Internet Engineering Task Force (IETF)
Request for Comments: 9499
BCP: 219
Obsoletes: 8499
Updates: 2308
Category: Best Current Practice
ISSN: 2070-1721

P. Hoffman
ICANN
K. Fujiwara
JPRS

March 2024

DNS Terminology

Терминология DNS

Аннотация

Система доменных имён (Domain Name System или DNS) определена в десятках разных RFC. Терминология, используемая при разработке и внедрении протоколов DNS, а также в работе операторов систем DNS, изменилась за десятилетия, прошедшие с момента исходного определения DNS. В этом документе приведены современные определения для многих терминов, применяемых в DNS.

Документ обновляет RFC 2308, уточняя определения терминов forwarder и QNAME. Документ отменяет RFC 8499, добавляя множество определений и уточнений. Полные списки изменённых и новых определений даны в Приложениях A и B.

Статус документа

Документ относится к категории Internet Best Current Practice.

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 документах BCP 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/rfc9499.

Оглавление

1. Введение

DNS - простой протокол «запрос-отклик», где сообщения имеют общий формат для обоих направлений (в разделе 2 дано определение термина global DNS, который для многих зачастую означает то же, что и DNS). Протокол и формат

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

сообщений заданы в [RFC1034] и [RFC1035], где определены некоторые термины. В последующих RFC определены другие термины. Некоторые из терминов, заданных в [RFC1034] и [RFC1035], сейчас имеют иное значение, нежели в 1987 г.

Этот документ включает широкий набор связанных с DNS терминов, сгруппированных по темам. Некоторые термины точно определены в предшествующих RFC, другие были ранее определены достаточно вольно, а третьи - совсем не определены в прежних RFC.

Связанные с DNS термины иногда определяют другие организации, например, рабочая группа WHATWG определила термин domain (см. https://url.spec.whatwg.org/). Консультативный комитет системы корневых серверов (Root Server System Advisory Committee или RSSAC) имеет хороший глоссарий [RSSAC026].

Большинство приведённых здесь определений представляют согласованный подход сообщества DNS - разработчиков протокола и операторов. Некоторые определения отличаются от прежних RFC и такие различия отмечены. При совпадении приведённых здесь определений с определениями прежних RFC приводится цитата из такого RFC. Если определение так или иначе изменено, прежний RFC указывается, но даётся новое определение. Список обновлённых определений представлен в Приложении A.

Важно отметить, что в процессе подготовки этого документа стало ясно, что некоторые термины, связанные с DNS, по-разному интерпретируются DNS-экспертами. Кроме того, некоторые термины из прежних DNS RFC имеют определения, которые в целом согласованы, но отличаются от исходных. Этот документ является незначительной переработкой [RFC8499], который был существенной переработкой [RFC7719].

Отметим, что нет согласованного определения DNS. Можно рассматривать DNS как некую комбинацию общепринятой схемы именования объектов в Internet, распределенной базы данных, представляющей имена и некоторые свойства этих объектов, архитектуры, обеспечивающей распределенное обслуживание, устойчивость и нестрогую когерентность распределенной базы данных и простого протокола «запрос-отклик» (как отмечено ниже), реализующего эту архитектуру. В разделе 2 даны определения терминов global DNS и private DNS, чтобы разобраться с этими разными определениями.

Использование заглавных букв в терминах DNS часто не согласуется в разных RFC и практике применения DNS. В этом документе заглавные буквы применяются в соответствии с наиболее распространённой практикой и не указывается, что иное использование заглавных букв является ошибочным или устаревшим. В некоторых случаях применяется несколько стилей использования заглавных букв для одного термина из-за цитирования разных RFC.

Термины byte (байт) и octet (октет) в этом документе взаимозаменяемы. Использование обоих терминов обусловлено их применением в прежних RFC, определяющих термины DNS.

Читателям следует обратить внимание на группировку терминов по темам. Не знакомые близко с DNS, вероятно, не смогут полностью разобраться с DNS на основании этого документа. Для получения достаточного для понимания отдельных терминов контекста единственным способом может оказаться временный пропуск некоторых определений. В документ включён предметный указатель, который может быть полезен для читателей, пытающихся изучать DNS по этому документу.

2. Имена

Naming system - система именования

Система именования связывает имена с данными. Системы именования имеют множество важных аспектов, позволяющих отличать одну систему от другой, наиболее заметные из них включают:

- состав имён;
- формат имён;
- администрирование имён;
- типы данных, которые могут быть связаны с именами;
- типы метаданных для имён;
- протокол для получения данных по имени;
- контекст для распознавания имени.

Отметим, что этот список представляет небольшое подмножество аспектов, которые были определены людьми для систем именования, и IETF ещё предстоит согласовать набор аспектов, которые хорошо подойдут для сравнения систем именования. Например, такие аспекты могут включать протокол для обновления данных по имени, приватность имён, приватность связанных с именами данных, но эти аспекты не определены так же хорошо, как перечисленные выше. Приведённый список выбран потому, что он помогает описать DNS и похожие на DNS системы именования.

Domain name - доменное имя

Упорядоченный список из одной или нескольких меток.

Отметим, что это определение независимо от DNS RFC ([RFC1034] и [RFC1035]) и применимо к отличным от DNS системам. В [RFC1034] определено пространство доменных имён (domain name space) с использованием математических деревьев и их узлов в теории графов и это определение имеет такой же практический результат, что и приведённое здесь. Любой путь в направленном ациклическом графе можно представить доменным именем, состоящим из меток узлов графа, упорядоченных по удалённости от корня (это соглашение DNS, включённое в данный документ). Доменное имя, в котором последняя метка указывает корень графа, является полным, другие имена, чьи метки формируют строгий префикс полного доменного имени, связаны с первым опущенным узлом.

В разных документах IETF и других организаций термин «доменное имя» может использоваться по-разному. Обычно в предшествующих документах этот термин означает «имена, соответствующие синтаксису [RFC1035]», возможно, с дополнительными правилами, такими как «и являются или могут быть распознаваемыми в глобальной системе DNS» или «но только с использованием формата представления».

Label - метка

Упорядоченный список октетов (возможно пустой), составляющих часть доменного имени. В теории графов метка идентифицирует узел в части графа всех возможных доменных имён.

Global DNS - глобальная система DNS

С использованием краткого набора аспектов из Naming system глобальную систему DNS можно определить, как показано ниже. Большинство правил взято из [RFC1034] и [RFC1035], но термин global DNS определяется впервые.

Composition of names - состав имён

Имя в глобальной системе DNS имеет одну или несколько меток, размер каждой из которых составляет от 0 до 63 октетов (включительно). В полном доменном имени последняя метка в упорядоченном списке имеет размер 0 октетов, это единственная метка такого размера и она называется корнем (root) или корневой меткой (root label). Размер доменного имени в глобальной системе DNS не может превышать 255 октетов в формате передачи, корень вносит в этот размер 1 октет (в Multicast DNS [RFC6762] разрешаются имена размером 255 байтов плюс 1 завершающий нулевой байт на основе иной интерпретации RFC 1035 и учёта включаемого в 255 октетов).

Format of names - формат имён

Имена в глобальной системе DNS являются доменными именами. Имеется три формата имён - формат передачи, формат представления и базовый формат отображения.

Wire format - формат передачи

Базовым форматом передачи для имён в глобальной системе DNS является список меток, упорядоченных по удалению от корня, где корневая метка является последней. Каждой метке предшествует октет её размера. В [RFC1035] задана схема сжатия, меняющая этот формат.

Presentation format - формат представления

Форматом представления имён в глобальной системе DNS является список меток, упорядоченных по удалению от корня, в кодировке ASCII с разделением меток символом точки (.). Ф формате представления полное доменное имя включает корневую метку и связанную с ней точку. Например, полное доменное имя с двумя некорневыми метками в формате представления будет иметь вид «example.tld.», а не «example.tld». В [RFC1035] определён метод показа октетов, не отображающихся в кодировке ASCII.

Common display format - базовый формат отображения

Базовый формат отображения применяется в приложениях и произвольных текстах. Он отличается от формата представления лишь необязательностью указания корневой метки и связанной с ней точки. Например, в базовом формате отображения полное доменное имя с двумя некорневыми метками обычно имеет вид «example.tld», а не «example.tld.». Имена в базовом формате отображения обычно записываются так, чтобы с учётом направления письма метки размещались в порядке снижения расстояния от корня. Например, в английском языке и языке программирования С корень или метка верхнего уровня (Top-Level Domain или TLD) размещаются справа, а в арабских языках могут размещаться слева в зависимости от местных традиций.

Administration of names - администрирование имён

Администрирование задаётся путём передачи полномочий (см. определение термина delegation в разделе 7). Правила администрирования корневой зоны в глобальной системе DNS определяются операционным сообществом, организуемым в рамках Корпорации Internet по назначению имён и номеров (Internet Corporation for Assigned Names and Numbers или ICANN). Это сообщество выбирает оператора функций IANA (Functions Operator) для корневой зоны глобальной системы DNS. Серверы имён, обслуживающие корневую зону, предоставляются независимыми корневыми операторами. В других зонах глобальной системы DNS имеются свои правила администрирования.

Types of data that can be associated with names - типы данных, которые могут быть связаны с именами

С именем могут (необязательно) связаны записи о ресурсах. Имеется множество типов таких записей с уникальными структурами данных, определёнными в разных RFC и реестре IANA [IANA_Resource_Registry].

Types of metadata for names - типы метаданных для имён

Любое имя, опубликованное в DNS, представляется как набор записей о ресурсах (см. определение термина RRset в разделе 5). Некоторые имена сами по себе не имеют связанных с ними данных в глобальной системе DNS, но «присутствуют» в DNS, поскольку являются частью более длинных имён, с которыми связаны данные (см. определение термина empty non-terminals в разделе 7).

Protocol for getting data from a name - протокол для получения данных по имени

Протокол, описанный в [RFC1035].

Context for resolving a name - контекст для распознавания имени

Корневая зона глобальной системы DNS, распределенная по общедоступным техническим идентификаторам (Public Technical Identifier или PTI).

Private DNS - приватная систма DNS

Имена, использующие протокол из [RFC1035], но не связанные с корневой зоной глобальной системы DNS, или недоступные всем в Internet по иным причинам. Система может использовать одновременно имена глобальной системы DNS и одной или нескольких приватных систем DNS (см., например, Split DNS в разделе 6).

Отметим, что имена, не появляющиеся в DNS и не предназначенные для поиска с использованием протокола DNS, не являются частью глобальной или приватной системы DNS, даже если они являются доменными именами.

Multicast DNS (mDNS)

«Multicast DNS (mDNS) обеспечивает возможность выполнения операций в стиле DNS на локальном канале при отсутствии какого либо обычного сервера Unicast DNS. В дополнение к этому Multicast DNS выделяет часть пространства имён DNS для свободного локального применения без необходимости внесения ежегодной платы, передачи полномочий или иной настройки традиционных серверов DNS для поиска этих имён.» (цитата из Аннотации к [RFC6762]). Несмотря на использование совместимого формата передачи, mDNS, строго говоря, является протоколом, отличным от DNS. Кроме того, в приведённой выше цитате вместо «части пространства имён DNS» уместней было бы сказать «часть пространства доменных имён». Имена mDNS не предназначены для поиска через DNS.

Locally served DNS zone - локально обслуживаемая зона DNS

Локально обслуживаемая зона DNS является частным случаем приватной системы DNS, где имена распознаются с использованием протокола DNS в локальном контексте. В [RFC6303] заданы субдомены IN-ADDR.ARPA, являющиеся зонами с локальным обслуживанием. Распознавание имён через локально обслуживаемые зоны может давать неоднозначные результаты. Например, одно и то же имя может распознаваться по-разному в разных контекстах локально обслуживаемых зон DNS. Контекст локально обслуживаемой зоны DNS может быть явным (например, как указано в [RFC6303] и [RFC7793]) или неявным (например, заданным локальным администратором DNS и неизвестным клиенту распознавания).

Fully Qualified Domain Name (FQDN) - полное доменное имя

Зачастую это просто эквивалент термина domain name of a node, указанного выше, однако такой вариант неоднозначен. Строго говоря, полное доменное имя должно включать все метки, в том числе метку корня с

нулевым размером - такое имя записывается как «www.example.net.» (точка в конце). Однако все имена имеют общий корень, поэтому они часто указываются относительно этого корня (www.example.net) и все равно называются полными. Термин был введён в [RFC819]. В этом документе имена часто указываются от корня.

Необходимость термина «полное доменное имя» обусловлена существованием неполных доменных имён, где одна или несколько последних меток в списке опущены (например, www относительно example.net указывает www.example.net). Такие относительные имена понятны только с учётом контекста.

Host name - имя хоста

Этот термин и его эквивалент hostname используются широко, но не определены в [RFC1034], [RFC1035], [RFC1123], [RFC2181]. Система DNS исходно была развёрнута в среде с таблицами хостов (Host Table), как описано в [RFC952], и термин, вероятно, неформально следовал определению из этого документа, но со временем определение изменилось. Имя хоста часто указывает доменное имя, соответствующее правилам из параграфа 3.5 в [RFC1034], которые называют также предпочтительным синтаксисом имён (preferred name syntax), где каждый символ в каждой метке является буквой, цифрой или дефисом (-). Отметим, что любая метка в доменном имени может содержать любые значения октетов, а имена хостов обычно считаются доменными именами, где каждая метка следует правилам предпочтительного синтаксиса имён с поправкой на то, что метки могут начинаться с цифр ASCII (параграф 2.1 в [RFC1123]).

Термин hostname иногда используют для обозначения первой метки в FQDN, например, printer в printer.admin.example.com (иногда это формализуется в конфигурации операционных систем). Кроме того, термин иногда служит для описания любого имени, указывающего машину, и может включать метки, не соответствующие правилам предпочтительного синтаксиса имён.

Top-Level Domain (TLD) - домен верхнего уровня

Доменом верхнего уровня называют зону на 1 уровень ниже корня, такую как com или jp. С точки зрения DNS в TLD нет ничего особого. Большинство TLD являются зонами, ориентированными на передачу полномочий (определена в разделе 7), и их функционирование связано с существенными политическими вопросами. TLD часто делятся на подгруппы, такие как домены верхнего уровня с кодом страны (Country Code Top-Level Domain или ccTLD), базовые домены верхнего уровня (Generic Top-Level Domainили gTLD) и т. п. такое деление является вопросом политики и выходит за рамки этого документа.

Internationalized Domain Name (IDN) - доменное имя на национальном языке

Протокол доменов на национальных языках для приложений (Internationalized Domain Names for Applications или IDNA) обеспечивает стандартный механизм для обработки доменных имён с символами, отличными от ASCII, в приложениях DNS. На момент подготовки этого документа текущий стандарт, обычно называемый IDNA2008, определялся [RFC5890], [RFC5891], [RFC5892], [RFC5893] и [RFC5894]. В этих документах задано множество относящихся к IDN терминов, таких как LDH label, A-label, U-label. В [RFC6365] определены дополнительные термины, связанные с использованием национальных языков (часть их относится к IDN), в [RFC6055] приведено дополнительное рассмотрение IDN, включая новую терминологию.

Subdomain - субдомен

«Домен является субдоменом другого домена, если он содержится в том домене. Для проверки принадлежности достаточно убедиться, что в конце имени субдомена содержится имя домена. » (цитата из параграфа 3.1 в [RFC1034]). Например, в имени хоста nnn.mmm.example.com компоненты mmm.example.com и nnn.mmm.example.com являются субдоменами домена example.com. Отметим, что при сравнении учитываются метки целиком, т. е. ooo.example.com не будет субдоменом oo.example.com.

Alias - псевдоним

Владелец записи о ресурсе CNAME или субдомен владельца записи о ресурсе DNAME (определена в [RFC6672]). См. также canonical name.

Canonical name - каноническое имя

Запись о ресурсе CNAME «идентифицирует имя своего владельца в качестве псевдонима и задаёт соответствующее каноническое имя в разделе RDATA записи RR» (цитата из параграфа 3.6.2 в [RFC1034]). Такое использование термина «канонический» связано с математической концепцией канонической формы.

CNAME

«По традиции [владельца] метку[и] записи CNAME называют просто «CNAME». Это неудачная традиция, поскольку CNAME является сокращением «canonical name», а [владелец] метку[и] записи CNAME чаще всего не является каноническим именем» (цитата из параграфа 10.1.1 в [RFC2181] с заменой метки на владельца метки).

3. Коды откликов DNS

Некоторые коды откликов (response code или RCODE), заданные в [RFC1035], получили свои сокращённые имена. Все RCODE перечислены в реестре [IANA_Resource_Registry], где строчные и прописные буквы смешаны, хотя в большинстве документов применяются только заглавные буквы. В этом разделе описаны некоторые распространённые имена, заданные в [RFC1035], а также включён новый код и его описание. Полный список RCODE приведён в реестре IANA.

NOERROR

Этот код описан как отсутствие ошибок (No error condition) в параграфе 4.1.1 [RFC1035].

FORMERR

Этот код описан как ошибка формата, не позволяющая серверу интерпретировать запрос (Format error - The name server was unable to interpret the query), в параграфе 4.1.1 [RFC1035].

SERVFAIL

Этот код описан как отказ сервера, связанный с его неспособностью обработать запрос из-за своих проблем (Server failure - The name server was unable to process this query due to a problem with the name server), в параграфе 4.1.1 [RFC1035].

NXDOMAIN

Этот код описан как ошибка имени, связанная с отсутствием на сервере указанного в запросе имени (Name Error [...] this code signifies that the domain name referenced in the query does not exist), в параграфе 4.1.1 [RFC1035]. В [RFC2308] код NXDOMAIN указан как синоним Name Error.

NOTIMP

Этот код описан как отсутствие поддержки сервером имён запрошенной функции (Not Implemented - The name server does not support the requested kind of query) в параграфе 4.1.1 [RFC1035].

REFUSED

Этот код описан как отклонение запроса в соответствии с правилами сервера, например, нежеланием предоставлять сведения конкретному запрашивающему или выполнять определённую информацию, такую как перенос зоны, для конкретных данных (Refused - The name server refuses to perform the specified operation for policy reasons. For example, a name server may not wish to provide the information to the particular requester, or a name server may not wish to perform a particular operation (e.g., zone transfer) for particular data) в параграфе 4.1.1 [RFC1035].

NODATA

«Псевдо-RCODE, указывающий, что имя корректно для данного класса, но записей этого типа нет. Код NODATA выводится из ответа» (цитата из раздела 1 в [RFC2308]). «NODATA указывается ответом с RCODE = NOERROR и отсутствием имеющей отношение к делу информации в разделе ответов. Раздел полномочий будет содержать запись SOA или в нем совсем не будет записей NS» (цитата из параграфа 2.2 в [RFC2308]). Отметим, что рекомендации (referral) имеют формат, похожий на NODATA, и в [RFC2308] указано, как различать их.

Термин NXRRSET иногда применяется как синоним NODATA, однако это является ошибкой, поскольку для NXRRSET задан конкретный код ошибки [RFC2136].

Negative response - негативный отклик

Отклик, заказывающий, что конкретного набора RRset не существует, или RCODE для него говорит, что сервер не может ответить. Типы негативных откликов подробно рассмотрены в разделах 2 и 7 [RFC2308].

4. Транзакции DNS

Заголовком сообщения DNS являются первые 12 октетов. Многие поля и флаги на рисунках в параграфах 4.1.1 - 4.1.3 [RFC1035] указываются их именами. Например, коды откликов указаны как RCODE, данные записей - как RDATA, а бит полномочности ответа - как флаг (бит) AA.

Class - класс

Класс указывает «семейство протоколов или экземпляр протокола» (цитата из параграфа 3.6 в [RFC1034]). «DNS помечает все данные тегом класса и типа, что позволяет параллельно использовать разные форматы для данных типа адрес.» (цитата из параграфа 2.2 в [RFC1034]). На практике почти в каждом запросе используется класс IN (Internet). Имеется несколько запросов для класса CH (Chaos), но они обычно служат для получения сведений о самом сервере, а не для получения другого типа адреса.

QNAME

Наиболее распространённым является грубое определение QNAME как поля в разделе запроса Question. «Стандартный запрос задает искомое доменное имя (QNAME), тип (QTYPE) и класс (QCLASS) запроса, а также запрашивает соответствующие записи RR.» (цитата из параграфа 3.7.1 в [RFC1034]). Строго говоря, определение взято из параграфа 4.1.2 в [RFC1035], где QNAME определяется применительно к разделу Question. Это определение, по-видимому, применяется согласованно, поскольку при обсуждении реверсных запросов в параграфе 6.4.1 [RFC1035] указывается «имя владельца RR запроса и значение TTL», так как при реверсных запросах заполняется поле Answer, а раздел Question остаётся пустым (реверсные запросы отменены в [RFC3425], поэтому в данном документе нет соответствующих определений).

В [RFC2308] имеется альтернативное определение, помещающее QNAME в ответ (или последовательность ответов) вместо запроса. QNAME определяется как «Имя в запросном разделе (query section) ответа или место, где оно преобразуется в CNAME или цепочку CNAME, поле данных последней записи CNAME. Последней CNAME в данном случае считается запись, содержащая значение, которое не преобразуется в другую запись CNAME». В этом определении есть некая внутренняя логика, обусловленная определением и способом подстановки CNAME. Если сервер имён не находит набора RRset, соответствующего запросу, но находит то же имя в неком классе с записью CNAME, он «включает запись CNAME в отклик и повторяет запрос для доменного имени, заданного в поле данных записи CNAME» (цитата из параграфа 3.6.2 в [RFC1034]). Это явно указано в алгоритме распознавания, описанном в параграфе 4.3.2 [RFC1034]: «QNAME меняется на каноническое имя в CNAME RR и выполняется возврат к п 1». Поскольку запись CNAME явно говорит, что имя владельца является каноническим именем того, что содержится в RDATA, можно рассматривать новое имя (имя, которое было в RDATA записи CNAME RR) как QNAME. Однако это создаёт путаницу, поскольку отклик на запрос, который ведёт к обработке CNAME, содержит в отражённом разделе Question два значения QNAME - имя в исходном запросе и содержимое поля данных в последнем CNAME. Путаница возникает из-за итерационного (рекурсивного) режима распознавания, возвращающего в результате отклик, который не обязательно имеет то же имя владельца, что и QNAME в исходном запросе.

Для предотвращения возможной путаницы полезно различать три указанных ниже значения.

QNAME (исходное)

Имя, фактически переданное в разделе Question исходного запроса, которое всегда отражается (echo) в разделе Question (финального) отклика, когда установлено значение 1 для бита QR.

QNAME (эффективное)

Фактически распознанное имя, которое является исходно запрошенным или полученным в цепочке откликов CNAME.

QNAME (финальное)

Фактически распознанное имя, которое является исходно запрошенным или последним именем в цепочке откликов CNAME.

Поскольку определение в [RFC2308] относится фактически не к тому понятию, которое было принято в [RFC1034], лучше было бы использовать в [RFC2308] другое имя для этого понятия. В современной практике QNAME почти всегда означает то, что выше отмечено как QNAME (исходное).

Referrals - рекомендации (перенаправление)

Тип отклика, в котором сервер, сообщая о своей полной неполномочности для отклика, указывает запрашивающему распознавателю другое место для отправки запроса. Рекомендации могут быть частичными.

Рекомендации возникают, когда сервер не выполняет рекурсивное обслуживание при ответе на запрос. Это показано на этапе 3(b) алгоритма [RFC1034] (параграф 4.3.2).

Имеется два типа перенаправления. Первый указывает перенаправление вниз (downward referral, иногда описывается как отклик делегирования - delegation response), когда сервер полномочен для некоторой части QNAME. Раздел Authority в RDATA набора RRset содержит серверы имён, указанные на срезе зоны referred-to. При обычной работе DNS этот тип откликов нужен для поиска имён ниже передачи полномочий. Использование термина referral без дополнительных атрибутов означает именно этот вариант и многие считают его единственным

допустимым типом перенаправления в DNS. Второй вариант перенаправляет вверх (upward referral, иногда описывается как перенаправление к корню - root referral), когда у сервера совсем нет полномочий для QNAME. В этом случае зоной referred-to в разделе Authority обычно является корневая зона (.). При нормальной работе DNS этот тип откликов не требуется для распознавания и корректного ответа на любой запрос. От серверов не требуется передавать перенаправление вверх и некоторые считают такое перенаправление признаком ошибочной настройки или ошибки. Для перенаправления вверх всегда требуется то или иное уточнение (например, upward или root) и оно никогда не указывается просто словом referral.

Отклик, содержащий лишь рекомендации, имеет пустой раздел Answer и содержит NS RRset для зоны referred-to в разделе Authority. Отклик может содержать RR, указывающие адреса, в разделе Additional. Бит AA сброшен.

В случае, когда запрос соответствует псевдониму (alias) и сервер не полномочен для цели этого псевдонима, но имеет полномочия для некого имени выше этой цели, алгоритм распознавания будет создавать отклик, который содержит полномочный ответ для псевдонима и перенаправление. Такой отклик с частичным ответом и перенаправлением содержит данные в разделе Answer, а в разделе Authority содержится NS RRset для зоны referred-to. Отклик может содержать RR, указывающие адреса, в разделе Additional. Бит AA установлен, поскольку первое имя в разделе Answer соответствует QNAME и сервер полномочен для ответа (см. параграф 4.1.1 в [RFC1035]).

5. Записи о ресурсах

RR

Сокращение для записи о ресурсах (resource record), см. параграф 3.6 в [RFC1034].

RRset

Набор записей о ресурсах «с совпадающими метками, типом и классом, но различными данными» (согласно разделу 5 в [RFC2181]). Иногда применяется обозначение RRSet. «Одна метка» в этом определении означает «одно имя владельца». Кроме того, в [RFC2181] сказано: «все значения TTL для записей RR в наборе RRSet должны быть одинаковы». Отметим, что записи RRSIG не соответствуют этому определению. В [RFC4035] сказано:

> Процесс создания RRSIG RR для данного набора RRset описан в [RFC4034]. Набор RRset может включать множество связанных с ним записей RRSIG. Отметим, что по причине тесной связи записей RRSIG RR с наборами RRset, чьи сигнатуры эти записи содержат, записи RRSIG RR, в отличие от других типов DNS RR, не формируют наборов RRset. В частности, значения TTL для записей RRSIG RR с общим именем владельца, не следуют правилам для RRset, описанным в [RFC2181].

Master file - первичный файл

«Первичные файлы являются текстовыми и содержат записи RR в виде текста. Поскольку содержимое зоны может быть выражено в форме списка RR, первичные файлы используются в основном для определения зон, хотя их можно применять и для списков содержимого кэша» (цитата из раздела 5 в [RFC1035]). Первичные файлы иногда называют файлами зоны (zone file).

Presentation format - формат представления

Текстовый формат, используемый в первичных файлах. Этот формат показан, но не определён формально в [RFC1034] и [RFC1035]. Термин presentation format впервые использован в [RFC4034].

EDNS

Механизмы расширения для DNS, определённые в [RFC6891]. Иногда применяются обозначения EDNS0 и EDNS(0) для указания номера версии. EDNS позволяет клиентам и серверам DNS задавать размер сообщений больше заданных исходно 512 октетов, расширять пространство кодов откликов и передавать дополнительные опции, влияющие на обработку запросов DNS.

OPT

Псевдо-RR (иногда называется meta-RR), используемая для управляющей информации, относящейся к последовательности запросов и откликов конкретной транзакции (перефразированное определение из параграфа 6.1.1 в [RFC6891]). Применяется в EDNS.

Owner - владелец

«Имя домена, где найдена RR» (цитата из параграфа 3.6 в [RFC1034]). Зачастую применяется термин owner name.

SOA field names - имена полей SOA

В документах DNS, включая приведённые здесь определения, поля в RDATA записи о ресурсах SOA указываются по именам. SOA является сокращением от начала зоны полномочий (start of a zone of authority). Эти поля определены в параграфе 3.3.13 [RFC1035]. Имена полей (в порядке их указания в SOA RDATA) - MNAME, RNAME, SERIAL, REFRESH, RETRY, EXPIRE, MINIMUM. Отметим, что назначение поля MINIMUM обновлено в разделе 4 [RFC2308] и новое определение говорит, что поле MINIMUM - это только «TTL для негативных откликов». В этом документе как правило используются имена полей, а не описывающие поля термины.

TTL

Максимальный срок действия (time to live) записи о ресурсе. «Поле TTL представляет собой целое число без знака с минимальным значением 0 и максимальным 2147483647 (т. е., 2^{31} - 1). При передаче это значение следует помещать в младшие биты (31) 32-битового поля TTL, устанавливая для старшего бита (знак) нулевое значение.» (цитата из раздела 8 в [RFC2181]). Отметим, что в [RFC1035] ошибочно указано, что это целое число со знаком. Ошибка исправлена в [RFC2181].

TTL «задаёт временной интервал, в течение которого запись может кэшироваться прежде, чем снова возникнет необходимость обращения к источнику данных» (цитата из параграфа 3.2.1 в [RFC1035]). В параграфе 4.1.3 [RFC1035] сказано: «временной интервал (в секундах), в течение которого запись может кэшироваться до ее отбрасывания». Несмотря на определение для записи о ресурсе, значение TTL в каждой записи RRset должно быть одинаковым ([RFC2181], параграф 5.2).

Причина того, что TTL указывает максимальный срок действия, заключается в том, что оператор может сократить срок действия в оперативных целях, например при наличии запрета TTL больше определённого значения. Известно, что некоторые серверы игнорируют TTL в некоторых RRset (например, когда для полномочных данных установлен очень короткий срок действия), хотя это противоречит рекомендациям [RFC1035]. RRset может удаляться из кэша до завершения интервала TTL, при этом значение TTL становится неизвестным, поскольку RRset, с которым оно связано, больше не существует.

Существует также концепция принятого по умолчанию срока действия (default TTL) для зоны, который может быть параметром конфигурации программы сервера. Часто это выражается принятым по умолчанию значением для всего сервера и для зоны с помощью директивы $TTL в файле зоны. Директива $TTL была добавлена в формат первичного файла документом [RFC2308].

Class independent - независимый от класса

Тип записи о ресурсе, синтаксис и сементика которого одинаковы для каждого класса DNS. Тип записи о ресурсе, не являющийся независимым от класса, имеет разную трактовку в зависимости от класса DNS, к которому относится запись, если трактовка не определена для некоторых классов. Большинство типов записей о ресурсах определено для класса 1 (IN, Internet), но многие записи не определены для других классов.

Address records - адресные записи

Записи типа A или AAAA. В [RFC2181] они неформально определены как «(A, AAAA и т. п.)». Отметим, что в будущем могут быть определены новые типы адресных записей.

6. Серверы и клиенты DNS

В этом разделе даны определения терминов, используемых для систем, являющихся клиентами и/или серверами DNS. В прошлых RFC серверы DNS иногда назывались серверами имён (name server, nameserver) или просто серверами. Формального определения сервера DNS не существует, но в RFC обычно предполагается, что это сервер Internet, прослушивающий запросы и отправляющий отклики с использованием протокола DNS, заданного в [RFC1035] и его преемниках.

Важно отметить, что термины сервер DNS и сервер имён требуют контекста для понимания предоставляемых услуг. Как полномочные (authoritative) серверы, так и рекурсивные распознаватели (recursive resolver) часто называют серверами DNS и серверами имён, хотя их функции различаются (те и другие могут быть частями одного программного пакета).

Термины, относящиеся к системе глобальных корневых серверов DNS, приведены в [RSSAC026], где определены такие термины как root server (корневой сервер), root server operator (оператор корневого сервера), а также термины, связанные со способами обслуживания корневой зоны глобальной системы DNS.

Resolver - распознаватель

«Программа, извлекающая из серверов имен информацию в ответ на запрос клиента» (цитата из параграфа 2.4 в [RFC1034]). Распознаватель выполняет запросы по имени, типу и классу, получая отклики. Логическая функция называется распознаванием (resolution). На практике термин обычно обозначает тот или иной тип распознавателя (некоторые типы определены ниже) и трактовка термина зависит от понимания контекста.

Связанным термином является resolve, для которого нет формального определения в [RFC1034] и [RFC1035]. Вмененное определение может иметь вид: «задание вопроса, состоящего из доменного имени, класса и типа и получение какого-то ответа». Вмененным определением для распознавания (resolution) может быть: «ответ, полученный от распознавания».

Stub resolver - распознаватель-заглушка

Распознаватель, не способный самостоятельно выполнить распознавание. Заглушки обычно зависят от рекурсивного распознавателя, который принимает на себя функцию фактического распознавания. Распознаватели-заглушки обсуждаются в параграфе 5.3.1 [RFC1034], но не определены там формально. Полное определение дано в параграфе 6.1.3.1 [RFC1123].

Iterative mode - итерационный режим

Режим распознавания, при котором получающий запросы сервер DNS отвечает ссылкой (рекомендацией — referral) на другой сервер. В параграфе 2.3 [RFC1034] это описано так: «сервер указывает клиенту другой сервер, который способен ответить на запрос клиента». Распознаватель, работающий в итерационном режиме иногда называют итерационным распознавателем (iterative resolver). См. также определение термина iterative resolution ниже.

Recursive mode - рекурсивный режим

Режим распознавания, при котором получающий запросы сервер DNS отвечает на них с использованием локального кэша или передаёт запросы другим серверам для получения окончательных ответов на них. В параграфе 2.3 [RFC1034] это описано так: «когда первый сервер транслирует (передаёт) запрос клиента другому серверу». В параграфе 4.3.1 [RFC1034] сказано: «в этом [рекурсивном] режиме сервер имён выполняет функции распознавателя имён и всегда возвращает ответ или сообщение об ошибке, но не ссылку на другой сервер». В этом же параграфе сказано:

> Рекурсивный режим возникает в тех случаях, когда запрос с установленным флагом RD поступает на сервер, который желает обеспечивать рекурсивный сервис; клиент может убедиться в использовании рекурсивного режима, проверяя наличие в отклике обоих флагов RA и RD.

Работающий в рекурсивном режиме сервер можно рассматривать как комбинацию сервера имён (отвечает на запросы) и распознавателя (выполняет функцию распознавания). Работающие в таком режиме системы обычно называют рекурсивными серверами (recursive server), а иногда - рекурсивными распознавателями (recursive resolver). Эти термины могут применяться как взаимозаменяемые. На практике нет возможности узнать заранее, будет ли запрашиваемый сервер выполнять рекурсию.

Recursive resolver - рекурсивный распознаватель

Распознаватель, работающий в рекурсивном режиме. В общем случае предполагается кэширование таким распознавателем полученных откликов, что делает его полнофункциональным распознавателем, но некоторые рекурсивные распознаватели могут не поддерживать кэширование. В [RFC4697] предпринята попытка провести различие между рекурсивными и итерационными распознавателями.

Recursive query - рекурсивный запрос

Запрос с установленным (1) битом желательности рекурсии (Recursion Desired или RD) в заголовке (см. параграф 4.1.1 в [RFC1035]). Если рекурсивный сервис доступен и в запросе установлен бит RD, сервер использует свой распознаватель для ответа на запрос (см. параграф 4.3.2 в [RFC1034].)

Non-recursive query - нерекурсивный запрос

Запрос со сброшенным (0) битом RD в заголовке. Сервер может отвечать на такой запрос только локальными сведениями или возвращать ссылку на другой сервер, который «ближе» к ответу (см. параграф 4.3.1 в [RFC1034]).

Iterative resolution - итерационное распознавание

Сервер имён может получить запрос, на который способен ответить только другой сервер. Для решения этой проблемы имеется два подхода - рекурсивный, когда первый сервер выполняет от имени клиента запрос к другому серверу, и итерационный, когда сервер указывает клиенту другой сервер для передачи запроса тому (см. параграф 2.3 в [RFC1034]). При итерационном распознавании клиент повторяет нерекурсивные запросы и следует за перенаправлениями и/или псевдонимами (alias). Алгоритм итерационного распознавания описан в параграфе 5.3.3 [RFC1034].

Full resolver - полный распознаватель

Этот термин применяется в [RFC1035], но не определён там. В RFC 1123 определён полнофункциональный распознаватель (full-service resolver), который может совпадать или не совпадать с тем, что подразумевалось по full resolver в [RFC1035]. Это термин не определён должным образом ни в одном RFC и нет единого мнения о его трактовке. Использовать термин без надлежащего контекста не рекомендуется.

Full-service resolver

В параграфе 6.1.3.1 [RFC1123] этот термин определён как распознаватель, работающий в рекурсивном режиме с кэшированием (и соответствующий другим требованиям).

Priming - подготовка

«Поиск списка корневых серверов по конфигурации, где указаны все или некоторые предполагаемые адреса IP корневых серверов» (цитата из раздела 2 в [RFC8109]). Для работы в рекурсивном режиме распознавателю нужно знать адрес хотя бы одного корневого сервера. Подготовка зачастую выполняется по конфигурации, содержащей список полномочных серверов корневой зоны.

Root hints - подсказки корневых серверов

«Операторам рекурсивных распознавателей DNS обычно нужно настроить «файл подсказки корневых серверов» (root hints file). Этот файл содержит имена и адреса IP полномочных серверов имён корневой зоны, чтобы программы могли запускать процесс распознавания DNS. Во многих программах этот список является встроенным» (цитата из [IANA_RootFiles]). Файл подсказок часто используется при подготовке.

Negative caching - негативное кэширование

«Хранение информации о том, что чего-либо не существует, ответ не может быть получен или его не дают» (цитата из раздела 1 в [RFC2308]).

Authoritative server - полномочный сервер

«Сервер, знающий содержимое зоны DNS из локальных сведений и способный, тем самым, отвечать на запросы для зоны без необходимости обращения к другим серверам» (цитата из раздела 2 в [RFC2182]). Полномочный сервер указан в записи NS (name server) для зоны. Это система, отвечающая на запросы DNS сведениями о зонах, для которых она была настроена на отклик, с установленным (1) в заголовке отклика флагом AA. Это сервер, имеющий полномочия для одной или нескольких зон DNS. Отметим, что полномочный сервер может отвечать на запросы без передачи ему полномочий родительской зоны. Полномочные серверы также предоставляют рекомендации (referral), обычно для дочерних зон, получивших полномочия от них. В этих рекомендациях бит AA сброшен (0) и содержатся данные перенаправления в разделе Authority, а при необходимости и в разделах Additional.

Authoritative-only server - сервер, выполняющий только функции полномочного (без рекурсии)

Сервер, обслуживающий лишь полномочные данные и игнорирующий запросы на рекурсию. Обычно он «не генерирует запросов сам. Сервер отвечает на нерекурсивные запросы от итерационных распознавателей, ищущих информацию в обслуживаемых им зонах» (цитата из параграфа 2.4 в [RFC4697]). В этом случае игнорирование запросов на рекурсию означает ответ на них откликами, указывающими, что рекурсия не выполняется.

Zone transfer - перенос зоны

Действие, при котором клиент запрашивает копию зоны, а полномочный сервер передаёт требуемые сведения (описание зон приведено в разделе 7). Имеется два базовых стандартных способа переноса зон - AXFR (Authoritative Transfer) для копирования всей зоны [RFC5936] и IXFR ("Incremental Transfer") для копирования лишь изменившихся частей зоны [RFC1995]. Во многих системах применяются нестандартные методы переноса зон, выходящие за рамки протокола DNS.

Slave server - ведомый сервер

См. Secondary server.

Secondary server - вторичный сервер

«Полномочный сервер, который использует перенос зоны для ее получения» (цитата из параграфа 2.1 в [RFC1996]). Вторичные серверы обсуждаются также в [RFC1034], а в [RFC2182] они описаны более подробно. Хотя в ранних DNS RFC, таких как [RFC1996], использовался термин «ведомый» (slave), сейчас принято называть такие серверы вторичными (secondary).

Master server - ведущий сервер

См. Primary server.

Primary server - первичный сервер

«Любой полномочный сервер, настроенный на то, чтобы играть роль источника при переносе зоны для одного или нескольких [вторичных] серверов» (цитата из параграфа 2.1 в [RFC1996]). Более конкретно в [RFC2136] указано, что это: «полномочный сервер, настроенный как источник данных AXFR или IXFR для одного или нескольких [вторичных] серверов». Первичные серверы обсуждаются также в [RFC1034]. Хотя в ранних DNS RFC, таких как [RFC1996], использовался термин «ведущий» (master), сейчас принято называть такие серверы первичными (primary).

Primary master - первичный ведущий

«Первичный ведущий сервер зоны указывается в поле SOA MNAME, а также может указываться в NS RR» (цитата из параграфа 2.1 в [RFC1996]). В [RFC2136] термин primary master определён как: «Ведущий сервер в корне графа зависимостей AXFR/IXFR. Первичный ведущий сервер зоны указывается в поле SOA MNAME, а также может указываться в NS RR. По определению имеется лишь один первичный ведущий сервер на зону».

Идея первичного ведущего сервера используется лишь в [RFC1996] и [RFC2136]. В современной интерпретации primary master - это сервер, который является полномочным для зоны и получает обновления зоны из конфигурации (например, первичного файла) или транзакций UPDATE.

Stealth server - скрытый сервер

«Похож на ведомый сервер, но не указывается в NS RR для данной зоны» (цитата из параграфа 2.1 в [RFC1996]).

Hidden master - скрытый ведущий

Скрытый сервер, который является первичным для переноса зон. «При такой схеме ведущий сервер имён, обрабатывающий обновления, недоступен для хостов общего назначения в Internet, он не указывается в NS RRset» (цитата из параграфа 3.4.3 в [RFC6781]). В [RFC4641] сказано, что имя скрытого ведущего «присутствует в поле MNAME записей SOA RR», однако это имя вообще не присутствует в некоторых серверах глобальной системы DNS. Скрытый ведущий может быть также вторичным сервером для самой зоны.

Forwarding - пересылка

Процесс передачи сервером запроса DNS с установленным (1) битом RD другому серверу для распознавания. Пересылка является функцией распознавателя DNS и отличается от простой ретрансляции запросов вслепую.

В [RFC5625] не дано конкретного определения пересылки, но подробно описаны функции которые должна поддерживать система, выполняющая пересылку. Системы с пересылкой иногда называют DNS-прокси, но этот термин ещё не определён (даже в [RFC5625]).

Forwarder - пересылающий сервер

В разделе 1 [RFC2308] пересылающий сервер описан как «Сервер имён, используемый для распознавания (resolve) запросов взамен прямого использования цепочки полномочных серверов имён». Кроме того, в [RFC2308] сказано: «Обычно пересылающий сервер имеет более качественный доступ в Internet или поддерживает кэш большего размера, совместно используемый множеством распознавателей имён». Из этого определения следует, что пересылающие серверы обычно обращаются в запросами лишь к полномочным серверам. Однако в настоящее время пересылающие серверы часто занимают промежуточное место между распознавателями-заглушками (stub) и рекурсивными серверами. В [RFC2308] не сказано, является ли пересылающий сервер только итерационным или полнофункциональным распознавателем.

Policy-implementing resolver - реализующий правила распознаватель

Распознаватель, работающий в рекурсивном режиме и изменяющий некоторые отклики, которые он возвращает, на основе критериев политики, например, для предотвращения доступа к сайтам с вредоносными программами или нежелательным содержимым. В общем случае распознаватели-заглушки не имеют представления о применении восходящими распознавателями политики и вносимых ею изменениях. В некоторых случаях пользователь распознавателя-заглушки выбирает распознаватель с применением правил с явным намерением использовать его для применения политики. В других случаях правила навязываются пользователям без уведомления пользователей распознавателя-заглушки.

Open resolver - открытый распознаватель

Полнофункциональный распознаватель, воспринимающий и обрабатывающий запросы от любых (или почтчи любых) клиентов. Их иногда называют общедоступными (public), хотя термин public resolver чаще применяется к распознавателям, которые предусмотрены как общедоступные, в отличие от распознавателей, которые открыты из-за ошибок в настройке. Открытые распознаватели обсуждаются в [RFC5358].

Split DNS - расщепление DNS

Термины split DNS и split-horizon DNS уже давно применяются в сообществе DNS без формального определения. Обычно они относятся к случаям, когда серверы DNS, полномочные для определённого набора доменов, дают разные ответы для этих доменов в зависимости от источника запроса. Результатом этого является то, что доменное имя, которое условно является уникальным в глобальном масштабе, имеет разный смысл для разных пользователей сети. Иногда это может быть результатом настройки представлений (view), описанных ниже.

В параграфе 3.8 [RFC2775] приведено связанное определение, которое слишком специфично, чтобы быть полезным в общем случае.

View - представление

Конфигурация сервера DNS, позволяющая ему предоставлять разные отклики в зависимости от атрибутов запроса, например для расщепления DNS. Обычно представления различаются по IP-адресу источника запроса, но могут различаться и по IP-адресу назначения, типу запроса (например, AXFR), его рекурсивности и т. п. Представления часто применяются для предоставления во «внутреннюю» защищённую сеть большего числа имён, чем во «внешнюю» незащищённую. Представления не являются стандартизованной частью DNS, но реализованы во многих серверных программах.

Passive DNS - пассивная система DNS

Механизм сбора данных DNS за счёт сохранения откликов DNS от серверов имён. Некоторые из таких систем собирают также связанные с откликами запросы DNS, хотя при этом возникают некоторые проблемы приватности. Базы данных пассивных систем DNS могут использоваться для ответов на исторические запросы о зонах DNS, например, о значениях, присутствовавших в прошлом, или времени появления имени. Базы данных пассивных DNS позволяют искать хранящиеся записи по ключам, отличающимся от имени и типа, например, «найти все имена, в которых есть запись A с определённым значением».

Anycast

«Технология, позволяющая сделать определённый адрес службы (Service Address) доступным во множестве дискретных, автономных пунктов, чтобы дейтаграмма, отправленная по anycast-адресу, маршрутизировалась в одно из доступных мест» (цитата из раздела 2 в [RFC4786]). В [RFC4786] приведено более подробное объяснение для Anycast и других терминов, связанный с таким использованием.

Instance - экземпляр

«При использовании anycast-маршрутизации, позволяющей нескольким серверам иметь один адрес IP, каждый из этих серверов принято называть экземпляром». Далее в [RSSAC026] сказано: «Экземпляр сервера, например, корневого, часто называют Anycast-экземпляром».

Privacy-enabling DNS server - сервер DNS с поддержкой приватности

«Сервер DNS, реализующий DNS на основе TLS [RFC7858], который может также поддерживать DNS на основе DTLS [RFC8094]» (цитата из раздела 2 в [RFC8310]). Поддержка приватности может обеспечиваться и другими типами серверов DNS, такими как DNS-over-HTTPS [RFC8484] и DNS-over-QUIC [RFC9250].

DNS-over-TLS (DoT) - DNS на основе TLS

DNS по протоколу TLS, как определено в [RFC7858] и преемниках.

DNS-over-HTTPS (DoH) - DNS на основе HTTPS

DNS по протоколу HTTPS, как определено в DNS [RFC8484] и преемниках.

DNS-over-QUIC (DoQ) - DNS на основе QUIC

DNS по протоколу QUIC, как определено в [RFC9250] и преемниках. В [RFC9250] DoQ определён как транспорт общего назначения для DNS, который может применяться между распознавателями-заглушками (stub) и рекурсивными серверами, между рекурсивными и полномочными серверами, а также для переноса зон.

Classic DNS - классический протокол DNS

DNS по протоколу UDP или TCP, как определено в [RFC1035] и преемниках. Classic DNS применяется при взаимодействии DNS между распознавателями-заглушками и рекурсивными распознавателями, а также между рекурсивными распознавателями и полномочными серверами. Протокол иногда называют Do53. Шифрование в классическом DNS не применяется.

Recursive DoT (RdoT) - рекурсивный DNS на основе TLS

RDoT - это транспорт DNS-over-TLS для между распознавателем-заглушкой и рекурсивным распознавателем или парой рекурсивных распознавателей. Этот термин нужен, поскольку предполагается в будущем применение DNS-over-TLS в качестве транспорта между рекурсивными распознавателями и полномочными серверами.

Authoritative DoT (ADoT) - полномочный DoT

Если DNS-over-TLS в будущем станет транспортом между рекурсивными распознавателями и полномочными серверами, ADoT будет обозначать такой транспорт.

XFR-over-TLS (XoT)

Перенос зоны DNS по протоколу TLS, как задано в [RFC9103]. Этот термин применим как для AXFR over TLS (AxoT), так и для IXFR over TLS (IXoT).

7. Зоны

В этом разделе определены термины, используемые при обсуждении зон, которые обслуживаются или извлекаются.

Zone - зона

«Полномочная информация организуется в блоки, называемые зонами (ZONE) и эти зоны могут автоматически распространяться серверам имён, которые являются резервными для данных зон» (цитата из параграфа 2.4 в [RFC1034]).

Child - потомок

«Сущность (объект) в записи, которой переданы полномочия для домена от родителя (Parent)» (цитата из параграфа 1.1 в [RFC7344]).

Parent - родитель

«Домен, в котором зарегистрирован потомок (Child)» (цитата из параграфа 1.1 в [RFC7344]). Ранее в [RFC0882] был определён термин parent name server (родительский сервер имён) как «сервер имён, имеющий полномочия для пространства имён, которое будет содержать новый домен» (отметим, что [RFC0882] был отменён [RFC1034] и [RFC1035]). В [RFC819] описаны некоторые взаимоотношения между родителями и потомками.

Origin - начало (источник)

Имеется два вариант использования этого термина.

(a) «Доменное имя, появляющееся наверху зоны (сразу под срезом, отделяющим зону от её родителя)... Имя зоны совпадает с именем домена в источнике зоны» (цитата из раздела 6 в [RFC2181]. В настоящее время термины origin и apex (вершина, см. ниже) часто применяются как взаимозаменяемые.

(b) Доменное имя, в рамках которого данное относительное доменное имя появляется в файлах зоны. Обычно рассматривается в контексте $ORIGIN - элемента управления, определённого в параграфе 5.1 [RFC1035] как часть формата первичного файла. Например, если $ORIGIN имеет значение example.org., строка первичного файла для www фактически является записью для www.example.org..

Apex - вершина

Точка в дереве, где размещается владелец SOA и соответствующего полномочного NS RRset. Эта точка называется также вершиной зоны (zone apex). В [RFC4033] вершина определена как «имя на дочерней стороне среза зоны». Понятие вершины может быть полезно в теоретико-информационном описании структуры дерева, а понятие начала (origin) - как название той же концепции при реализации в файлах зоны. Однако это различие не всегда сохраняется на практике и можно найти примеры использования, противоречащие данному определению. В [RFC1034] используется термин «верхний узел зоны» в качестве синонима вершины, но этот термин не получил широкого распространения. В наши дни первое значение термина origin (см. выше) и термин apex часто используются как взаимозаменяемые.

Zone cut - срез зоны

Точка разграничения зон, где начало одной зоны является потомком другой. «Зоны ограничены «срезами». Каждый срез отделяет «дочернюю» зону (ниже среза) от «родительской» (выше среза)» (цитата из раздела 6 в [RFC2181], хотя это определение достаточно поверхностно). В параграфе 4.2 [RFC1034] вместо термина «срез зоны» используется просто срез (cut).

Delegation - передача полномочий (делегирование)

Процесс, в котором под вершиной данной зоны в пространстве имён создаётся отдельная зона. Передача полномочий происходит при добавлении в родительскую зону NS RRset для начала (origin) дочерней зоны. Делегирование всегда выполняется на срезе зоны. Термин часто является существительным[1] - новая зона создаётся актом передачи полномочий.

Authoritative data - полномочные данные

«Все записи RR, связанные со всеми узлами от вершины зоны до узлов ветвей или узлов над срезами на нижнем краю зоны» (цитата из параграфа 4.2.1 в [RFC1034]). Отметим, что это определение может приводить к непреднамеренному включению любых присутствующих в зоне записей NS, которые на деле не являются полномочными, поскольку идентичные NS RR имеются ниже среза зоны. В этом проявляется неоднозначность понятия полномочных данных, поскольку записи NS на родительской стороне полномочно указывают делегирование, хотя сами не являются полномочными.

В разделе 2 [RFC4033] даётся определение Authoritative RRset, которое связано с полномочными данными, но более точно.

Lame delegation - неудачное делегирование

«Неудачное делегирование имеет место, когда серверу имён переданы полномочия предоставлять службу имён для зоны (через записи NS), но тот не обслуживает имена для этой зоны (обычно из-за того, что он не настроен как первичный или вторичный сервер этой зоны). (цитата из параграфа 2.8 в [RFC1912]). Согласно другому определению, неудачное делегирование «… возникает, когда сервер имён указан в записях NS для некого домена, но на деле не является сервером имён для этого домена. Запросы в этом случае передаются серверам, которые ничего [!] не знают об интересующем домена (по меньшей мере не возвращают ожидаемого). Более того, иногда на этих узлах (если они существуют) даже нет серверов имён» (цитата из параграфа 2.3 в [RFC1713]).

Приведённые ранние определения не совпадают с современным использованием термина lame delegation, но единого мнения о том, что считать неудачным делегированием, ент. Термин применяется не только для указания приведённых выше случаев, но и для ряда других ошибок при передаче полномочий, которые ведут к отсутствию откликов или возврату неполномочных откликов:

- сервер имён с записью NS для зоны не отвечает на запросы DNS;
- сервер имён с адресом IP, недоступным распознавателю;
- сервер имён отвечает на запросы для определённого имени ошибкой или без бита полномочий.

Поскольку современное применение термина отличается от исходного определения, его следует считать устаревшим (историческим) и отказываться от него в пользу более чётких терминов.

[1] В английском языке. *Прим. перев.*

Glue records - склеивающие записи

«... записи [RR], которые не относятся к полномочным данным зоны и являются RR с адресами серверов имён. Эти RR требуются только в тех случаях, когда имя сервера [имён] находится «ниже» среза и используются только, как часть отклика со ссылкой». Без склеивающих записей «может возникнуть ситуация, когда NS RR скажут, что для получения адреса сервера имён следует обратиться к серверу имён, адрес которого мы хотим узнать» (цитата из параграфа 4.2.1 в [RFC1034]).

В соответствии с более поздним определением склеивающие записи - это «любые записи в файле зоны, которые не являются в полной мере частью данной зоны, включая имена серверов DNS делегированных субзон (записи NS), адресные записи, сопровождающие эти записи NS (A, AAAA и т. п.), а также любые другие «приблудившиеся» данные» (цитата из параграфа 5.4.1 в [RFC2181]). Хотя терми иногда используется сегодня в соответствии с этим расширенным определением, контекст определения в [RFC2181] позволяет предположить, что оно относится лишь к использованию термина в этом документе.

В записях NS имеется три типа отношений между владельцем записи, именем в NS RDATA и началом зоны: отсутствие связи, нахождение в домене (in-domain) и братский домен. Применение этих трёх типов к склеивающим записям описано в [RFC9471].

Отсутствие связи - это отношения, где NS RDATA содержит сервер имён, который не является подчиненным началу зоны и, следовательно, не является частью самой зоны.

Нахождение в домене (in-domain) - это отношения, где NS RDATA содержит сервер имён, чьё имя является подчинённым или (редко) совпадает с именем владельца записей NS. Например, передача полномочий для child.example.com может создавать сервер имён в домене (in-domain) ns.child.example.com.

Братские отношения имеются, когда NS RDATA NS RDATA содержит сервер имён, чьё имя является подчинённым или (редко) совпадает с началом зоны родителя, но не является подчиненным или совпадающим с с именем владельца записей NS. Например, передача полномочий для child.example.com в зоне example.com может создавать сервер имён братского домена ns.another.example.com.

Примеры типов передачи полномочий приведены в таблице 1.

Таблица 1.

Делегирование	***Родитель***	***Имя сервера имён***	***Тип***
com	.	a.gtld-servers.net	sibling domain
net	.	a.gtld-servers.net	in-domain
example.org	org	ns.example.org	in-domain
example.org	org	ns.ietf.org	sibling domain
example.org	org	ns.example.com	unrelated
example.jp	jp	ns.example.jp	in-domain
example.jp	jp	ns.example.ne.jp	sibling domain
example.jp	jp	ns.example.com	unrelated

Bailiwick - сфера компетенции

Модификаторы In-bailiwick и Out-of-bailiwick служат для описания отношений между зоной и обслуживающими её серверами имён. Отмечено, что определение термина bailiwick в словаре вызывает больше путаницы, чем приносит пользы. Эти термины следует считать историческими (устаревшими) по своей природе.

Root zone - корневая зона

Зона дерева на основе DNS, вершиной которой является пустая метка. Иногда называется корнем DNS (DNS root).

Empty non-terminals (ENTs) - пустые нетерминальные элементы

«Доменные имена, в которых нет записей о ресурсах, но имеются субдомены» (цитата из параграф 2.2.2 в [RFC4592]). Типичный пример е примеры в записях SRV - в имени _sip._tcp.example.com, домен _tcp.example.com, вероятно, не имеет RRset, но _sip._tcp.example.com имеет (по меньшей мере) SRV RRset.

Delegation-centric zone - ориентированная на передачу полномочий зона

Зона, состоящая в основном из передачи полномочий дочерним зонам. Это противоположность зоне, которая может включать делегирование дочерним зонам, но включает множество записей о ресурсах самой зоны и/или дочерних зон. Термин применяется в [RFC4956] и [RFC5155], но не определён ни в одном из них.

Occluded name - поглощённое имя

«Добавление точки делегирования через динамическое обновление будет переводить все подчинённые доменные имена в «подвешенное» состояние, когда они остаются частью зоны, но утрачивают доступность для поиска. Добавление записи DNAME даёт такой же эффект. Такие подчинённые имена называют поглощёнными (скрытыми)» (цитата из параграфа 3.5 в [RFC5936]).

Fast flux DNS - быстрая смена

Это «происходит, когда домен [найденный] в DNS использует записи A с несколькими адресами IP, имеющие очень короткий срок действия (Time-to-Live или TTL). Это означает, что домен распознаётся по разным адресам IP в течение короткого интервала времени» (цитата из параграфа 1.1.5 в [RFC6561] с исправлением опечаток). Помимо легитимных применений быструю смену можно использовать для доставки вредоносных программ. Поскольку адреса меняются быстро, сложно проверить все хосты. Следует отметить, что этот метод работает и с записями AAAA, но на момент создания этого документа такое использование редко наблюдалось в Internet.

Reverse DNS, reverse lookup - обратный (реверсный) поиск

«Процесс отображения адреса на имя обычно называется реверсным поиском (reverse lookup), а о зонах IN-ADDR.ARPA и IP6.ARPA говорят как об обратной системе DNS (reverse DNS)» (цитата из раздела 1 в [RFC5855]).

Forward lookup - прямой поиск

«Трансляция имени хоста в адрес» (цитата из раздела 6 в [RFC3493]).

arpa (Address and Routing Parameter Area Domain) - домен arpa

«Домен arpa был создан как часть исходного развёртывания DNS для предоставления механизма перехода от таблиц хостов (Host Table), применяемых в сети ARPANET, а также в качестве домена для реверсного отображения адресов IPv4. В 2000 г. аббревиатура была переименована в Address and Routing Parameter Area (область адресов и параметров маршрутизации) в надежде снизить путаницу с названием сети» (цитата из раздела 2 в [RFC3172]). Домен .arpa является «инфраструктурным», (ролью которого является поддержка операционной инфраструктуры Internet» (цитата из раздела 2 в [RFC3172]). История имени описана в [RFC3172].

Service name - имя службы

«Имена служб являются уникальными ключами реестра Service Name and Transport Protocol Port Number. Это уникальные символьные имена служб, которые могут использоваться для других целей, например, в записях DNS SRV» (цитата из раздела 5 в [RFC6335]).

8. Шаблоны

Wildcard - шаблон

В [RFC1034] термин wildcard (шаблон) определён так, что это оказалось непонятным для внедряющих протокол. Расширенное обсуждение шаблонов, включая более чёткие определения, приведено в [RFC4592]. Особое внимание уделено RR, в которых имя владельца начинается с метки *. «Такие RR называют шаблонами. Шаблонные RR можно представлять, как инструкцию по синтезированию RR» (цитата из параграфа 4.3.3 в [RFC1034])

Asterisk label - метка *

«Первый октет - это обычный тип и размер 1-октетной метки, а второй содержит код ASCII [RFC20] для символа *. Описательным именем для такой метки является «звёздочка» (цитата из параграфа 2.1.1 в [RFC4592]).

Wildcard domain name - шаблонное доменное имя

«Шаблонное имя домена определяется наличием в его начале (левые или младшие символы) метки с двоичным представлением 0000 0001 0010 1010 = 0x01 0x2a (шестнадцатеричное)» (цитата из параграфа 2.1.1 в [RFC4592]). Второй октет этой метки является кодом ASCII для символа *.

Closest encloser - ближайшее включающее [имя]

«Самый длинный предок имени» (цитата из параграфа 1.3 в [RFC5155]). Прежним определением было: «Узел в дереве зоны имеющихся доменных имён, в котором наибольшее число меток соответствует имени в запросе (последовательно вниз от корневой метки). Каждое совпадение является совпадением метки и порядок меток одинаков» (цитата из параграфа 3.3.1 в [RFC4592]).

Closest provable encloser- ближайшее подтверждённое включающее [имя]

«Самый длинный предок имени, наличие которого может быть доказано. Отметим, что это имя отличается от ближайшего включающего имени в зоне Opt-Out» (цитата из параграфа 1.3 в [RFC5155]). Определение opt-out дано в разделе 10.

Next closer name - имя вслед за включающим

«Имя, которое на 1 метку длиннее ближайшего подтверждённого включающего имени (closest provable encloser)» (цитата из параграфа 1.3 в [RFC5155]).

Source of Synthesis - источник синтезирования

«Источник синтеза определяется в контексте процесса запроса как шаблонное доменное имя, непосредственно порождаемое (descending) ближайшим включающим именем (closest encloser), при условии существования такого шаблонного имени. Непосредственно порождаемое означает, что источник источник синтезирования имеет форму <asterisk label>.<closest encloser>» (цитата из параграфа 3.3.1 в [RFC4592]).

9. Модель регистрации

Registry - реестр

Внесение в реестр - это административная операция в зоне, позволяющая зарегистрировать имена из этой зоны. Этот термин часто применяется к организациям к организациям, регистрирующим большие зоны, ориентированные на передачу полномочий (такие как TLD), но формально реестром зоны является тот, кто определяет включаемые в зону данные. Это определение реестра представлено с точки зрения DNS и для некоторых зон правила выбора содержимого зоны определяются вышестоящими зонами, а не оператором реестра.

Registrant - регистрирующий

Организация или человек, от имени которого зона регистрируется в реестре. Во многих случаях реестр (registry) и регистрирующий (registrant) могут быть одним лицом, но для TLD это часто не так.

Registrar - регистратор

Поставщик услуг, выступающий посредником между регистрирующим лицом и реестром. Регистратор требуется не для всех регистраций, хотя регистраторы обычно участвуют в регистрации TLD.

EPP

Расширяемый протокол обеспечения (Extensible Provisioning Protocol или EPP), обычно применяемый для передачи регистрационных сведений между реестром и регистрирующим. Протокол EPP определён в [RFC5730].

WHOIS

Протокол, заданный в [RFC3912] и часто применяемый для запроса к базам данных реестров. Данные WHOIS часто применяются для связывания данных регистрации (таких, как контакты управляющих зоной лиц) с доменными именами. Термин «данные WHOIS» часто служит синонимом базы данных реестра, хотя сама база может обслуживаться другими протоколами, в частности, RDAP. Протокол WHOIS применяется также для работы с данными реестров адресов IP.

RDAP

Протокол доступа к данным регистрации (Registration Data Access Protocol), заданный в [RFC7480], [RFC7481], [RFC7485], [RFC9082], [RFC9083] и [RFC9224]. Протокол и формат данных RDAP предназначены для замены WHOIS.

DNS operator - оператор DNS

Сторона, отвечающая за работу серверов DNS. Для полномочных серверов зоны оператором DNS может служить регистрирующая зону сторона (registrant), регистратор, выступающий от её имени, или сторонний оператор. Для некоторых зон функции реестра выполняет оператор DNS вместе со сторонами, определяющими содержимое зоны.

Public suffix - суффикс общего пользования

«Домен, контролируемый публичным регистратором» (цитата из параграфа 5.3 в [RFC6265]). Общепринятым толкованием этого термина является домен, в котором третьи лица могут регистрировать свои субдомены, а HTTP cookie (см. [RFC6265]) не следует устанавливать. В доменном имени нет сведений, является ли имя публичным суффиксом и определить это можно лишь внешними средствами. Фактически общедоступными суффиксами может быть как домен, так и его субдомены. Одним из ресурсов для нахождения публичных суффиксов является список (Public Suffix List или PSL), поддерживаемых компанией Mozilla <https://publicsuffix.org/>. Например, в момент создания этого документа домен com.au был указан в PSL как общедоступный суффикс (отметим, что впредь это может измениться).

Отметим, что термин public suffix по многим причинам вызывает разногласия в сообществе DNS и в будущем может быть существенно изменён. Одним из примеров сложностей отнесения домена к суффиксам общего пользования является то, что обозначение может меняться по мере изменения правил регистрации в зоне, как в случае домена uk (TLD) в 2014 г.

Subordinate и Superordinate - подчинённый и вышестоящий

Эти термины применяются в [RFC5731] для модели регистрации, но не определены там. Вместо этого они приведены в примерах: «Например, доменное имя example.com является вышестоящим для имени хоста ns1.example.com... Например, имя хоста ns1.example1.com является подчиненным для домена example1.com, но не является таковым для example2.com» (цитата из параграфа 1.1 в [RFC5731]). Эти термины указывают строгие способы обозначения отношений между доменами, когда один является субдоменом другого.

10. Базовые термины DNSSEC

Большинство терминов DNSSEC определено в [RFC4033], [RFC4034], [RFC4035] и [RFC5155]. Здесь выделены термины, вызывающие путаницу в сообществе DNS.

DNSSEC-aware и DNSSEC-unaware - с поддержкой или без поддержки DNSSEC

Эти два термина используются в некоторых RFC, но не определены формально. Однако в разделе 2 [RFC4033] определены многие типы распознавателей и валидаторов, включая «не проверяющий достоверность защищённый оконечный распознаватель» (non-validating security-aware stub resolver), «не проверяющий корректность оконечный распознаватель» (non-validating stub resolver), «защищённый сервер имён» (security-aware name server), «защищённый рекурсивный сервер имён» (security-aware recursive name server), «защищённый распознаватель» (security-aware resolver), «защищённый оконечный распознаватель» (security-aware stub resolver), «обычное <нечто>» (security-oblivious 'anything'). Отметим, что термин «проверяющий распознаватель» (validating resolver), используемый в связанных с DNSSEC документах также не определён в указанных RFC, но определён ниже.

Signed zone - подписанная зона

«Зона с подписанными наборами RRset, содержащая корректно созданный ключ DNSKEY, подпись RRSIG, записи NSEC и (необязательно) DS» (цитата из раздела 2 в [RFC4033]). В другом контексте отмечалось, что сама зона фактически не подписывается, но все соответствующие RRset в зоне подписываются. Тем не менее, если зона, которую следует подписывать, содержит какие-либо не подписанные (или отклонённые) RRset, эти наборы будут считаться фиктивными, поэтому вся зона должна обслуживаться каким-либо способом.

Следует также отметить, что с момента публикации [RFC6840], записи NSEC больше не требуются для подписанных зон и вместо них подписанная зона может включать записи NSEC3. В [RFC7129] представлен дополнительный справочный комментарий и некоторый контекст для механизмов NSEC и NSEC3, используемых в DNSSEC для предоставления аутентифицированных откликов о несуществовании (denial-of-existence). NSEC и NSEC3 описаны ниже.

Online signing - подписание по запросам

В [RFC4470] определён термин on-line signing (через дефис) как: «генерация и подписывание этих записей по запросу», где «эти» относится к записям NSEC. Текущее определение расширено включением генерации и подписывания по запросам записей RRSIG, NSEC и NSEC3.

Unsigned zone - неподписанная зона

В разделе 2 [RFC4033] указано, что это «зона, не имеющая подписи». В разделе 2 [RFC4035] указано: «Зона, не включающая записи [корректно созданные записи DNSKEY, RRSIG, NSEC и (не обязательно) DS] в соответствии с указанными правилами, является неподписанной». Важно подчеркнуть, что в конце параграфа 5.2 [RFC4035] указана дополнительная ситуация, когда зона считается неподписанной: «Если распознаватель не поддерживает ни одного алгоритма, указанного в DS RRset, он не сможет проверить путь аутентификации к дочерней зоне. В таких случаях распознавателю **следует** трактовать дочернюю зону, как неподписанную».

NSEC

«Запись NSEC позволяет защищённому распознавателю аутентифицировать негативный отклик в случаях отсутствия имени или типа с использованием того же механизма, который применяется при аутентификации других откликов DNS» (цитата из параграфа 3.2 в [RFC4033]). Короче говоря, запись NSEC предоставляет аутентифицированные сведения о несуществовании.

«Запись NSEC содержит два отдельных элемента - имя следующего владельца (в каноническом порядке для зоны), содержащего полномочные данные, или точка передачи полномочий (делегирования) NS RRset и множество типов RR, присутствующих в имени владельца NSEC RR» (цитата из раздела 4 в [RFC4034]).

NSEC3

Подобно NSEC, запись NSEC3 предоставляет аутентифицированные сведения о несуществовании, однако записи NSEC3 смягчают перечисление зоны и поддерживают Opt-Out. Записи NSEC3 требуют связанных записей о ресурсах NSEC3PARAM. Записи NSEC3 и NSEC3PARAM определены в [RFC5155].

Отметим, что в [RFC6840] сказано, что [RFC5155] «в настоящее время считается частью семейства документов DNS Security, как указано в разделе 10 [RFC4033]». Это означает, что некоторые определения из прежних RFC, где говорится только о записях NSEC, вероятно, следует считать относящимися как к NSEC, так и к NSEC3.

Opt-out

«Флаг Opt-Out указывает, что NSEC3 RR может охватывать неподписанное делегирование» (цитата из параграфа 3.1.2.1 в [RFC5155]). Opt-Out решает проблему высоких затрат на защиту делегирования в незащищённую зону. При использовании Opt-Out имена, являющиеся незащищённым делегированием и пустые нетерминальные элементы, выводимое только из незащищённого делегирования) не требуют записи NSEC3 или соответствующих записей RRSIG. Записи Opt-Out NSEC3 не могут подтверждать или опровергать наличие незащищённого делегирования (взято из параграфа 5.1 в [RFC7129]).

Insecure delegation - незащищённая передача полномочий

«Подписанное имя, содержащее делегирование (NS RRset), но не имеющее DS RRset, что означает передачу полномочий в неподписанную субзону (цитата из раздела 2 в [RFC4956]).

Zone enumeration - перечисление зоны

«Практика выявления полного содержимого зоны с помощью последовательных запросов» (цитата из параграфа 1.3 в [RFC5155]). Иногда применяется термин zone walking (прохождение по зоне). Перечисление зоны отличается от предсказывания содержимого зоны - при предсказывании используется большой словарь возможных меток и передаются последовательные запросы для них или сопоставляет содержимое записей NSEC3 с таким словарём.

Validation - проверка

Проверкой в контексте DNSSEC считается одно из указанных ниже действий.

- Проверка достоверности подписей DNSSEC.
- Проверка достоверности откликов DNS, в том числе аутентифицированных сведений о несуществовании.
- Создание цепочки аутентификации от привязки доверия до отклика DNS или отдельных DNS RRset в нем.

В двух первых определениях рассматривается лишь достоверность отдельных компонентов DNSSEC, таких как RRSIG и доказательства NSEC. Третье определение учитывает всю цепочку проверки подлинности DNSSEC и распознаватель «должен быть настроен так, чтобы он знал хотя бы одну аутентифицированную запись DNSKEY или DS» (цитата из раздела 5 в [RFC4035]).

В разделе 2 [RFC4033] сказано, что «проверяющий достоверность защищённый оконечный распознаватель ... выполняет проверку достоверности подписи» и использует привязку доверия «как стартовую точку для создания цепочки аутентификации к подписанному отклику DNS». Таким образом, используются первое и третье определение. Процесс проверки достоверности записей RRSIG описана в параграфе 5.3 [RFC4035].

В [RFC5155] проверка достоверности откликов упоминается в контексте хэшированных аутентифицированных откликов о несуществовании, где применяется второе определение.

Термин аутентификация используется как взаимозаменяемый с проверкой достоверности в смысле третьего определения. В разделе 2 [RFC4033] описана цепочка, связывающая привязку доверия с данными DNS, как цепочка аутентификации (authentication chain). Отклик считается подлинным, если «все RRset в разделах Answer и Authority [проверены] на предмет аутентичности» (цитата из [RFC4035]). Данные DNS и отклики, сочтённые подлинными или достоверными, имеют статус безопасности secure (параграф 4.3 в [RFC4035] и раздел 5 в [RFC4033]). «Последнее слово при анализе аутентификации для ключей и данных DNS остаётся за локальной политикой, которая может расширить или переназначить расширения протокола [DNSSEC]» (цитата из параграфа 3.1 в [RFC4033]).

При использовании термина проверка (verification) он обычно является синонимом проверки достоверности.

Validating resolver - проверяющий распознаватель

Поддерживающий защиту рекурсивный распознаватель или распознаватель-заглушка, применяющий хотя бы одно из приведённых выше определений проверки достоверности в соответствии с контекстом распознавания. Трактовка термина не всегда однозначна и зависит от контекста, как и для базового термина resolver (см. раздел 6).

Key signing key (KSK) - ключ подписания ключей

Ключ DNSSEC, «подписывающий только DNSKEY RRset на вершине зоны» (цитата из параграфа 3.1 в [RFC6781]).

Zone signing key (ZSK) - ключ подписания зоны

«Ключ DNSSEC, который может применяться для подписания всех RRset в зоне, для которых требуется подпись, за исключением DNSKEY RRset на вершине» (цитата из параграфа 3.1 в [RFC6781]). Отметим, что иногда ZSK применяется и для подписания DNSKEY RRset на вершине.

Combined signing key (CSK) - комбинированный ключ подписания

«В случаях, когда различия между KSK и ZSK не проводится, т. е. каждый может играть обе роли, говорят о схеме однотипного подписания (Single-Type Signing Scheme)» (цитата из параграфа 3.1 в [RFC6781]). Иногда применяется термин «комбинированный ключ подписания» (combined signing key или CSK). Применение определённого ключа ZSK, KSK или CSK определяет практика работы, а не протокол.

Secure Entry Point (SEP) - защищённая точка входа

Флаг в DNSKEY RDATA, который «можно использовать для различения ключей, предназначенных служить защищёнными точками входа в зону при создании цепочек доверия, т. е. на них (должны) будут указывать родительские DS RR или они будут заданы как привязки доверия. ... Поэтому предполагается устанавливать флаг SEP для ключей, применяемых как KSK, но не для ключей, служащих ZSK, хотя в тех случаях, когда эти ключи не различаются (Single-Type Signing Scheme), предлагается устанавливать флаг SEP для всех ключей» (цитата из параграфа 3.2.3 в [RFC6781]). Отметим, что флаг SEP служит лишь подсказкой и его наличие или отсутствие не может применяться для дисквалификации применения DNSKEY RR в качестве KSK или ZSK при проверке достоверности.

Исходное определение SEP дано в [RFC3757] и чётко указывает, что SEP является ключом, а не просто битом в ключе. В аннотации к [RFC3757] сказано: «С помощью записи DS RR (Delegation Signer) была введена концепция открытого ключа, служащего защищённой точкой входа (secure entry point или SEP). В процессе обмена открытыми ключами с родителем возникает необходимость отличать ключи SEP от других открытых ключей в наборе записей DNSKEY (Domain Name System KEY). Бит флага в DNSKEY RR определён для индикации того, что DNSKEY применяется как SEP». Определение SEP как ключа было отменено в [RFC4034], а определение [RFC6781] согласуется с определением [RFC4034].

Trust anchor - привязка доверия

«Сконфигурированная запись DNSKEY RR или хэш DS RR записи DNSKEY RR. Проверяющий защищённый оконечный распознаватель использует этот открытый ключ или хэш а качестве стартовой точки для построения аутентификационной цепочки отклика DNS. В общем случае проверяющий распознаватель будет получать начальные значения таких привязок с помощью того или иного защищённого или доверенного способа, не входящего в протокол DNS.» (цитата из раздела 2 в [RFC4033].

DNSSEC Policy (DP) - правила (политика) DNSSEC

Заявление, которое «устанавливает требования и стандарты безопасности для реализации в зоне, подписанной DNSSEC» (цитата из раздела 2 в [RFC6841]).

DNSSEC Practice Statement (DPS) - заявление о практике DNSSEC

«Раскрывающий практику документ, который может поддерживать и дополнять правила DNSSEC (при наличии) и в котором говорится, как в управлении данной зоной реализованы процедуры и элементы управления на высоком уровне» (цитата из раздела 2 в [RFC6841]).

Hardware security module (HSM) - аппаратный модуль защиты

Специальное аппаратное средство, служащее для создания ключей подписи и подписания сообщений без раскрытия секретного ключа. В DNSSEC модули HSM часто применяются для хранения секретных ключей для KSK и ZSK, а также для создания подписей, используемых в записях RRSIG с периодическими интервалами.

Signing software - программы для подписания

Полномочные серверы DNS, поддерживающие DNSSEC, часто включают программы, облегчающие создание и поддержку в зонах подписей DNSSEC. Имеются также автономные программы, которые можно применять для подписи зоны независимо от поддержки подписей самим полномочным сервером. Иногда программы для подписи могут поддерживать определённые модули HSM.

11. Состояния DNSSEC

Проверяющий достоверность распознаватель может определить, что отклик имеет одно из четырёх состояний - secure, insecure, bogus, indeterminate. Эти состояния определены в [RFC4033] и [RFC4035], хотя определения в этих

документах несколько различаются. Здесь не предпринимается попытки согласовать эти определения и не высказывается мнения о необходимости такого согласования.

В разделе 5 [RFC4033] сказано:

> Проверяющий распознаватель может определять 4 перечисленных ниже состояния.
>
> ***Secure - защищённое***
> Проверяющий распознаватель имеет доверенную привязку или цепочку доверия или способен проверить все подписи в отклике.
> ***Insecure - незащищённое***
> Проверяющий распознаватель имеет доверенную привязку или цепочку доверия и (в некой точке делегирования) подписанное подтверждение отсутствия записи DS. Это показывает, что последующие ветви дерева могут оказаться незащищёнными. Проверяющий распознаватель может иметь локальное правило для маркировки части доменного пространства, как незащищённой.
> ***Bogus - подделка***
> Проверяющий распознаватель имеет доверенную привязку и защищённое делегирование, показывающие, что дополнительные данные подписаны, но проверка отклика по той или иной причине дала отрицательный результат (отсутствие подписи, просроченная подпись, отсутствие данных, которые должны присутствовать в соответствующей NSEC RR и т. п.).
> ***Indeterminate - неопределённое***
> Нет доверенной привязки, которая показывает, что определённая часть дерева защищена. Это состояние принимается по умолчанию.

В параграфе 4.3 [RFC4035] сказано:

> Защищённый распознаватель **должен** быть способен должен различать перечисленные ниже случаи.
>
> ***Защищённый (Secure)***
> RRset, для которого распознаватель способен построить цепочку подписанных записей DNSKEY и DS RR от доверенной защитной привязки (security anchor) до RRset. В этом случае набору RRset следует быть подписанным и для него выполняется проверка подписи, описанная выше.
> ***Незащищённый (Insecure)***
> RRset, для которого распознаватель знает об отсутствии цепочки подписанных записей DNSKEY и DS RR от любой доверенной стартовой точки до RRset. Это может наблюдаться в тех случаях, когда целевой набор RRset находится в неподписанной зоне или потомке такой зоны. В этом случае набор RRset может быть как подписанным, так и неподписанным и распознаватель не сможет проверить подпись.
> ***Подделка (Bogus)***
> RRset, для которого распознаватель предполагает возможность установить цепочку доверия, но не может сделать этого по причине того или иного отказа при проверке подписи или отсутствия данных, наличие которых указывают имеющие отношение к делу записи DNSSEC RR. Это может говорить об атаке, ошибке в конфигурации или повреждении данных.
> ***Неопределённость (Indeterminate)***
> RRset, для которого распознаватель не может определить необходимость наличия подписи по причине невозможности получить требуемые записи DNSSEC RR. Это может происходить в тех случаях, когда распознаватель не может контактировать с осведомленными о защите серверами имен для соответствующих зон.

12. Вопросы безопасности

Приведённые здесь определения не меняют соображений безопасности для глобальных и приватных систем DNS.

13. Взаимодействие с IANA

Ссылки на RFC 8499 в реестрах IANA заменены ссылками на этот документ.

14. Литература

14.1. Нормативные документы

[IANA_RootFiles] IANA, "Root Files", <https://www.iana.org/domains/root/files>.

[RFC0882] Mockapetris, P., "Domain names: Concepts and facilities", RFC 882, DOI 10.17487/RFC0882, November 1983, <https://www.rfc-editor.org/info/rfc882>.

[RFC1034] Mockapetris, P., "Domain names - concepts and facilities", STD 13, RFC 1034, DOI 10.17487/RFC1034, November 1987, <https://www.rfc-editor.org/info/rfc1034>.

[RFC1035] Mockapetris, P., "Domain names - implementation and specification", STD 13, RFC 1035, DOI 10.17487/RFC1035, November 1987, <https://www.rfc-editor.org/info/rfc1035>.

[RFC1123] Braden, R., Ed., "Requirements for Internet Hosts - Application and Support", STD 3, RFC 1123, DOI 10.17487/RFC1123, October 1989, <https://www.rfc-editor.org/info/rfc1123>.

[RFC1912] Barr, D., "Common DNS Operational and Configuration Errors", RFC 1912, DOI 10.17487/RFC1912, February 1996, <https://www.rfc-editor.org/info/rfc1912>.

[RFC1996] Vixie, P., "A Mechanism for Prompt Notification of Zone Changes (DNS NOTIFY)", RFC 1996, DOI 10.17487/RFC1996, August 1996, <https://www.rfc-editor.org/info/rfc1996>.

[RFC2136] Vixie, P., Ed., Thomson, S., Rekhter, Y., and J. Bound, "Dynamic Updates in the Domain Name System (DNS UPDATE)", RFC 2136, DOI 10.17487/RFC2136, April 1997, <https://www.rfc-editor.org/info/rfc2136>.

[RFC2181] Elz, R. and R. Bush, "Clarifications to the DNS Specification", RFC 2181, DOI 10.17487/RFC2181, July 1997, <https://www.rfc-editor.org/info/rfc2181>.

[RFC2182] Elz, R., Bush, R., Bradner, S., and M. Patton, "Selection and Operation of Secondary DNS Servers", BCP 16, RFC 2182, DOI 10.17487/RFC2182, July 1997, <https://www.rfc-editor.org/info/rfc2182>.

[RFC2308] Andrews, M., "Negative Caching of DNS Queries (DNS NCACHE)", RFC 2308, DOI 10.17487/RFC2308, March 1998, <https://www.rfc-editor.org/info/rfc2308>.

[RFC4033] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "DNS Security Introduction and Requirements", RFC 4033, DOI 10.17487/RFC4033, March 2005, <https://www.rfc-editor.org/info/rfc4033>.

[RFC4034] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Resource Records for the DNS Security Extensions", RFC 4034, DOI 10.17487/RFC4034, March 2005, <https://www.rfc-editor.org/info/rfc4034>.

[RFC4035] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Protocol Modifications for the DNS Security Extensions", RFC 4035, DOI 10.17487/RFC4035, March 2005, <https://www.rfc-editor.org/info/rfc4035>.

[RFC4592] Lewis, E., "The Role of Wildcards in the Domain Name System", RFC 4592, DOI 10.17487/RFC4592, July 2006, <https://www.rfc-editor.org/info/rfc4592>.

[RFC5155] Laurie, B., Sisson, G., Arends, R., and D. Blacka, "DNS Security (DNSSEC) Hashed Authenticated Denial of Existence", RFC 5155, DOI 10.17487/RFC5155, March 2008, <https://www.rfc-editor.org/info/rfc5155>.

[RFC5358] Damas, J. and F. Neves, "Preventing Use of Recursive Nameservers in Reflector Attacks", BCP 140, RFC 5358, DOI 10.17487/RFC5358, October 2008, <https://www.rfc-editor.org/info/rfc5358>.

[RFC5730] Hollenbeck, S., "Extensible Provisioning Protocol (EPP)", STD 69, RFC 5730, DOI 10.17487/RFC5730, August 2009, <https://www.rfc-editor.org/info/rfc5730>.

[RFC5731] Hollenbeck, S., "Extensible Provisioning Protocol (EPP) Domain Name Mapping", STD 69, RFC 5731, DOI 10.17487/RFC5731, August 2009, <https://www.rfc-editor.org/info/rfc5731>.

[RFC5855] Abley, J. and T. Manderson, "Nameservers for IPv4 and IPv6 Reverse Zones", BCP 155, RFC 5855, DOI 10.17487/RFC5855, May 2010, <https://www.rfc-editor.org/info/rfc5855>.

[RFC5936] Lewis, E. and A. Hoenes, Ed., "DNS Zone Transfer Protocol (AXFR)", RFC 5936, DOI 10.17487/RFC5936, June 2010, <https://www.rfc-editor.org/info/rfc5936>.

[RFC6561] Livingood, J., Mody, N., and M. O'Reirdan, "Recommendations for the Remediation of Bots in ISP Networks", RFC 6561, DOI 10.17487/RFC6561, March 2012, <https://www.rfc-editor.org/info/rfc6561>.

[RFC6781] Kolkman, O., Mekking, W., and R. Gieben, "DNSSEC Operational Practices, Version 2", RFC 6781, DOI 10.17487/RFC6781, December 2012, <https://www.rfc-editor.org/info/rfc6781>.

[RFC6840] Weiler, S., Ed. and D. Blacka, Ed., "Clarifications and Implementation Notes for DNS Security (DNSSEC)", RFC 6840, DOI 10.17487/RFC6840, February 2013, <https://www.rfc-editor.org/info/rfc6840>.

[RFC6841] Ljunggren, F., Eklund Lowinder, AM., and T. Okubo, "A Framework for DNSSEC Policies and DNSSEC Practice Statements", RFC 6841, DOI 10.17487/RFC6841, January 2013, <https://www.rfc-editor.org/info/rfc6841>.

[RFC6891] Damas, J., Graff, M., and P. Vixie, "Extension Mechanisms for DNS (EDNS(0))", STD 75, RFC 6891, DOI 10.17487/RFC6891, April 2013, <https://www.rfc-editor.org/info/rfc6891>.

[RFC7344] Kumari, W., Gudmundsson, O., and G. Barwood, "Automating DNSSEC Delegation Trust Maintenance", RFC 7344, DOI 10.17487/RFC7344, September 2014, <https://www.rfc-editor.org/info/rfc7344>.

[RFC7719] Hoffman, P., Sullivan, A., and K. Fujiwara, "DNS Terminology", RFC 7719, DOI 10.17487/RFC7719, December 2015, <https://www.rfc-editor.org/info/rfc7719>.

[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>.

[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>.

[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>.

[RFC9471] Andrews, M., Huque, S., Wouters, P., and D. Wessels, "DNS Glue Requirements in Referral Responses", RFC 9471, DOI 10.17487/RFC9471, September 2023, <https://www.rfc-editor.org/info/rfc9471>.

14.2. Дополнительная литература

[IANA_Resource_Registry] IANA, "Resource Record (RR) TYPEs", <https://www.iana.org/assignments/dns-parameters/>.

[RFC20] Cerf, V., "ASCII format for network interchange", STD 80, RFC 20, DOI 10.17487/RFC0020, October 1969, <https://www.rfc-editor.org/info/rfc20>.

[RFC819] Su, Z. and J. Postel, "The Domain Naming Convention for Internet User Applications", RFC 819, DOI 10.17487/RFC0819, August 1982, <https://www.rfc-editor.org/info/rfc819>.

[RFC952] Harrenstien, K., Stahl, M., and E. Feinler, "DoD Internet host table specification", RFC 952, DOI 10.17487/RFC0952, October 1985, <https://www.rfc-editor.org/info/rfc952>.

[RFC1713] Romao, A., "Tools for DNS debugging", FYI 27, RFC 1713, DOI 10.17487/RFC1713, November 1994, <https://www.rfc-editor.org/info/rfc1713>.

[RFC1995] Ohta, M., "Incremental Zone Transfer in DNS", RFC 1995, DOI 10.17487/RFC1995, August 1996, <https://www.rfc-editor.org/info/rfc1995>.

[RFC2775] Carpenter, B., "Internet Transparency", RFC 2775, DOI 10.17487/RFC2775, February 2000, <https://www.rfc-editor.org/info/rfc2775>.

[RFC3172] Huston, G., Ed., "Management Guidelines & Operational Requirements for the Address and Routing Parameter Area Domain ("arpa")", BCP 52, RFC 3172, DOI 10.17487/RFC3172, September 2001, <https://www.rfc-editor.org/info/rfc3172>.

[RFC3425] Lawrence, D., "Obsoleting IQUERY", RFC 3425, DOI 10.17487/RFC3425, November 2002, <https://www.rfc-editor.org/info/rfc3425>.

[RFC3493] Gilligan, R., Thomson, S., Bound, J., McCann, J., and W. Stevens, "Basic Socket Interface Extensions for IPv6", RFC 3493, DOI 10.17487/RFC3493, February 2003, <https://www.rfc-editor.org/info/rfc3493>.

[RFC3757] Kolkman, O., Schlyter, J., and E. Lewis, "Domain Name System KEY (DNSKEY) Resource Record (RR) Secure Entry Point (SEP) Flag", RFC 3757, DOI 10.17487/RFC3757, April 2004, <https://www.rfc-editor.org/info/rfc3757>.

[RFC3912] Daigle, L., "WHOIS Protocol Specification", RFC 3912, DOI 10.17487/RFC3912, September 2004, <https://www.rfc-editor.org/info/rfc3912>.

[RFC4470] Weiler, S. and J. Ihren, "Minimally Covering NSEC Records and DNSSEC On-line Signing", RFC 4470, DOI 10.17487/RFC4470, April 2006, <https://www.rfc-editor.org/info/rfc4470>.

[RFC4641] Kolkman, O. and R. Gieben, "DNSSEC Operational Practices", RFC 4641, DOI 10.17487/RFC4641, September 2006, <https://www.rfc-editor.org/info/rfc4641>.

[RFC4697] Larson, M. and P. Barber, "Observed DNS Resolution Misbehavior", BCP 123, RFC 4697, DOI 10.17487/RFC4697, October 2006, <https://www.rfc-editor.org/info/rfc4697>.

[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>.

[RFC4956] Arends, R., Kosters, M., and D. Blacka, "DNS Security (DNSSEC) Opt-In", RFC 4956, DOI 10.17487/RFC4956, July 2007, <https://www.rfc-editor.org/info/rfc4956>.

[RFC5625] Bellis, R., "DNS Proxy Implementation Guidelines", BCP 152, RFC 5625, DOI 10.17487/RFC5625, August 2009, <https://www.rfc-editor.org/info/rfc5625>.

[RFC5890] Klensin, J., "Internationalized Domain Names for Applications (IDNA): Definitions and Document Framework", RFC 5890, DOI 10.17487/RFC5890, August 2010, <https://www.rfc-editor.org/info/rfc5890>.

[RFC5891] Klensin, J., "Internationalized Domain Names in Applications (IDNA): Protocol", RFC 5891, DOI 10.17487/RFC5891, August 2010, <https://www.rfc-editor.org/info/rfc5891>.

[RFC5892] Faltstrom, P., Ed., "The Unicode Code Points and Internationalized Domain Names for Applications (IDNA)", RFC 5892, DOI 10.17487/RFC5892, August 2010, <https://www.rfc-editor.org/info/rfc5892>.

[RFC5893] Alvestrand, H., Ed. and C. Karp, "Right-to-Left Scripts for Internationalized Domain Names for Applications (IDNA)", RFC 5893, DOI 10.17487/RFC5893, August 2010, <https://www.rfc-editor.org/info/rfc5893>.

[RFC5894] Klensin, J., "Internationalized Domain Names for Applications (IDNA): Background, Explanation, and Rationale", RFC 5894, DOI 10.17487/RFC5894, August 2010, <https://www.rfc-editor.org/info/rfc5894>.

[RFC6055] Thaler, D., Klensin, J., and S. Cheshire, "IAB Thoughts on Encodings for Internationalized Domain Names", RFC 6055, DOI 10.17487/RFC6055, February 2011, <https://www.rfc-editor.org/info/rfc6055>.

[RFC6265] Barth, A., "HTTP State Management Mechanism", RFC 6265, DOI 10.17487/RFC6265, April 2011, <https://www.rfc-editor.org/info/rfc6265>.

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

[RFC6335] Cotton, M., Eggert, L., Touch, J., Westerlund, M., and S. Cheshire, "Internet Assigned Numbers Authority (IANA) Procedures for the Management of the Service Name and Transport Protocol Port Number Registry", BCP 165, RFC 6335, DOI 10.17487/RFC6335, August 2011, <https://www.rfc-editor.org/info/rfc6335>.

[RFC6365] Hoffman, P. and J. Klensin, "Terminology Used in Internationalization in the IETF", BCP 166, RFC 6365, DOI 10.17487/RFC6365, September 2011, <https://www.rfc-editor.org/info/rfc6365>.

[RFC6672] Rose, S. and W. Wijngaards, "DNAME Redirection in the DNS", RFC 6672, DOI 10.17487/RFC6672, June 2012, <https://www.rfc-editor.org/info/rfc6672>.

[RFC6762] Cheshire, S. and M. Krochmal, "Multicast DNS", RFC 6762, DOI 10.17487/RFC6762, February 2013, <https://www.rfc-editor.org/info/rfc6762>.

[RFC7129] Gieben, R. and W. Mekking, "Authenticated Denial of Existence in the DNS", RFC 7129, DOI 10.17487/RFC7129, February 2014, <https://www.rfc-editor.org/info/rfc7129>.

[RFC7480] Newton, A., Ellacott, B., and N. Kong, "HTTP Usage in the Registration Data Access Protocol (RDAP)", STD 95, RFC 7480, DOI 10.17487/RFC7480, March 2015, <https://www.rfc-editor.org/info/rfc7480>.

[RFC7481] Hollenbeck, S. and N. Kong, "Security Services for the Registration Data Access Protocol (RDAP)", STD 95, RFC 7481, DOI 10.17487/RFC7481, March 2015, <https://www.rfc-editor.org/info/rfc7481>.

[RFC9082] Hollenbeck, S. and A. Newton, "Registration Data Access Protocol (RDAP) Query Format", STD 95, RFC 9082, DOI 10.17487/RFC9082, June 2021, <https://www.rfc-editor.org/info/rfc9082>.

[RFC9083] Hollenbeck, S. and A. Newton, "JSON Responses for the Registration Data Access Protocol (RDAP)", STD 95, RFC 9083, DOI 10.17487/RFC9083, June 2021, <https://www.rfc-editor.org/info/rfc9083>.

[RFC9224] Blanchet, M., "Finding the Authoritative Registration Data Access Protocol (RDAP) Service", STD 95, RFC 9224, DOI 10.17487/RFC9224, March 2022, <https://www.rfc-editor.org/info/rfc9224>.

[RFC7485] Zhou, L., Kong, N., Shen, S., Sheng, S., and A. Servin, "Inventory and Analysis of WHOIS Registration Objects", RFC 7485, DOI 10.17487/RFC7485, March 2015, <https://www.rfc-editor.org/info/rfc7485>.

[RFC7793] Andrews, M., "Adding 100.64.0.0/10 Prefixes to the IPv4 Locally-Served DNS Zones Registry", BCP 163, RFC 7793, DOI 10.17487/RFC7793, May 2016, <https://www.rfc-editor.org/info/rfc7793>.

[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>.

[RFC8094] Reddy, T., Wing, D., and P. Patil, "DNS over Datagram Transport Layer Security (DTLS)", RFC 8094, DOI 10.17487/RFC8094, February 2017, <https://www.rfc-editor.org/info/rfc8094>.

[RFC8109] Koch, P., Larson, M., and P. Hoffman, "Initializing a DNS Resolver with Priming Queries", BCP 209, RFC 8109, DOI 10.17487/RFC8109, March 2017, <https://www.rfc-editor.org/info/rfc8109>.

[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>.

[RFC9103] Toorop, W., Dickinson, S., Sahib, S., Aras, P., and A. Mankin, "DNS Zone Transfer over TLS", RFC 9103, DOI 10.17487/RFC9103, August 2021, <https://www.rfc-editor.org/info/rfc9103>.

[RSSAC026] Root Server System Advisory Committee (RSSAC), "RSSAC0226 RSSAC Lexicon", 2017, <https://www.icann.org/en/system/files/files/rssac-026-14mar17-en.pdf>.

Приложение A. Определения, обновлённые этим документом

Ниже указаны определения из других RFC, обновлённые этим документом.

- Forwarder из [RFC2308]
- QNAME из [RFC2308]
- Secure Entry Point (SEP) из [RFC3757] (этот RFC уже устарел, см. [RFC4033], [RFC4034], [RFC4035]).

Приложение B. Определения, добавленные этим документом

Ниже указаны определения, добавленные этим документом.

- Alias в разделе 2
- Apex в разделе 7
- arpa в разделе 7
- Authoritative DoT (ADot)" в разделе 6
- Bailiwick в разделе 7
- Class independent в разделе 5
- Classic DNS в разделе 6
- Delegation-centric zone в разделе 7
- Delegation в разделе 7
- DNS operator в разделе 9
- DNSSEC-aware в разделе 10
- DNSSEC-unaware в разделе 10
- Forwarding в разделе 6
- Full resolver в разделе 6
- Fully Qualified Domain Name в разделе 2
- Global DNS в разделе 2
- Hardware Security Module (HSM) в разделе 10

- Host name в разделе 2
- IDN в разделе 2
- In-domain в разделе 7
- Iterative resolution в разделе 6
- Label в разделе 2
- Locally served DNS zone в разделе 2
- Naming system в разделе 2
- Negative response в разделе 3
- Non-recursive query в разделе 6
- Open resolver в разделе 6
- Passive DNS в разделе 6
- Policy-implementing resolver в разделе 6
- Presentation format в разделе 5
- Priming в разделе 6
- Private DNS в разделе 2
- Recursive DoT (RDot) в разделе 6
- Recursive resolver в разделе 6
- Referrals в разделе 4
- Registrant в разделе 9
- Registrar в разделе 9
- Registry в разделе 9
- Root zone в разделе 7
- Secure Entry Point (SEP) в разделе 10
- Sibling domain в разделе 7
- Signing software в разделе 10
- Split DNS в разделе 6
- Stub resolver в разделе 6
- Subordinate в разделе 8
- Superordinate в разделе 8
- TLD в разделе 2
- Validating resolver в разделе 10
- Validation в разделе 10
- View в разделе 6
- Zone transfer в разделе 6

Благодарности

Andrew Sullivan был соавтором [RFC8499] и его предшественника - [RFC7719]. У текущего документа, который является небольшим обновлением [RFC8499], всего два автора. Работа Andrew над предыдущими документами заслуживает высокой оценки.

В создание [RFC8499] и [RFC7719] внесли вклад многие люди, отмеченные в разделах благодарностей этих документов.

Несмотря на то, что этот документ является лишь незначительной переработкой, многие люди из рабочей группы DNSOP внесли в него свой вклад, и их работа заслуживает высокой оценки.

Предметный указатель

Zone signing key (ZSK)	13	Zone transfer	7

Адреса авторов

Paul Hoffman
ICANN
Email: paul.hoffman@icann.org

Kazunori Fujiwara
Japan Registry Services Co., Ltd.
Email: fujiwara@jprs.co.jp

Перевод на русский язык

Николай Малых

nmalykh@protokols.ru