Internet Engineering Task Force (IETF)
Request for Comments: 9463
Category: Standards Track
ISSN: 2070-1721

M. Boucadair, Ed.
Orange
T. Reddy.K, Ed.
Nokia
D. Wing
Cloud Software Group
N. Cook
Open-Xchange
T. Jensen
Microsoft

November 2023

DHCP and Router Advertisement Options for the Discovery of Network-designated Resolvers (DNR)

Опции DHCP и Router Advertisement для обнаружения назначенных сетью распознавателей

Аннотация

В этом документе заданы новые опции DHCP и IPv6 Router Advertisement для обнаружения распознавателей DNS с шифрованием (например, DNS over HTTPS, DNS over TLS, and DNS over QUIC). Они позволяют, в частности, хосту узнавать имя домена аутентификации (Authentication Domain Name) вместе со списком IP-адресов и набором параметров сервиса для доступа к распознавателям 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/rfc9463.

Оглавление

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

1. Введение

Этот документ посвящён обнаружению распознавателей DNS с шифрованием, использующих такие протоколы, как DNS over HTTPS (DoH) [RFC8484], DNS over TLS (DoT) [RFC7858], DNS over QUIC (DoQ) [RFC9250] в локальных сетях. Документ, в частности, указывает, как подключённые хосты могут обнаружить локальный распознаватель DNS с шифрованием средствами DHCPv4 [RFC2132], DHCPv6 [RFC8415] и IPv6 Router Advertisement (RA) [RFC4861]. Эти опции предназначены для передачи имени домена аутентификации (ADN), списка адресов IP и набора параметров сервиса. Процедура называется обнаружением назначенных сетью распознавателей (Discovery of Network-designated Resolvers или DNR).

Заданные в этом документе опции могут быть внедрены в разных системах, например, в локальных сетях с оборудованием в помещениях заказчика (Customer Premises Equipment или CPE), которое может (не обязательно) управляться поставщиком услуг Internet (Service Provider или ISP), или в локальных сетях с узлами пересылки DNS (forwarder) или без них. Предоставление вариантов внедрения выходит за рамки документа. Не рассматриваются здесь и вопросы выбора распознавателей, а также политика (включая взаимодействие с пользователями).

2. Терминология

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.

В этом документе применяются термины, определённые в [RFC8499], а также определённые ниже.

Authentication Domain Name (ADN) - имя домена аутентификации
: Имя домена, используемое клиентом DNS для проверки подлинности распознавателя DNS.

ADN-only mode - режим с извлечением только ADN
: Режим обнаружения DNS, при котором извлекается лишь ADN распознавателя DNS (см. параграф 3.1.6).

Do53
: DNS без шифрования.

DNR
: Процедура обнаружения назначенных сетью распознавателей (Discovery of Network-designated Resolvers).

Encrypted DNS - DNS с шифрованием
: Схема, где обмен DNS осуществляется по шифрованному каналу. Примерами служат DoT, DoH, DoQ.

Encrypted DNS resolver - распознаватель DNS с шифрованием
: Распознаватель DNS поддерживающий схему DNS с шифрованием.

Encrypted DNS options - опции DNS с шифрованием
: Опции, определённые в разделах 4, 5 и 6.

DHCP
: DHCPv4 и DHCPv6.

3. Обзор

Этот документ описывает, как клиент DNS может обнаружить локальные распознаватели DNS с шифрованием, используя опции DNS с шифрованием протоколов DHCP (разделы 4 и 5) и Neighbor Discovery (раздел 6). Эти опции задают ADN, список адресов IP и набор параметров сервиса распознавателя DNS с шифрованием. Дополнительные сведения об этих опциях приведены ниже.

3.1. Данные конфигурации для DNS с шифрованием

3.1.1. ADN как ссылочный идентификатор для аутентификации DNS

Для обеспечения возможности аутентификации распознавателя DNS клиенту на основе PKIX опции Encrypted DNS всегда включают ADN. Это имя представляется как ссылочный идентификатор для аутентификации DNS. Такое решение соответствует текущей практике выпуска сертификатов, как указано в параграфе 1.7.2 [RFC6125].

> Некоторые удостоверяющие центры выпускают сертификаты на основе адресов IP, но предварительные данные показывают что такие сертификаты составляют очень малую (менее 1%) часть выдаваемых сертификатов.

3.1.2. Независимость от внешних распознавателей

Чтобы избежать при распознавании ADN зависимости от другого сервера, опции Encrypted DNS возвращают адрес(а) IP для распознавателя DNS с шифрованием. Такие распознаватели DNS могут размещаться на одном или разных адресах IP в зависимости от конкретного внедрения. Для оптимизации размера сообщений обнаружения, когда все распознаватели DNS размещаются по одному адресу IP, в ранних версиях этого документа рассматривалось применение механизмов обнаружения из [RFC2132], [RFC3646], [RFC8106] для получения списка адресов IP, по которым доступны распознаватели DNS. Однако токай подход требует от клиента, поддерживающего более одного протокола DNS с шифрованием (например, DoH и DoT), запрашивать этот список адресов IP. Чтобы избежать такого зондирования, опции, заданные в разделах 4 - 6 связывают протокол DNS с шифрованием и адрес IP. В результате зондирования не требуется.

3.1.3. Один или несколько адресов IP

Список адресов IP для доступа к распознавателю DNS с шифрованием может возвращаться в опции Encrypted DNS, чтобы приспособиться к имеющимся системам, полагающимися на первичный и резервный распознаватель. Кроме того, DNR можно использовать в контексте иных схем резервирования DNS (например, anycast из BCP 126 [RFC4786]).

Возврат одного или нескольких адресов IP в опции Encrypted DNS зависит от конкретной системы. Например, маршрутизатор со встроенным рекурсивным сервером или элементом пересылки (forwarder) будет включать один адрес IP, указывающий один из его интерфейсов в ЛВС. Обычно это приватный адрес IPv4, адрес Link-Local, уникальный локальный адрес IPv6 (Unique Local Address или ULA) или глобальный индивидуальный адрес (Global Unicast Address или GUA).

Если в опции Encrypted DNS возвращается несколько адресов IP, они упорядочиваются по приоритету для клиента.

3.1.4. Одна опция для ADN и адресов IP

Для передачи ADN и адресов IP используется одна опция, поскольку иначе потребовалось бы сопоставление передаваемого в опции адреса IP с ADN из другой опции (например, при наличии в сети более одного ADN).

3.1.5. Параметры сервиса

Поскольку в сети могут применяться разные протоколы DNS с шифрованием (например, DoT, DoH, DoQ) и некоторые из этих протоколов могут использовать настраиваемый номер порта вместо принятого по умолчанию, опции Encrypted DNS спроектированы для возврата набора параметров сервиса. Эти параметры кодируются по тем же правилам, что и SvcParams с использованием формата передачи, заданного в параграфе 2.2 [RFC9460]. Такое кодирование может увеличить размер опций, но его достоинством является использование имеющегося реестра IANA, что позволит использовать новые протоколы DNS с шифрованием и параметры сервиса, которые могут быть заданы в будущем. Реализации DNR **должны** поддерживать перечисленные ниже параметры сервиса.

alpn
: Указывает набор поддерживаемых протоколов (параграф 7.1 в [RFC9460]).

port
: Служит для указания номера целевого порта в соединениях DNS с шифрованием (параграф 7.2 в [RFC9460]).

Кроме того, **рекомендуется** поддерживать ещё один параметр.

dohpath
: Служит для предоставления относительного шаблона DoH URI (раздел 5[1] в [RFC9461]).

3.1.6. Режим ADN-Only

Следует применять режим, где хосту предоставляется ADN, список адресов IP и набор параметров сервиса распознавателя DNS с шифрованием, поскольку опции Encrypted DNS являются самодостаточными и не требуют дополнительных запросов DNS. В [RFC7969] представлен обзор расширенных возможностей, поддерживаемых серверами DHCP для заполнения данных конфигурации (например, запросы DNS).

В условиях, когда для запрашивающих хостов допустимы дополнительные сложности, можно рассмотреть возврат лишь ADN. Представленное имя ADN будет предеваться локальной библиотеке распознавания (обычно клиенту DNS), которая будет вносить запросы привязки сервиса (Service Binding или SVCB) [RFC9461]. Эти запросы SVCB могут передаваться самому обнаруженному распознавателю DNS с шифрованием или назначенному сетью распознавателю Do53. Отметим, что этот режим подвержен активным атакам, которые можно смягчить с помощью DNSSEC.

Передача ADN в локальную библиотеку распознавания зависит от реализации.

3.1.7. Упорядочение опций Encrypted DNS

Опции DHCP, заданные в разделах 4 и 5 упорядочиваются в соответствии с разделом 17 в [RFC7227], для опции RA (раздел 6) применяются рекомендации раздела 9 в [RFC4861].

3.1.8. Проверка действительности DNR

При получении опции Encrypted DNS клиент DHCP (или хост IPv6) выполняет указанные ниже проверки.

- Наличие ADN с кодированием в соответствии с разделом 10 в [RFC8415].
- При наличии дополнительных данных:
  - проверяется кодирование параметров сервиса в соответствии с правилами параграфа 2.2 в [RFC9460];
  - проверяется наличие хотя бы одного действительного адреса IP;
  - проверяется отсутствие в параметрах сервиса ipv4hint и ipv6hint.

При отрицательном результате любой из проверок получатель отбрасывает принятую опцию Encrypted DNS.

[1] В оригинале ошибочно указан параграф 5.1, см. https://www.rfc-editor.org/errata/eid7784. *Прим. перев.*

3.1.9. Другие механизмы для получения сведений DNR

Указанные в этом документе механизмы предоставления могут быть недоступны в конкретных сетях (например, в некоторых сотовых сетях применяются лишь опции настройки протокола (Protocol Configuration Options или PCOs) [TS.24008]) или не подходить в некоторых условиях (например, если требуется защищённое обнаружение). В таких случаях могут рассматриваться другие механизмы предоставления распознавателей DNS с шифрованием. Запрашивающим хостам **рекомендуется** предоставлять по меньшей мере указанные ниже сведения DNR.

- Приоритет службы, если механизм обнаружения не полагается на неявное упорядочение при наличии нескольких экземпляров DNS с шифрованием.
- ADN (обязательный параметр).
- Список адресов IP для доступа к распознавателю DNS с шифрованием.
- Набор параметров сервиса.

3.2. Обработка конфликтов данных конфигурации

Если распознаватели DNS хост обнаруживает с помощью RA и DHCP, должны применяться правила параграфа 5.3.1 из [RFC8106].

Опции DHCP/RA для нахождения распознавателей DNS с шифрованием (включая шаблоны DoH URI) имеют преимущество перед DDR [RFC9462], так как в DDR применяется Do53 с внешним распознавателем DNS, подверженный внутренним и внешним атакам, а DHCP/RA обычно защищены (см. параграф 7.1).

Если клиент узнает Do53 и распознаватели DNS с шифрованием из одной сети и нет явной настройки, **рекомендуется** использовать для этой сети распознаватель DNS с шифрованием. Если клиент не может организовать защищённое и аутентифицированное соединение с распознавателем DNS с шифрованием, можно применять распознаватель Do53.

3.3. Проверка обнаруженных распознавателей

В этом параграфе описаны проверки для подтверждения соответствия распознавателя DNS с шифрованием полученному с помощью DNR (например, DHCP или RA). Эти проверки не предназначены для подтверждения безопасности механизмов предоставления DNR или доверительных отношений пользователя с сетью.

Если локальный клиент DNS поддерживает один из обнаруженных протоколв DNS с шифрованием, указанных идентификаторами протокола согласования прикладного уровня (Application-Layer Protocol Negotiation или ALPN) или иным параметром сервиса, указывающим механизм рассогласования протокола, клиент DNS организует шифрованную сессию DNS в соответствии с приоритетом обнаруженных распознавателей с шифрованием.

Клиент DNS проверяет соединение с помощью PKIX [RFC5280] из сертификата распознавателя DNS и применяет методы проверки [RFC6125] для сравнения ADN из опций Encrypted DNS с представленным сертификатом (параграф 8.1 в [RFC8310]). Клиент DNS использует привязки доверия системы или приложения PKI, если не заданы явные привязки доверия. Связанные с ALPN вопросы рассмотрены в параграфе 7.1 [RFC9460]. Вопросы, связанные с проверкой статуса отзыва сертификата распознавателя DNS с шифрованием, рассмотрены в разделе 10 [RFC8484].

3.4. Многодомные устройства

Устройства могут подключаться к нескольким сетям, каждая из которых обеспечивает свою конфигурацию DNS с помощью описанных здесь механизмов. Тем не менее, выбор DNS на многодомных устрйоствах выходит за рамки документа. Такие вопросы относятся к общим задачам обработки нескольких источников обеспечения и их не следует рассматривать отдельно, как это рекомендовано в разделе 12 [RFC7227].

В [RFC6731] рассматривается выбор DNS и приведён пример выбора распознавателя DNS на устройстве с несколькими интерфейсами. В [Local-DNS-Authority] рассмотрено применение DNR и ключа домена обеспечения (Provisioning Domain или PvD) dnsZones (параграф 4.3 в [RFC8801]) в средах с «расщеплением DNS» (раздел 6 в [RFC8499]).

4. Опция DHCPv6 в DNS с шифрованием

4.1. Формат опции

Формат опции DHCPv6 для DNS с шифрованием показан на рисунке 1.

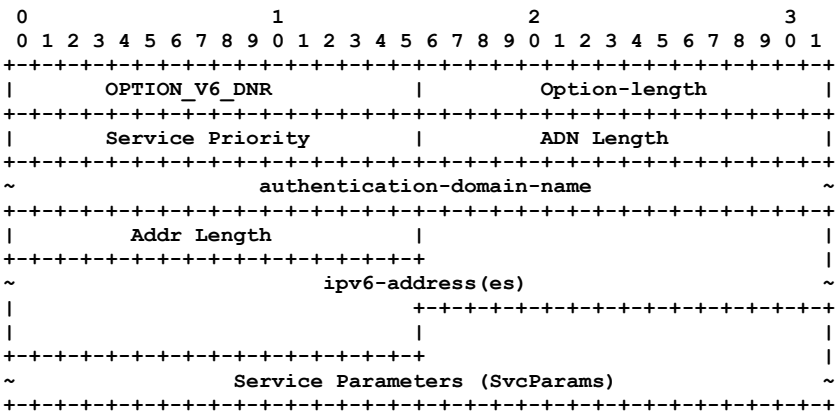

Рисунок 1. Опция DHCPv6 Encrypted DNS

Option-code

OPTION_V6_DNR (144, см. параграф 9.1).

Option-length

Размер вложенных данных в октетах. При включении лишь ADN поле имеет значение (ADN Length + 4).

Service Priority

Приоритет этого экземпляра OPTION_V6_DNR по отношению к другим. Это 16-битовое целое число без знака, интерпретируемое по правилам параграфа 2.4.1 в [RFC9460].

ADN Length

Размер поля authentication-domain-name в октетах.

authentication-domain-name (переменный размер)

Полное доменное имя (Fully Qualified Domain Name или FQDN) распознавателя DNS с шифрованием. Формат поля соответствует разделу 10 в [RFC8415]. Пример кодирования authentication-domain-name показан на рисунке 2 с использованием FQDN doh1.example.com. и соответствующим этому значением ADN Length = 18.

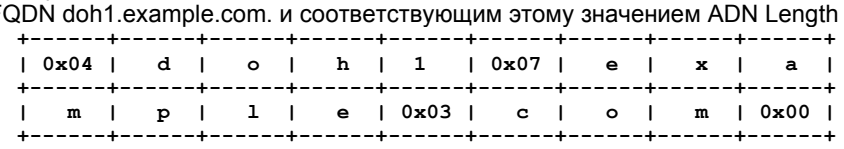

Рисунок 2. Пример кодирования authentication-domain-name.

Addr Length

Размер вложенных адресов IPv6 в октетах. При наличии поля, значение **должно** быть кратно 16.

ipv6-address(es) (переменный размер)

Один или несколько адресов IPv6 для доступа к распознавателю DNS с шифрованием. Адресом может быть Link-Local, ULA или GUA. Формат поля показан на рисунке 3.

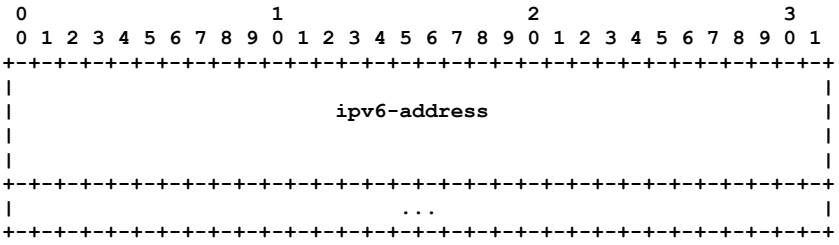

Рисунок 3. Поле ipv6-address.

Service Parameters (SvcParams) (переменный размер)

Набор параметров сервиса, закодированных по правилам параграфа 2.2 в [RFC9460]. Параметры могут включать, например, список идентификаторов протоколов ALPN или номера портов. В это поле **следует** включать хотя бы alpn SvcParam. Параметр alpn может не требоваться в ситуациях, вроде варианта DNS через проткол приложений с ограничениями (Constrained Application Protocol или CoAP), где сообщения шифруются с использованием OSCORE[1] [RFC8613]. В параметры сервиса **недопустимо** включать ipv4hint или ipv6hint, поскольку они переопределяются включёнными адресами IP.

Если порт не указан, следует использовать принятый по умолчанию порт (853 для DoT и DoQ, 443 для DoH).

Размер этого поля составляет (Option-length - 6 - ADN Length - Addr Length).

Поля Addr Length, ipv6-address(es) и Service Parameters (SvcParams) отсутствуют в режиме ADN-only (параграф 3.1.6).

4.2. Поведение клиента DHCPv6

Для обнаружения распознавателя DNS с шифрованием клиент DHCPv6 **должен** включить опцию OPTION_V6_DNR в опцию запроса опций (Option Request Option или ORO) в соответствии с параграфами 18.2.1, 18.2.2, 18.2.4, 18.2.5, 18.2.6, 21.7 в [RFC8415]. Клиент DHCPv6 **должен** быть готов получить несколько экземпляров опции OPTION_V6_DNR, каждый из которых считается представляющим отдельный распознаватель DNS с шифрованием. Эти экземпляры **должны** обрабатываться в соответствии с приоритетом сервиса (меньшее значение указывает больший приоритет).

Клиент DHCPv6 **должен** без уведомления отбрасывать любые опции OPTION_V6_DNR, не прошедшие проверку в соответствии с параграфом 3.1.8. Клиент DHCPv6 **должен** без уведомления отбрасывать групповые адреса и петлевые (loopback) адреса хоста, полученные в опции OPTION_V6_DNR.

5. Опция DHCPv4 в DNS с шифрованием

5.1. Формат опции

Формат опции DHCPv4 для DNS с шифрованием показан на рисунке 4.

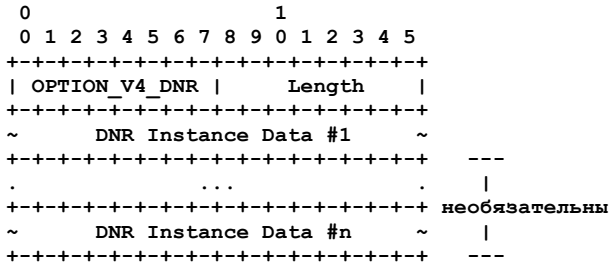

Рисунок 4. Опция DHCPv4 Encrypted DNS.

Code

OPTION_V4_DNR (162, см. параграф 9.2).

Length

Размер вложенных данных в октетах.

[1]Object Security for Constrained RESTful Environments - защита объекта для сред RESTful с ограничениями.

DNR Instance Data

Данные конфигурации распознавателя DNS с шифрованием. Формат поля показан на рисунке 5.

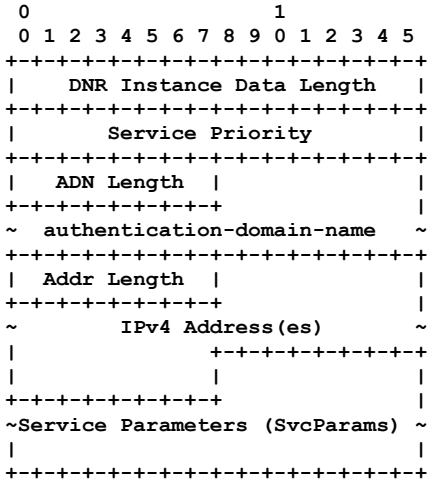

Рисунок 5. Формат экземпляра данных DNR.

При включении нескольких распознавателей DNS с шифрованием поле DNR Instance Data повторяется.

DNR Instance Data Length

Размер последующих данных в октетах. При передаче лишь ADN для экземпляра DNR это будет (ADN Length + 3).

Service Priority

Приоритет этого экземпляра DNR по отношению к другим (16-битовое целое число без знака, интерпретируемое в соответствии с параграфом 2.4.1 в [RFC9460]).

ADN Length

Размер поля authentication-domain-name в октетах.

authentication-domain-name (переменный размер)

ADN распознавателя DNS с шифрованием. Поле форматируется в соответствии с разделом 10 в [RFC8415], пример представлен на рисунке 2.

Addr Length

Размер включённых адресов IPv4 в октетах. При наличии поля его значение **должно** быть кратно 4.

IPv4 Address(es) (переменный размер)

Один или несколько адресов IPv4 для доступа к распознавателю DNS с шифрованием. Могут указываться как публичные, так и приватные адреса IPv4. Формат поля показан на рисунке 6 и предполагает кодирование адресов в форме a1.a2.a3.a4.

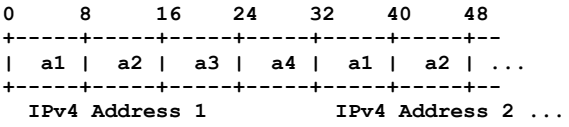

Рисунок 6. Формат поля IPv4 Address.

Service Parameters (SvcParams) (переменный размер)

Набор параметров сервиса, закодированных по правилам параграфа 2.2 в [RFC9460]. Параметры могут включать, например, список идентификаторов протоколов ALPN или номера портов. В это поле **следует** включать хотя бы alpn SvcParam. Параметр alpn может не требоваться в ситуациях, вроде варианта DNS через проткол приложений с ограничениями (Constrained Application Protocol или CoAP), где сообщения шифруются с использованием OSCORE [RFC8613]. В параметры сервиса **недопустимо** включать ipv4hint или ipv6hint, поскольку они переопределяются включёнными адресами IP.

Если порт не указан, следует использовать принятый по умолчанию порт.

Размер этого поля составляет (DNR Instance Data Length - 4 - ADN Length - Addr Length).

Поля Addr Length, IPv4 Address(es), Service Parameters (SvcParams) отсутствуют в режиме ADN-only (параграф 3.1.6).

Опция OPTION_V4_DNR требует конкатенации, поэтому **должен** применяться механизм [RFC3396], если OPTION_V4_DNR превышает максимальный размер опции DHCPv4 (255 октетов).

5.2. Поведение клиента DHCPv4

Для обнаружения распознавателя DNS с шифрованием клиент DHCPv4 запрашивает его включением опции OPTION_V4_DNR в опцию Parameter Request List [RFC2132]. Клиент DHCPv4 **должен** быть готов получить в опции OPTION_V4_DNR несколько записей DNR Instance Data, каждая из которых считается представляющей отдельный экземпляр распознавателя DNS с шифрованием. Эти записи **должны** обрабатываться в соответствии с приоритетом сервиса (меньшее значение указывает больший приоритет).

Клиент DHCPv4 **должен** без уведомления отбрасывать любые опции OPTION_V4_DNR, не прошедшие проверку в соответствии с параграфом 3.1.8. Клиент DHCPv4 **должен** без уведомления отбрасывать групповые адреса и петлевые (loopback) адреса хоста, полученные в опции OPTION_V4_DNR.

6. Опция IPv6 RA в DNS с шифрованием

6.1. Формат опции

В этом разделе определена новая опция обнаружения соседей (Neighbor Discovery) [RFC4861] - IPv6 RA Encrypted DNS. Опция полезна в условиях, похожих на рассмотренные в параграфе 1.1 [RFC8106].

Формат опции IPv6 RA Encrypted DNS показан на рисунке 7.

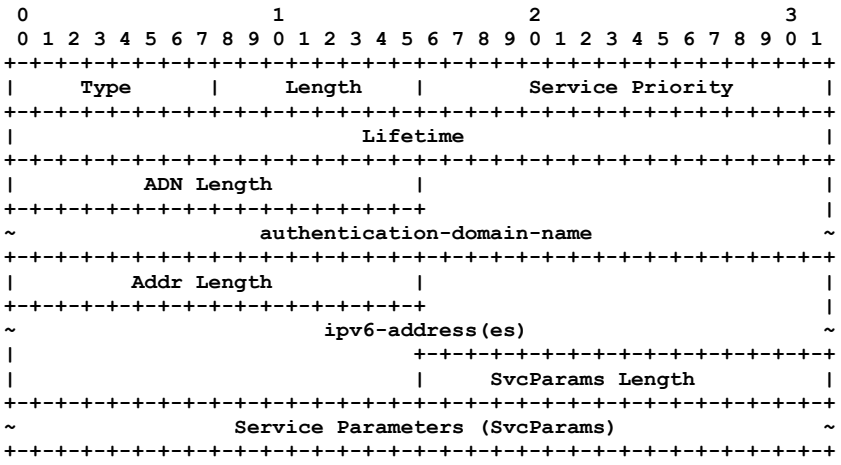

Рисунок 7. Опция RA.

Type
8-битовые идентификатор опции Encrypted DNS, выделенный IANA (144, см. параграф 9.3).

Length
8-битовое целое число, указывающее количество 8-октетных блоков в опции (включая поля Type и Length).

Service Priority
16-битовое целое число без знака. Приоритет данной опции Encrypted DNS сравнивается с другими экземплярами по правилам параграфа 2.4.1 в [RFC9460].

Lifetime
32-битовое целое число без знака, указывающее максимальное число секунд (с момента получения пакета), в течение которого обнаруженное имя ADN действительно. По умолчанию в поле Lifetime следует использовать значение не меньше 3 * MaxRtrAdvInterval, где MaxRtrAdvInterval - максимальный интервал RA в соответствии с [RFC4861]. Значение, содержащее только 1 (0xffffffff) указывает неограниченный срок действия, 0 указывает, что ADN **недопустимо** использовать в дальнейшем.

ADN Length
16-битовое целое число без знака, указывающее размер поля authentication-domain-name в октетах.

authentication-domain-name (переменный размер)
Имя ADN для распознавателя DNS с шифрованием в формате, заданном разделом 10 в [RFC8415].

Addr Length
16-битовое целое число без знака, указывающее размер вложенных адресов IPv6 в октатх. При наличии поля значение должно быть кратным 16.

ipv6-address(es) (переменный размер)
Один или несколько адресов IPv6 (Link-Local, ULA, GUA) распознавателя DNS с шифрованием. Все адреса используют общее поле Lifetime. Если желательно использовать разные сроки действия адресов (см. [RFC8106]) можно использовать несколько опций Encrypted DNS. Формат поля показан на рисунке 3.

SvcParams Length
16-битовое целое число без знака, указывающее размер поля Service Parameters (SvcParams) в октетах.

Service Parameters (SvcParams) (переменный размер)
Набор параметров сервиса, закодированных по правилам параграфа 2.2 в [RFC9460]. Параметры могут включать, например, список идентификаторов протоколов ALPN или номера портов. В это поле **следует** включать хотя бы alpn SvcParam. Параметр alpn может не требоваться в ситуациях, вроде варианта DNS через проткол приложений с ограничениями (Constrained Application Protocol или CoAP), где сообщения шифруются с использованием OSCORE. В параметры сервиса **недопустимо** включать ipv4hint или ipv6hint, поскольку они переопределяются включёнными адресами IP.

Если порт не указан, следует использовать принятый по умолчанию порт.

Поля Addr Length, ipv6-address(es), SvcParams Length[1] и Service Parameters (SvcParams) отсутствуют в режиме ADN-only (параграф 3.1.6).

Опция должна дополняться нулями до размера, кратного 8 октетам (параграф 4.6 в [RFC4861]).

6.2. Поведение хоста IPv6

Процедура настройки DNS такая же, как для других опций Neighbor Discovery [RFC4861]. Кроме того, хост следует процедуре из параграфа 5.3.1 в [RFC8106] при обработке опций Encrypted DNS с требованиями к форматированию из параграфа 6.1 проверками пригодности из параграфа 3.1.8, заменёнными проверкой размера и значений полей.

Хост должен быть готов получить несколько экземпляров опций Encrypted DNS в RA. Эти экземпляры **должны** обрабатываться в соответствии с приоритетом сервиса (меньшее значение указывает больший приоритет).

Хост **должен** без уведомления отбрасывать групповые адреса и петлевые (loopback) адреса хоста, полученные в опциях Encrypted DNS.

7. Вопросы безопасности

7.1. Атаки с подменой

Сообщения DHCP/RA не шифруются и не защищены от изменения внутри ЛВС. Если атаки с подменой не смягчены, как указано ниже, содержимое сообщений DHCP и RA может быть подделано или изменено активными атакующими, например, скомпрометированными устройствами в локальной сети. Активный атакующий (параграф 3.3 в [RFC3552]) может подделать отклик DHCP/RA предоставляя свой распознаватель DNS с шифрованием. Он может организовать и

[1] В оригинале это поле ошибочно не указано, см. https://www.rfc-editor.org/errata/eid7804. *Прим. перев.*

другие атаки, как отмечено в разделе 22 [RFC8415]. Злоумышленник может получить доменное имя с подтверждённым доменом путличным сертификатом от удостоверяющего центра (Certificate Authority или CA) и разместить там распознаватель DNS с шифрованием.

Для смягчения атак с поддельными или изменёнными откликами DHCP и сообщениями RA внутри локальной сети можно использовать указанные ниже механизмы.

Экран DHCPv6 [RFC7610]
: Узел доступа в сеть (например, граничный маршрутизатор, CPE, точка доступа (Access Point или AP)) отбрасывает сообщения с откликами DHCP, полученные от любой локальной конечной точки.

RA-Guard [RFC7113]
: Узел доступа в сеть отбрасывает сообщения RA, полученные от любой локальной конечной точки.

Улучшение проверки адреса источника (Source Address Validation Improvement или SAVI) для DHCP [RFC7513]
: Узел доступа в сеть отфильтровывает пакеты с поддельными IP-адресами отправителя.

Эти механизмы обеспечивают получение конечной точкой корркткных данных конфигурации распознавателей DNS, выбранных сервером DHCP (или отправителем RA), но не могут предоставить каких-либо сведений о сервере DHCP или объекте, на котором этот сервер DHCP (или отправитель RA) размещен.

Шифрованные сессии DNS с мошенническими распознавателями, подделывающими IP-адрес распознавателя DNS, будут сталкиваться с отказами, поскольку клиент DNS получит отказ при проверке подлинности мошеннического распознавателя на основе аутентификации PKIX [RFC6125], в частности для ADN в опции Encrypted DNS. Клиенты DNS, игнорирующие отказ при аутентификации и воспринимающие поддельные сертификаты, будут подвержены атакам (например, перенаправление на поддельные распознаватели или перехват конфиденциальных данных).

7.2. Атаки с удалением

Если атакующий отбрасывает отклики DHCP или RA, клиент может вернуться к использованию ранее заданного распознавателя DNS с шифрованием. Однако правила выбора распознавателей выходят за рамки этого документа.

Отметим, что атаки с удалением не являются спецификой DHCP/RA.

7.3. Пассивные атаки

Пассивный атакующий (параграф 3.2 в [RFC3552]) может определить использование хостом DHCP/RA для обнаружения распознавателя DNS с шифрованием и сделать вывод о способности хоста использовать DoH/DoT/DoQ для шифрования сообщений DNS. Однако он не сможет поддедать или изменить сообщения DHCP/RA.

7.4. Атаки с аутентификацией в беспроводных сетях

Беспроводные ЛВС (Wireless LAN или WLAN), часто используемые в локальных сетях (например, в домашних), уязвимы для различных атак (например, [Evil-Twin], [Krack], [Dragonblood]). По этой причине в беспроводных ЛВС доверяют лишь криптографически аутентифицированным коммуникациям. Это означает, что любые сведения (например, о серверах NTP, распознавателях DNS, списках доменоа для поиска), предоставляемые такими сетями через DHCP, DHCPv6, RA, являются недоверенными, поскольку подлинность сообщений DHCP и RA не проверяется.

Если заранее распределенные ключи (pre-shared key или PSK) совпадают у всех клиентов, подключённых к одной WLAN (например, Wi-Fi Protected Access Pre-Shared Key (WPA-PSK)), ключ будет доступен и злоумышленникам, что позволяет организовать активную атаку на пути. Такие атаки возможны внутри локальной сети, поскольку в этой форме аутентификации WLAN не проверяется подлинность партнёров. Это ведёт к необходимости предоставлять клиентам уникальные свидетельства (credentials). Конечным точка могут предоставляться уникальные свидетелства (обычно, имя пользователя и пароль), заданные администратором локальной сети, для взаимной аутентификации на локальной WLAN AP, например, 802.1x Wireless User Authentication в OpenWrt [dot1x], EAP[1]-pwd [RFC8146]. Не все конечные устройства (например, IoT[2]) поддерживают просителей 802.1x (supplicant) и им нужен другой механизм для подключения к локальной сети. Для снятия этого ограничения можно создать уникальный PSK для каждого такого устройства и использовать WPA-PSK (например, [IPSK]).

8. Вопросы приватности

Вопросы приватности, актуальные и для механизмов предоставления DNR, рассмотрены в разделе 23 [RFC8415] и в in [RFC7824]. Профили анонимности для клиентов DHCP рассмотрены в [RFC7844]. Определённые в этом документе механизмы можно применять для определения поддержки клиентом DHCP или хостом IPv6 опций Encrypted DNS, но эти механизмы не раскрывают возможности локальных клиентов DNS воспринимать эти опции и использовать шифрование. В остальном эти механизмы не раскрывают дополнительных приватных сведений по сравнению с опциями обнаружения Do53.

Как отмечено в [RFC9076], использование DNS с шифрованием не снижает уровень доступности данных в распознавателе DNS. Конкретные соображения по защите приватности для DNS с шифрованием приведены в разделе 8 [RFC8484] и разделе 7 [RFC9250].

9. Взаимодействие с IANA

9.1. Опция DHCPv6

Агентство IANA включило указанный в таблице 1 код опции DHCPv6 в реестр Option Codes [DHCPV6].

Таблица 1. Опция DHCPv6.

Значение	***Описание***	***Client ORO***	***Одиночная опция***	***Документ***
144	OPTION_V6_DNR	Yes	No	RFC 9463

[1]Extensible Authentication Protocol - расширяемый протокол аутентификации.
[2]Internet of Things - Internet вещейю

9.2. Опция DHCPv4

Агентсво IANA включило указанный в таблице 2 код опции DHCP в реестр BOOTP Vendor Extensions and DHCP Options [BOOTP].

Таблица 2. Опция DHCPv4.

Тег	Имя	Размер данных	Значение	Документ
162	OPTION_V4_DNR	N	Encrypted DNS Server	RFC 9463

9.3. Опция Neighbor Discovery

Агентство IANA включило указанный в таблице 3 тип опции IPv6 Neighbor Discovery Option в субреестр IPv6 Neighbor Discovery Option Formats реестра Internet Control Message Protocol version 6 (ICMPv6) Parameters [ND].

Таблица 3. Опция Neighbor Discovery.

Тип	Описание	Документ
144	Encrypted DNS Option	RFC 9463

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>.

[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>.

[RFC3396] Lemon, T. and S. Cheshire, "Encoding Long Options in the Dynamic Host Configuration Protocol (DHCPv4)", RFC 3396, DOI 10.17487/RFC3396, November 2002, <https://www.rfc-editor.org/info/rfc3396>.

[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>.

[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>.

[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>.

[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>.

[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>.

10.2. Дополнительная литература

[BOOTP] IANA, "BOOTP Vendor Extensions and DHCP Options", <https://www.iana.org/assignments/bootp-dhcp-parameters/>.

[DHCPV6] IANA, "Option Codes", <https://www.iana.org/assignments/dhcpv6-parameters/>.

[DNS-TLS-DHCPv6-Opt] Pusateri, T. and W. Toorop, "DHCPv6 Options for private DNS Discovery", Work in Progress, Internet-Draft, draft-pusateri-dhc-dns-driu-00, 2 July 2018, <https://datatracker.ietf.org/doc/html/draft-pusateri-dhc-dns-driu-00>.

[dot1x] OpenWrt, "Introduction to 802.1X", December 2021, <https://openwrt.org/docs/guide-user/network/wifi/wireless.security.8021x>.

[Dragonblood] Vanhoef, M. and E. Ronen, "Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd", 2020 IEEE Symposium on Security and Privacy (SP), San Francisco, pp. 517-533, DOI 10.1109/SP40000.2020.00031, May 2020, <https://ieeexplore.ieee.org/document/9152782>.

[Evil-Twin] Wikipedia, "Evil twin (wireless networks)", November 2022, <https://en.wikipedia.org/wiki/Evil_twin_(wireless_networks)>.

[IPSK] Cisco, "8.5 Identity PSK Feature Deployment Guide", December 2021, <https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-5/b_Identity_PSK_Feature_Deployment_Guide.html>.

[Krack] Vanhoef, M. and F. Piessens, "Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2", CCS '17: Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, pp. 1313-1328, DOI 10.1145/3133956.3134027, October 2017, <https://dl.acm.org/doi/10.1145/3133956.3134027>.

[Local-DNS-Authority] Reddy, T., Wing, D., Smith, K., and B. Schwartz, "Establishing Local DNS Authority in Validated Split-Horizon Environments", Work in Progress, Internet-Draft, draft-ietf-add-split-horizon-authority-04, 8 March 2023, <https://datatracker.ietf.org/doc/html/draft-ietf-add-split-horizon-authority-04>.

[ND] IANA, "IPv6 Neighbor Discovery Option Formats", <https://www.iana.org/assignments/icmpv6-parameters/>.

[RFC3552] Rescorla, E. and B. Korver, "Guidelines for Writing RFC Text on Security Considerations", BCP 72, RFC 3552, DOI 10.17487/RFC3552, July 2003, <https://www.rfc-editor.org/info/rfc3552>.

[RFC3646] Droms, R., Ed., "DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3646, DOI 10.17487/RFC3646, December 2003, <https://www.rfc-editor.org/info/rfc3646>.

[RFC4786] Abley, J. and K. Lindqvist, "Operation of Anycast Services", BCP 126, RFC 4786, DOI 10.17487/RFC4786, December 2006, <https://www.rfc-editor.org/info/rfc4786>.

[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>.

[RFC6125] Saint-Andre, P. and J. Hodges, "Representation and Verification of Domain-Based Application Service Identity within Internet Public Key Infrastructure Using X.509 (PKIX) Certificates in the Context of Transport Layer Security (TLS)", RFC 6125, DOI 10.17487/RFC6125, March 2011, <https://www.rfc-editor.org/info/rfc6125>.

[RFC6731] Savolainen, T., Kato, J., and T. Lemon, "Improved Recursive DNS Server Selection for Multi-Interfaced Nodes", RFC 6731, DOI 10.17487/RFC6731, December 2012, <https://www.rfc-editor.org/info/rfc6731>.

[RFC7113] Gont, F., "Implementation Advice for IPv6 Router Advertisement Guard (RA-Guard)", RFC 7113, DOI 10.17487/RFC7113, February 2014, <https://www.rfc-editor.org/info/rfc7113>.

[RFC7227] Hankins, D., Mrugalski, T., Siodelski, M., Jiang, S., and S. Krishnan, "Guidelines for Creating New DHCPv6 Options", BCP 187, RFC 7227, DOI 10.17487/RFC7227, May 2014, <https://www.rfc-editor.org/info/rfc7227>.

[RFC7513] Bi, J., Wu, J., Yao, G., and F. Baker, "Source Address Validation Improvement (SAVI) Solution for DHCP", RFC 7513, DOI 10.17487/RFC7513, May 2015, <https://www.rfc-editor.org/info/rfc7513>.

[RFC7610] Gont, F., Liu, W., and G. Van de Velde, "DHCPv6-Shield: Protecting against Rogue DHCPv6 Servers", BCP 199, RFC 7610, DOI 10.17487/RFC7610, August 2015, <https://www.rfc-editor.org/info/rfc7610>.

[RFC7824] Krishnan, S., Mrugalski, T., and S. Jiang, "Privacy Considerations for DHCPv6", RFC 7824, DOI 10.17487/RFC7824, May 2016, <https://www.rfc-editor.org/info/rfc7824>.

[RFC7844] Huitema, C., Mrugalski, T., and S. Krishnan, "Anonymity Profiles for DHCP Clients", RFC 7844, DOI 10.17487/RFC7844, May 2016, <https://www.rfc-editor.org/info/rfc7844>.

[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>.

[RFC7969] Lemon, T. and T. Mrugalski, "Customizing DHCP Configuration on the Basis of Network Topology", RFC 7969, DOI 10.17487/RFC7969, October 2016, <https://www.rfc-editor.org/info/rfc7969>.

[RFC8146] Harkins, D., "Adding Support for Salted Password Databases to EAP-pwd", RFC 8146, DOI 10.17487/RFC8146, April 2017, <https://www.rfc-editor.org/info/rfc8146>.

[RFC8310] Dickinson, S., Gillmor, D., and T. Reddy, "Usage Profiles for DNS over TLS and DNS over DTLS", RFC 8310, DOI 10.17487/RFC8310, March 2018, <https://www.rfc-editor.org/info/rfc8310>.

[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>.

[RFC8499] Hoffman, P., Sullivan, A., and K. Fujiwara, "DNS Terminology", BCP 219, RFC 8499, DOI 10.17487/RFC8499, January 2019, <https://www.rfc-editor.org/info/rfc8499>.

[RFC8613] Selander, G., Mattsson, J., Palombini, F., and L. Seitz, "Object Security for Constrained RESTful Environments (OSCORE)", RFC 8613, DOI 10.17487/RFC8613, July 2019, <https://www.rfc-editor.org/info/rfc8613>.

[RFC8801] Pfister, P., Vyncke, É., Pauly, T., Schinazi, D., and W. Shao, "Discovering Provisioning Domain Names and Data", RFC 8801, DOI 10.17487/RFC8801, July 2020, <https://www.rfc-editor.org/info/rfc8801>.

[RFC9076] Wicinski, T., Ed., "DNS Privacy Considerations", RFC 9076, DOI 10.17487/RFC9076, July 2021, <https://www.rfc-editor.org/info/rfc9076>.

[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>.

[RFC9462] Pauly, T., Kinnear, E., Wood, C. A., McManus, P., and T. Jensen, "Discovery of Designated Resolvers", RFC 9462, DOI 10.17487/RFC9462, November 2023, <https://www.rfc-editor.org/info/rfc9462>.

[TS.24008] 3GPP, "Technical Specification Group Core Network and Terminals; Mobile radio interface Layer 3 specification; Core network protocols; Stage 3 (Release 18)", version 18.4.0, September 2023, <https://www.3gpp.org/DynaReport/24008.htm>.

Благодарности

Большое спасибо Christian Jacquenet и Michael Richardson за их рецензии.

Спасибо Stephen Farrell, Martin Thomson, Vittorio Bertola, Stéphane Bortzmeyer, Ben Schwartz, Iain Sharp, Chris Box за их комментарии.

Спасибо Mark Nottingham за отклик по перенаправлению HTTP, обсуждаемому в черновых вариантах спецификации.

Использование протокола DHCP в качестве кандидата для извлечения ADN было упомянуто в параграфе 7.3.1 [RFC8310] и Internet-Draft, авторами которого являются Tom Pusateri и Willem Toorop [DNS-TLS-DHCPv6-Opt].

Спасибо Bernie Volz за рецензию по DHCP.

Christian Amsüss указал случай, когда параметр сервиса ALPN не может использоваться.

Спасибо Andrew Campling за рецензию Shepherd и Éric Vyncke за рецензию AD.

Спасибо Rich Salz за рецензии secdir, Joe Clarke за рецензию opsdir, Robert Sparks за рецензию artart, David Blacka за рецензию dnsdir.

Спасибо Lars Eggert, Roman Danyliw, Erik Kline, Martin Duke, Robert Wilton, Paul Wouters, Zaheduzzaman Sarker за рецензию IESG.

Участники работы

Nicolai Leymann
Deutsche Telekom
Germany
Email: n.leymann@telekom.de

Zhiwei Yan
CNNIC
No.4 South 4th Street, Zhongguancun
Beijing
100190
China
Email: yan@cnnic.cn

Адреса авторов

Mohamed Boucadair (editor)
Orange
35000 Rennes
France
Email: mohamed.boucadair@orange.com

Tirumaleswar Reddy.K (editor)
Nokia
India
Email: kondtir@gmail.com

Dan Wing
Cloud Software Group Holdings, Inc.
United States of America
Email: dwing-ietf@fuggles.com

Neil Cook
Open-Xchange
United Kingdom
Email: neil.cook@noware.co.uk

Tommy Jensen
Microsoft
United States of America
Email: tojens@microsoft.com

Перевод на русский язык

Николай Малых

nmalykh@protokols.ru