. Кэширующим серверам имён не следует пересылать запросы для таких имён, чтобы избежать отказов при проверке из-за несовпадения адресов IP.

5. Должны ли разработчики полномочных серверов имён требовать от них считать эти имена особыми и использовать их по-особому? Если да, то как?

   Нет. DDR предназначается для использования рекурсивными распознавателями. Теоретически полномочный сервер имён может поддерживать такие имена, если он хочет анонсировать предпочтение протоколов DNS с шифрованием перед открытыми протоколами DNS, но это рассматривается в рабочей группе IETF DNSOP.

6. Оказывает ли резервирование специального доменного имени влияние на операторов серверов DNS? Если они попытаются настроить свой полномочный сервер DNS как полномочный для этого имени, будет ли соответствующий спецификациям сервер отвергать его как недействительное? Нужно ли операторам серверов DNS знать это и понимать причины? Даже если программы сервера имён не препятствуют использованию зарезервированного имени, имеются ли другие варианты, при которых это может не работать ожидаемым образом и оператору сервера DNS следует знать об этом?

   Это имя обслуживается локально и поддерживающим его распознавателям не следует пересылать запросы для него. Операторам серверов DNS следует знать, что записи для этого имени будут применяться клиентами для изменения способа соединения с их распознавателями.

7. Как реестрам/регистраторам DNS следует относиться к запросам на регистрацию зарезервированного доменного имени? Следует ли отклонять такие запросы? Следует ли разрешать такие запросы, но лишь специально назначенным органам?

   Это имя зарегистрировано IANA и запросы других органов на регистрацию этого имени следует отклонять.

9. Литература

9.1. Нормативные документы

[RFC1918] Rekhter, Y., Moskowitz, B., Karrenberg, D., de Groot, G. J., and E. Lear, "Address Allocation for Private Internets", BCP 5, RFC 1918, DOI 10.17487/RFC1918, February 1996, <https://www.rfc-editor.org/info/rfc1918>.

[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>.

[RFC3927] Cheshire, S., Aboba, B., and E. Guttman, "Dynamic Configuration of IPv4 Link-Local Addresses", RFC 3927, DOI 10.17487/RFC3927, May 2005, <https://www.rfc-editor.org/info/rfc3927>.

[RFC4193] Hinden, R. and B. Haberman, "Unique Local IPv6 Unicast Addresses", RFC 4193, DOI 10.17487/RFC4193, October 2005, <https://www.rfc-editor.org/info/rfc4193>.

[RFC4291] Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", RFC 4291, DOI 10.17487/RFC4291, February 2006, <https://www.rfc-editor.org/info/rfc4291>.

[RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, DOI 10.17487/RFC5280, May 2008, <https://www.rfc-editor.org/info/rfc5280>.

[RFC6303] Andrews, M., "Locally Served DNS Zones", BCP 163, RFC 6303, DOI 10.17487/RFC6303, July 2011, <https://www.rfc-editor.org/info/rfc6303>.

[RFC6761] Cheshire, S. and M. Krochmal, "Special-Use Domain Names", RFC 6761, DOI 10.17487/RFC6761, February 2013, <https://www.rfc-editor.org/info/rfc6761>.

[RFC7858] Hu, Z., Zhu, L., Heidemann, J., Mankin, A., Wessels, D., and P. Hoffman, "Specification for DNS over Transport Layer Security (TLS)", RFC 7858, DOI 10.17487/RFC7858, May 2016, <https://www.rfc-editor.org/info/rfc7858>.

[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>.

[RFC8484] Hoffman, P. and P. McManus, "DNS Queries over HTTPS (DoH)", RFC 8484, DOI 10.17487/RFC8484, October 2018, <https://www.rfc-editor.org/info/rfc8484>.

[RFC9250] Huitema, C., Dickinson, S., and A. Mankin, "DNS over Dedicated QUIC Connections", RFC 9250, DOI 10.17487/RFC9250, May 2022, <https://www.rfc-editor.org/info/rfc9250>.

[RFC9460] Schwartz, B., Bishop, M., and E. Nygren, "Service Binding and Parameter Specification via the DNS (SVCB and HTTPS Resource Records)", RFC 9460, DOI 10.17487/RFC9460, November 2023, <https://www.rfc-editor.org/info/rfc9460>.

[RFC9461] Schwartz, B., "Service Binding Mapping for DNS Servers", RFC 9461, DOI 10.17487/RFC9461, November 2023, <https://www.rfc-editor.org/info/rfc9461>.

[RFC9463] Boucadair, M., Ed., Reddy.K, T., Ed., Wing, D., Cook, N., and T. Jensen, "DHCP and Router Advertisement Options for the Discovery of Network-designated Resolvers (DNR)", RFC 9463, DOI 10.17487/RFC9463, November 2023, <https://www.rfc-editor.org/info/rfc9463>.

9.2. Дополнительная литература

[DoH-HINTS] Schinazi, D., Sullivan, N., and J. Kipp, "DoH Preference Hints for HTTP", Work in Progress, Internet-Draft, draft-schinazi-httpbis-doh-preference-hints-02, 13 July 2020, <https://datatracker.ietf.org/doc/html/draft-schinazi-httpbis-doh-preference-hints-02>.

[ECH] Rescorla, E., Oku, K., Sullivan, N., and C. A. Wood, "TLS Encrypted Client Hello", Work in Progress, Internet-Draft, draft-ietf-tls-esni-17, 9 October 2023, <https://datatracker.ietf.org/doc/html/draft-ietf-tls-esni-17>.

[RFC2132] Alexander, S. and R. Droms, "DHCP Options and BOOTP Vendor Extensions", RFC 2132, DOI 10.17487/RFC2132, March 1997, <https://www.rfc-editor.org/info/rfc2132>.

[RFC6105] Levy-Abegnoli, E., Van de Velde, G., Popoviciu, C., and J. Mohacsi, "IPv6 Router Advertisement Guard", RFC 6105, DOI 10.17487/RFC6105, February 2011, <https://www.rfc-editor.org/info/rfc6105>.

[RFC8106] Jeong, J., Park, S., Beloeil, L., and S. Madanapalli, "IPv6 Router Advertisement Options for DNS Configuration", RFC 8106, DOI 10.17487/RFC8106, March 2017, <https://www.rfc-editor.org/info/rfc8106>.

[RFC8415] Mrugalski, T., Siodelski, M., Volz, B., Yourtchenko, A., Richardson, M., Jiang, S., Lemon, T., and T. Winters, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 8415, DOI 10.17487/RFC8415, November 2018, <https://www.rfc-editor.org/info/rfc8415>.

[RFC8446] Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", RFC 8446, DOI 10.17487/RFC8446, August 2018, <https://www.rfc-editor.org/info/rfc8446>.

[RFC8880] Cheshire, S. and D. Schinazi, "Special Use Domain Name 'ipv4only.arpa'", RFC 8880, DOI 10.17487/RFC8880, August 2020, <https://www.rfc-editor.org/info/rfc8880>.

Приложение A. Обоснование использования специального домена

Специальное доменное имя (SUDN) resolver.arpa похоже на ipv4only.arpa в том смысле, что запрашивающему клиенту не нужен ответ от полномочных серверов имён arpa. Назначение SUDN состоит в том, чтобы позволить клиентам взаимодействовать с распознавателем DNS без шифрования, подобно тому, как ipv4only.arpa позволяет клиентам взаимодействовать с посредниками. Более подробное обоснования для ipv4only.arpa приведено в [RFC8880].

Приложение B. Обоснование использования записей SVCB

Эти механизмы используют записи о ресурсах SVCB/HTTPS [RFC9460] для передачи сведений о том, что данный домен назначил определённый распознаватель для использования клиентами вместо распознавателя DNS без шифрования (с использованием SUDN) или другого распознавателя DNS с шифрованием (с использованием доменного имени).

Имеются и другие предложения в части предоставления похожих функций. Записи SVCB выбраны для этих механизмов по нескольким причинам.

- Обнаружение распознавателей DNS с шифрованием по записям DNS сохраняет логику клиентов для DNS автономной и позволяет операторам распознавателей DNS задавать, какие имена и IP-адреса распознавателей связаны друг с другом.
- Использование записей DNS не требует начальной загрузки с операциями приложений верхнего уровня (таких, какие рассматриваются в [DoH-HINTS]).
- Записи SVCB являются расширяемыми и позволяют определять ключи параметров, что делает их отличным механизмом расширения по сравнению с такими подходами, как перегрузка (overloading) записей TXT. Одни и те же ключи могут служить для обнаружения назначенных распознавателей с разными типами транспорта, а также анонсируемых распознавателями DNS без шифрования или другим распознавателем DNS с шифрованием.
- Клиентам и серверам, заинтересованным в приватности имён, уже требуется поддерживать записи SVCB для использования шифрованных приветствий TLS [ECH]. Без шифрования имён в TLS ценность шифрования DNS снижается, поэтому сочетание этих решений обеспечивает наибольшие преимущества.

Адреса авторов

Tommy Pauly
Apple Inc.
One Apple Park Way
Cupertino, California 95014
United States of America
Email: tpauly@apple.com

Eric Kinnear
Apple Inc.
One Apple Park Way
Cupertino, California 95014
United States of America
Email: ekinnear@apple.com

Christopher A. Wood
Cloudflare
101 Townsend St
San Francisco, California 94107
United States of America
Email: caw@heapingbits.net

Patrick McManus
Fastly
Email: mcmanus@ducksong.com

Tommy Jensen
Microsoft
Email: tojens@microsoft.com

Перевод на русский язык

Николай Малых

nmalykh@protokols.ru