Internet Engineering Task Force (IETF) B. Schwartz
Request for Comments: 9461 Meta Platforms, Inc.
Category: Standards Track November 2023
ISSN: 2070-1721

# Service Binding Mapping for DNS Servers

Отображение привязки служб для серверов DNS

**Аннотация**

Тип SVCB для записей о ресурсах DNS выражает связанную коллекцию метаданных конечной точки для использования при организации соединения с именованной службой. DNS теже может быть такой службой, когда сервер идентифицируется доменным именем. Этот документ предоставляет отображение SVCB для именованных серверов DNS, позволяющее им указывать поддержку транспортных протоколов 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/rfc9461.



# Оглавление

1. Введение....1
2. Уровни требований....2
3. Идентификаторы и имена....2
3.1. Использование портов, не принятых по умолчанию....2
4. Применимые имеющиеся ключи SvcParamKey....2
4.1. alpn....2
4.2. port....2
4.3. Другие применимые SvcParamKey....3
5. Новый ключ SvcParamKey dohpath....3
6. Ограничения....3
7. Примеры....3
8. Вопросы безопасности....3
8.1. Злоумышленник на пути запроса....3
8.1.1. Атаки с понижением....4
8.1.2. Атаки с перенаправлением....4
8.2. Злоумышленник на транспортном пути....4
9. Взаимодействие с IANA....4
10. Литература....4
10.1. Нормативные документы....4
10.2. Дополнительная литература....5
Приложение A. Сводка отображений....5
Благодарности....5
Адрес автора....5

## *1. Введение*

Тип SVCB для записей о ресурсах (RR) [SVCB] обеспечивает клиентам сведения для доступа к дополнительным конечным точкам сервиса. Эти точки могут предоставлять большую производительнсть или улучшенную защиту приватности. Службы идентифицируются схемой (scheme), указывающей тип сервиса, именем хоста, а также необязательными сведениями, такими как номер порта. Сервер DNS часто указывается лишь адресом IP (например, в DHCP), но в некоторых случаях может указываться также именем хоста (например, записи NS, настройка распознавателя вручную), а иногда и нестандартным номером порта.

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

Использование RR типа SVCB требует документа об отображении для каждого типа сервиса (параграф 2.4.3 в [SVCB]), указывающего, как клиент этой службы может интерпретировать содержимое SVCB SvcParam. Этот документ предоставляет отображение для сервиса типа dns, позволяющее серверам DNS предлагать дополнительные конечные точки и транспорт, включая шифрованный, например, DNS over TLS (DoT) [RFC7858], DNS over HTTPS (DoH) [RFC8484], DNS over QUIC (DoQ) [RFC9250].

Описанное в документе отображение SVCB предназначено в качестве базового для общего пользования. В последующих спецификациях этот механизм будет адаптирован для конкретных конфигураций (например, для взаимодействия оконечных и рекурсивных распознавателей).

# *2. 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.

# *3. Идентификаторы и имена*

Имена записей SVCB (т. е. QNAME) для служб DNS формируются с использованием префиксного именования портов (Port Prefix Naming, параграф 2.3 в [SVCB]) и схемы dns. Например, записи SVCB для сервиса DNS, идентифицируемого именем dns1.example.com, будут запрашиваться у _dns.dns1.example.com. В некоторых случаях имена, служащие для извлечения этих записей DNS отличаются от идентификатора сервера, применяемого для аутентификации защищённого транспорта. Чтобы различать их в документе применяются особые термины.

***Binding authority - основание привязки***
: Имя службы (параграф 1.3 в [SVCB]) и необязательный номер порта для ввода в префиксное именование порта.

***Authentication name - имя для аутентификации***
: Имя, служащее для аутентификации защищённого транспорта. Это **должно** быть DNS-имя хоста или литеральный адрес IP. Если не задано иное, это будет имя службы от органа привязки.

## 3.1. Использование портов, не принятых по умолчанию

Обычно служба DNS идентифицируется по адресу IP или доменному имени. При подключении к службе с использованием DNS без шифрования по протоколу UDP или TCP клиенты используют принятый по умолчанию порт DNS (53). Однако в редких случаях служба DNS может указываться именем и номером порта. Например, схема DNS URI [DNSURI] опционально включает основание (authority), состоящее из хоста и номера порта (по умолчанию 53). В DNS URI обычно не включается основание или указывается адрес IP, но разрешено имя хоста и отличный от принятого по умолчанию порт.

Если основеание привязки задаёт не используемый по умолчанию порт, префиксное именование пора указывает порт как дополнительный префикс имени. Например, если основанием привязки является dns1.example.com:9953, клиент будет запрашивать записи SVCB по _9953._dns.dns1.example.com. Если две службы DNS, работающие на разных портах, обеспечивают разное поведение, такая схема позволяет сохранить различие при указании дополнительных конечных точек.

# *4. Применимые имеющиеся ключи SvcParamKey*

## 4.1. alpn

Этот ключ указывает набор поддерживаемых протоколов (параграф 7.1 в [SVCB]). Принятого по умолчанию протокола нет, поэтому ключ no-default-alpn не применим. Если alpn SvcParamKey отсутствует, клиент **должен** считать запись SVCB «несовместимой» (как указано в разделе 8 [SVCB]), если только какой-то другой распознанный SvcParam не укзывает поддерживаемый протокол.

Если набор протоколов содержит какие-либо версии HTTP (например, h2, h3), запись указывает поддержку DoH и **должен** присутствовать ключ dohpath (раздел 5). Все ключи, указанные для использования с записью HTTPS, применимы к результирующему соединению HTTP.

Если набор содержит протоколы с другими портами по умолчанию и ключ port не указан, к этим протоколам обращаются отдельно через их принятый по умолчанию порт. Отметим, что в этой конфигурации согласование протокола прикладного уровня (Application-Layer Protocol Negotiation или ALPN) на защищает от кросс-протокольных атак с понижением.

## 4.2. port

Этот ключ указывает целевой порт для соединения (параграф 7.2 в [SVCB]) и при отсутствии ключа клиенту **нужно** обращаться в принятый по умолчанию порт лоя каждого транспортного протокола (853 для DoT и DoQ, 443 для DoH).

Ключ автоматически становится обязательным для данной привязки. Это означает, что клиент, не соблюдающий ключ port, **должен** игнорировать любые записи SVCB с таким ключом (определение «автоматической обязательности» дано в разделе 8 [SVCB]).

Поддержка ключа port может быть небезопасной, если клиент имеет неявный повышенный доступ к некой сетевой службе (например, к локальному сервису, недоступному удаленным сторонам) и этот сервис использует основанный на TCP протокол, отличный от TLS. Враждебный сервер DNS может оказаться способным манипулировать этой службой, заставив клиента отправить специально подготовленный индикатор TLS SNI (Server Name Indication) или сеансовую квитанцию, которые могут ошибочно разобраны как команда или эксплойт. Для предотвращения таких атак клиентам **не следует** поддерживать ключ port, пока не выполняется одно из указанных ниже условий.

- Клиент используется с сервером DNS, который является доверенным и не будет организовывать атак.
- Клиент будет использоваться в контексте, где неявное повышение уровня доступа не может быть применено.

- Клиент ограничивает набор разрешённых портов TCP с исключением любых портов, на которых представляется возможной атака с «путаницей» (см., например, список портов в параграфе 2.9 [FETCH]).

## 4.3. Другие применимые SvcParamKey

Перечисленные ниже ключи SvcParamKey из [SVCB] применимы к схеме dns без изменений.

- mandatory
- ipv4hint
- ipv6hint

Будущие ключи SvcParamKey также могут быть применимыми.

# *5. Новый ключ SvcParamKey dohpath*

Ключ dohpath - это SvcParamKey с одним значением, которое (в формате представления и в формате передачи) **должно** быть относительной формой URI Template (параграф 1.1 в [RFC6570]) с кодировкой UTF-8 [RFC3629]. Если alpn указывает поддежку HTTP, ключ dohpath **должен** присутствовать. В URI Template **должна** быть переменная dns и шаблон **должен** быть выбран так, что результат преобразования DoH URI Template (раздел 6 в [RFC8484]) всегда был действительным и являлся функциональным значением :path (параграф 8.3.1 в [RFC9113]).

При использовании такой записи SVCB клиент **должен** передавать любый запросв DoH источнику HTTP, указанному схемой https, именем для аутентификации и портом из port SvcParam (при наличии). Запросы HTTP **должны** направляться к ресурсу, полученному преобразованием DoH URI Template для значения dohpath.

Клиентам **не следует** запрашивать какие-либо HTTPS RR при использовании dohpath. Вместо этого **следует** использовать SvcParam и адресные записи, связанные с записью SVCB, для соединения HTTPS с той же семантикой, что и HTTPS RR. Однако для согласованности оператору сервиса **следует** публиковать эквивалент HTTPS RR, особенно в случаях, когда клиент может узнать о сервисе DoH через другой канал.

# *6. Ограничения*

Этот документ касается исключительно транспорта DNS и не влияет на построение и интерпретацию сообщений DNS. Например, ничто в этом документе не указывает, предназначена ли служба для использования в качестве рекурсивного или полномочного сервера DNS. Клиенту нужно узнавать назначение служб из контекста.

Не все функции из этой спецификации будут применимы или эффективны в любых условиях.

- Если имя для аутентификации получено по незащищённому каналу (например, склеивающая запись NS), эта спецификаци не может предотвратить соединение клиента со злоумышленником.
- Для разный целей (например, запросы к рекуривному распознавателю или полномочному серверу) может применяться разный транспорт. Разработчики не обязаны реализовать все определённые виды транспорта, хотя это обеспечивает преимущества в плане совместимости.
- Когда важна скорость распознавания для SVCB TargetName **следует** выполнять соглашение из параграфа 10.2 в [SVCB], а использовать записи AliasMode (параграф 2.4.2 в [SVCB]) **не рекомендуется**.

# *7. Примеры*

- Распознаватель, известный как simple.example и поддерживающий DNS через TLS на порту 853 (неявно, поскольку этот порт принят по умолчанию)

```
_dns.simple.example. 7200 IN SVCB 1 simple.example. alpn=dot
```

- Распознаватель с поддержкой только DoH по адресу https://doh.example/dns-query{?dns} (DNS через TLS не поддерживается)

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

- Распознаватель, известный как resolver.example и поддерживающий:
  - DoT на resolver.example через порты 853 (неявный в записи 1) и 8530 (явный в записи 2) с resolver.example как доменным именем для аутентификации;
  - DoQ на resolver.example через порт 853 (запись 1);
  - DoH по адресу https://resolver.example/q{?dns} (запись 1);
  - экспериментальный протокол на fooexp.resolver.example:5353 (запись 3)

```
_dns.resolver.example.  7200 IN \
  SVCB 1 resolver.example. alpn=dot,doq,h2,h3 dohpath=/q{?dns}
  SVCB 2 resolver.example. alpn=dot port=8530
  SVCB 3 fooexp.resolver.example. \
    port=5353 alpn=foo foo-info=...
```

- Сервер имён ns.example., конфигурация сервиса которого опубликована в другом домене

```
_dns.ns.example. 7200 IN SVCB 0 _dns.ns.nic.example.
```

# *8. Вопросы безопасности*

## 8.1. Злоумышленник на пути запроса

В этом разделе рассматриваются злоумышленники, способные добавлять или удалять отклики на запросы SVCB.

В процессе организации защищённого транспорта клиент **должен** проверить подлинность сервера по его аутентификационному имени, на которое не влияет содержимое записи SVCB. Поэтому документ не требует использования DNSSEC. Документ также не задаёт способ проверки клиентом подлинности имени (например, выбор корня доверия), поскольку это может меняться в зависимости от контекста.

### *8.1.1. Атаки с понижением*

Злоумышленник не может выдать себя за защищённую конечную точку, но может подменить отклик, указав, что запрошенной записи SVCB не существует. Для полагающегося на SVCB клиента (раздел 3 в [SVCB]), это ведёт лишь к отказу в обслуживании. Однако клиенты без обязательности SVCB в этом случае обычно будут возвращаться к DNS без защиты, раскрывая всеть трафик DNS для атак.

### *8.1.2. Атаки с перенаправлением*

Полагающиеся на SVCB клиенты всегда применяют Authentication Domain Name, но это не препятствует атакам с использованием транспорта, номера порта и значения dohpath, которые контролируются злоумышленником. Меняя эти значения в ответах SVCB, атакующий может направить запросы DNS для $HOSTNAME в любой порт $HOSTNAME и на любой путь https://$HOSTNAME. Если клиент DNS использует общее состояние TLS или HTTP, он может быть корректно аутентифицирован (например, по сертификату клиента TLS или HTTP cookie). Такое поведение создаёт возможность ряда атак для некоторых конфигураций серверов. Например, если https://$HOSTNAME/upload воспринимает любой запрос POST как общедоступную выгрузку файла, злоумышленник может подделать запись SVCB, содержащую dohpath=/upload{?dns}. Это заставит клиента выгружать и публиковать каждый запрос, что приведёт к непредвиденному заполнению хранилища сервера и потере приватности клиента. Аналогично, при доступности двух конечных точек DoH в одном источнике с назначением службой одной из точек для использования этой спецификации злоумышленник может вынудить клиентов использовать другую конечную точку.

Для смягчения атак с перенаправлением клиенту этого отображения SVCB **недопустимо** идентифицировать или аутентифицировать себя при выполнении запросов DNS, за исключением серверов, заведомо неуязвимых для таких атак. Если конечная точка передаёт недействительный отклик на запрос DNS, клиенту **не следует** отправлять ей дополнительные запросы, а ошибку **можно** занести в системный журнал. Нескольким службам DNS **недопустимо** использовать общее имя хоста (раздел 3), если только они не похожи настолько, что безопасно позволить злоумышленнику выбрать, какой из них использовать.

## 8.2. Злоумышленник на транспортном пути

В этом параграфе рассматриваются злоумышленники, способные изменить сетевой трафик между клиентом и дополнительным сервером (указанным TargetName).

Для полагающегося на SVCB клиента такой злоумышленник сможет вызвать лишь отказ в обслуживании. Однако DNS по умолчанию не шифруется и злоумышленник может выполнить атаку с понижением на клиентов, где SVCB не обязательно. Соответственно, при необязательности использования этой спецификации клиентам **следует** переключиться на поведение, основанное на SVCB, если распознавание SVCB успешно. Спецификации, использующие это отображение, **могут** настроить поведение отката в соответствии со своими требованиями.

# *9. Взаимодействие с IANA*

В соответствии с [SVCB] агентство IANA агентство IANA добавило указанную в таблице 1 запись в реестр Service Parameter Keys (SvcParamKeys).

*Таблица 1.*

| *Номер* | *Имя* | *Назначение* | *Документ для формата* | *Контролёр изменений* | *Документ* |
|---|---|---|---|---|---|
| 7 | dohpath | Шаблон пути HTTPS | DNS-over-RFC 9461 | IETF | RFC 9461 |

В соответствии с [Attrleaf] агентство IANA добавило указанную в таблице 2 запись в реестр Underscored and Globally Scoped DNS Node Names.

*Таблица 2.*

| *Тип RR* | *Имя _NODE* | *Документ* |
|---|---|---|
| SVCB | _dns | RFC 9461 |

# *10. Литература*

## 10.1. 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>.

[RFC3629] Yergeau, F., "UTF-8, a transformation format of ISO 10646", STD 63, RFC 3629, DOI 10.17487/RFC3629, November 2003, <https://www.rfc-editor.org/info/rfc3629>.

[RFC6570] Gregorio, J., Fielding, R., Hadley, M., Nottingham, M., and D. Orchard, "URI Template", RFC 6570, DOI 10.17487/RFC6570, March 2012, <https://www.rfc-editor.org/info/rfc6570>.

[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>.

[RFC9113] Thomson, M., Ed. and C. Benfield, Ed., "HTTP/2", RFC 9113, DOI 10.17487/RFC9113, June 2022, <https://www.rfc-editor.org/info/rfc9113>.

[SVCB] 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>.

## 10.2. Дополнительная литература

[Attrleaf] Crocker, D., "Scoped Interpretation of DNS Resource Records through "Underscored" Naming of Attribute Leaves", BCP 222, RFC 8552, DOI 10.17487/RFC8552, March 2019, <https://www.rfc-editor.org/info/rfc8552>.

[DNSURI] Josefsson, S., "Domain Name System Uniform Resource Identifiers", RFC 4501, DOI 10.17487/RFC4501, May 2006, <https://www.rfc-editor.org/info/rfc4501>.

[FETCH] WHATWG, "Fetch Living Standard", October 2023, <https://fetch.spec.whatwg.org/>.

[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>.

[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>.

# *Приложение A. Сводка отображений*

В таблице 3 приведена ненормативная сводка отображений DNS для SVCB.

*Таблица 3.*

| ***Отображаемая схема*** | ***"dns"*** |
|---|---|
| Тип RR | SVCB (64) |
| Префикс имени | _dns для порта 53, иначе _$PORT._dns |
| Требуемые ключи | alpn или эквивалент |
| Автоматически обязательные ключи | Порт |
| Специальное поведение | Поддержка всех HTTPS RR SvcParamKey<br>Переопределяет HTTPS RR для DoH<br>Принятый по умолчанию порт от транспорта<br>Откат к открытым данным не рекомендуется |

# *Благодарности*

Спасибо многочисленным рецензентам и участникам работы, включая Andrew Campling, Peter van Dijk, Paul Hoffman, Daniel Migault, Matt Nordhoff, Eric Rescorla, Andreas Schulze, Éric Vyncke.

# *Адрес автора*

**Benjamin Schwartz**
Meta Platforms, Inc.
Email: ietf@bemasc.net

**Перевод на русский язык**

Николай Малых

nmalykh@protokols.ru