Internet Engineering Task Force (IETF)
Request for Comments: 7719
Category: Informational
ISSN: 2070-1721

P. Hoffman
ICANN
A. Sullivan
Dyn
K. Fujiwara
JPRS

December 2015

Терминология DNS

DNS Terminology

Тезисы

Определения DNS распылены по десяткам RFC. Терминология, используемая разработчиками приложений и протокола DNS, а также операторами систем DNS, за десятки лет существования DNS претерпела некоторые изменения. В этом документе приводятся современные определения многих терминов, применяемых в DNS.

Статус документа

Этот документ не относится к категории проектов стандартов и публикуется с информационными целями.

Документ является результатом работы IETF[1] и представляет собой согласованное мнение сообщества IETF. Документ был вынесен на публичное рассмотрение и одобрен для публикации IESG[2]. Дополнительная информация о документах BCP представлена в разделе 2 документа RFC 5741.

Информация о текущем статусе этого документа, обнаруженных ошибках и способах обратной связи может быть найдена по ссылке http://www.rfc-editor.org/info/rfc7719.

Оглавление

1. Введение

DNS[3] представляет собой простой протокол «запрос-отклик», в котором сообщения запросов и откликов имеют одинаковый формат. Протокол и формат сообщений определены в [RFC1034] и [RFC1035]. В этих документах определены некоторые термины, а в более поздних документах определены другие термины. Трактовка некоторых терминов из RFC 1034 и 1035 с 1987 года изменилась.

В этом документе собрано множество терминов, связанных с DNS. Некоторые из терминов были определены в ранних RFC, другие были определены там недостаточно четко, а ряд терминов совсем не был определен в этих RFC.

Большинство приведенных здесь определений принято сообществом DNS - как разработчиками, так и операторами. Некоторые определения отличаются от принятых в ранних RFC и такие различия отмечены здесь. Те термины, для

[1]Internet Engineering Task Force.
[2]Internet Engineering Steering Group.
[3]Domain Name System - система доменных имен.

которых согласованное определение совпадает с определением одного из ранних RFC, приведены в виде цитат. При наличии тех или иных изменений, упоминается исходный документ RFC, но приводится современное определение.

Важно отметить, что в процессе подготовки этого документа выяснилось, что ряд связанных с DNS терминов по разному интерпретируется специалистами. Более того, некоторые термины, определенные в ранних RFC, стали трактоваться иначе. Авторы предполагают возможность пересмотра этого документа в недалеком будущем. Такой пересмотр может включать более обстоятельное обсуждение некоторых терминов, а также добавление новых терминов. Документ также послужит обновлением для некоторых RFC.

Термины в документе организованы по темам. Даны определения некоторых терминов, применяемых в сообществе DNS, но не определенных ранее.

Связанные с DNS термины иногда определяют и другие организации. Например, W3C определяет термин domain (см. https://specs.webplatform.org/url/webspecs/develop/).

Отметим, что здесь не приводится единого согласованного определения DNS. Этот термин может использоваться в разных смыслах: общепринятая схема именования объектов в сетях Internet, распределенная база данных с именами и некоторыми свойствами объектов, архитектура, обеспечивающая распределенную поддержку, устойчивость и самосогласованность для этой базы данных, простой протокол «запрос-отклик» для реализации этой архитектуры.

Использование заглавных букв в терминах DNS зачастую различается в разных RFC и на практике DNS. В данном документе использование заглавных букв в терминах следует принятой практике, но это не означает, что другие способы обозначения терминов являются неверными или устаревшими. В некоторых случаях для одного термина могут применяться разные варианты использования заглавных букв - это связано с цитированием разных RFC.

2. Имена

Domain name - доменное имя

В параграфе 3.1 документа [RFC1034] сказано: «Пространство имен имеет структуру дерева. … Каждый узел имеет метку размером от 0 до 63 октетов. … Доменное имя узла представляет собой список меток на пути от узла до корня дерева. … Для упрощения реализации общее число октетов, представляющих доменное имя (т. е., октетов меток и их размеров), ограничено значением 255.[1]» Любая метка в доменном имени может содержать произвольные октеты.

Fully qualified domain name (FQDN) - полное доменное имя

Зачастую это означает то же самое, что доменное имя узла, как определено выше. Однако термин этот не однозначен. Строго говоря, полное доменное имя содержит все метки, включая финальную метку корня нулевого размера, например, «www.example.net.» (обратите внимание на точку в конце). Однако, поскольку все имена обычно используют общий корень, их часто указывают относительно этого корня (например, www.example.net), по прежнему называя полными (fully qualified). Этот термин был введен в [RFC819]. В данном документе имена зачастую указываются относительно корня.

Необходимость термина «fully qualified domain name» обусловлена использованием частичных (локальных) доменных имен, когда имя указывается относительно того или иного домена, который не указывается в записи.

Label - метка

Идентификатор отдельного узла в последовательности узлов, идентифицируемой полным доменным именем.

Host name - имя хоста

Этот термин и его эквивалент hostname используются достаточно широко, но не были определены в [RFC1034], [RFC1035], [RFC1123] и [RFC2181]. DNS изначально была развернута в среде Host Table, как описано в [RFC952], и данный термин произошел оттуда. Со временем трактовка термина претерпела изменения. Сейчас термин Host name обычно означает доменное имя в соответствии с правилами параграфа 3.5. Синтаксис имен в [RFC1034]. Напомним, что любая метка в доменном имени может содержать любое октетное значение, именами хостов обычно называют метки, соответствующие правилам для синтаксиса имен, с поправкой на то, что метки могут начинаться с цифр в кодировке ASCII (поправка взята из параграфа 2.1 [RFC1123]).

Иногда термин hostname используют для обозначения первой метки FQDN - например, printer в printer.admin.example.com (это может формализоваться в настройках операционной системы). Кроме того, иногда этим термином обозначают имя машины, которое может включать метки, не соответствующие правилам синтаксиса имен.

TLD - домен верхнего уровня

Доменом верхнего уровня (Top-Level Domain) называют зону, находящуюся на один уровень ниже корня (например, com или jp). С точки зрения DNS домены TLD не представляют ничего особенного. Большинство из таких доменов являются центрами передачи полномочий (деленирования) и их деятельность регламентируется множеством правил. TLD часто делят на группы типа доменов для стран (ccTLD[2]), базовых доменов (gTLD[3]) и т. п.. С точки зрения правил такое деление не имеет значения и выходит за пределы данного документа.

IDN

Сокращение для Internationalized Domain Name. Протокол IDNA обеспечивает стандартный механизм обслуживания в DNS доменных имен с именами, в которых содержатся отличные от ASCII символы. Текущий стандарт, обычно называемый IDNA2008, определен в [RFC5890], [RFC5891], [RFC5892], [RFC5893] и [RFC5894]. Эти документы определяют множество связанных с IDN терминов типа LDH label, A-label, U-label. В [RFC6365] определены дополнительные термины, связанные с использованием других кодировок (часть из них связана с IDN), а в [RFC6055] приведено обсуждение 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.» ([RFC1034], параграф 3.1). Например, в имени хоста nnn.mmm.example.com, имена mmm.example.com и nnn.mmm.example.com являются субдоменами example.com.

Alias - псевдоним

Владелец записи CNAME или субдомен владельца записи DNAME [RFC6672]. См. также *canonical name*.

[1]Приведена цитата из перевода RFC 1034. *Прим. перев.*
[2]Country Code Top-Level Domain.
[3]Generic Top-Level Domain.

Canonical name - каноническое имя

Запись CNAME «идентифицирует имя своего владельца в качестве псевдонима и задает соответствующее каноническое имя в разделе RDATA записи RR» ([RFC1034], параграф 3.6.2). Такое использование термина «канонический» связано с математической концепцией канонических форм.

CNAME

«По традиции метку записи CNAME называют просто CNAME. Это неудачная традиция, поскольку CNAME является сокращением «canonical name», а метка записи CNAME чаще всего не является каноническим именем.» ([RFC2181], параграф 10.1.1)[1].

Public suffix - общественный суффикс, суффикс общего пользования

«Домен, контролируемый публичным регистратором.» ([RFC6265], параграф 5.3). В соответствии с общим определением данный термин означает домен, в котором могут быть зарегистрированы субдомены, и для которого не должны устанавливаться HTTP-куки ([RFC6265]). В доменных именах нет индикации общественного суффикса, его можно определить только с использованием внешних средств. Фактически, общественным суффиксом может быть как домен, так и его субдомены. На момент публикации данного документа рабочая группа IETF DBOUND [DBOUND] занималась вопросами, связанными с общественными суффиксами. Одним из ресурсов для идентификации общественных суффиксов является список PSL[2], поддерживаемый Mozilla (http://publicsuffix.org/). Например, на момент публикации этого документа домен com.au был указан в списке PSL, как общественный суффикс (отметим, что эта ситуация может измениться в будущем).

Отметим, что термин «общественный суффикс» по ряду причин считается в сообществе DNS спорным и его трактовка может существенно измениться в будущем. Одной из связанных с общественными суффиксами сложностей является то, что статус такого суффикса может измениться при изменении политики регистрации для зоны, как для uk TLD на момент публикации этого документа.

3. Заголовок и коды откликов DNS

Заголовок сообщения DNS составляют первые 12 октетов. Многие из полей и флагов на схемах заголовков в параграфах 4.1.1 - 4.1.3 документа [RFC1035] называют в соответствии с обозначениями на этих схемах. Например, коды откликов называют RCODE, данные записи - RDATA, а бит полномочности ответа - флагом (битом) AA.

Некоторые из определенных в [RFC1035] получили сокращенные имена. Имена кодов откликов общего назначения, которые приводятся без числовых значений, включают FORMERR, SERVFAIL, NXDOMAIN (последний называют также «ошибкой в имени» - Name Error). Все значения RCODE перечислены в http://www.iana.org/assignments/dns-parameters, (на сайте используются обозначения строчными и прописными символами, но во многих документах применяются только заглавные буквы).

NODATA

«Псевдо-RCODE, показывающий, что имя корректно для данного класса, но записей этого типа нет. Отклик NODATA выводится из ответа.» ([RFC2308], раздел 1). «NODATA указывается ответом с установленным для RCODE значением NOERROR и отсутствием имеющих отношение к делу ответов в разделе answer. Раздел полномочий (authority) будет содержать запись SOA или в нем не будет записи NS.» ([RFC2308], параграф 2.2). Отметим, что такой же формат применяется в отсылках; в [RFC2308] разъясняется, как отличить их от NODATA.

Иногда используют термин NXRRSET в качестве синонима NODATA. Однако это ошибка, поскольку NXRRSET является кодом конкретной ошибки, определенным в [RFC2136].

Negative response - негативный отклик

Отклик, показывающий, что конкретного RRset не существует, или RCODE, указывающий отсутствие ответа у сервера имен. В разделах 2 и 7 [RFC2308] подробно описаны типы негативных откликов.

Referrals - отсылки

Данные из раздела authority неполномочного (non-authoritative) ответа. В параграфе 2.1 [RFC1035] приведено определение «полномочных» данных. Однако отсылки на срезах зон (см. раздел 6) не являются полномочными. Отсылки могут быть записями NS на срезе зоны и их склеивающими записями. Записи NS на родительской стороне среза являются полномочным делегированием, но обычно не трактуются, как полномочные данные. В общем случае отсылка является для сервера способом передачи ответа, говорящим, что сервер не знает ответа, но знает, куда следует направить запрос для получения ответа. Исторически многие полномочные серверы отвечали отсылками к корневым серверам по запросам имен, для которых у них нет полномочий, но такая практика была отменена.

4. Записи о ресурсах

RR

Сокращение для resource record (запись о ресурсе), параграф 3.6 [RFC1034]).

RRset

Набор записей о ресурсах с одной меткой, классом и типом, но разными данными (определение из [RFC2181]). В некоторых документах используется также обозначение RRSet. Слова «одна метка» (same label) в этом определении означают «одного владельца имен» (same owner name). В дополнение к этому в [RFC2181] сказано, что «значения TTL всех RR в RRSet должны совпадать» (это явно отличается от «отклик на запрос для QTYPE=ANY», что является явным недоразумением).

EDNS

Механизм расширения для DNS, определенный в [RFC6891]. Иногда его называют EDNS0 или EDNS(0) для указания номера версии. EDNS позволяет клиентам и серверам DNS задать размер сообщения, превышающий исходное ограничение в 512 октетов, для расширения пространства кодов отклика и возможно для передачи дополнительных параметров (опций), влияющих на обработку запроса DNS.

OPT

Псевдо-RR (иногда используется термин мета-RR), используемая только для управляющей информации, относящейся к последовательности запросов и откликов в конкретной транзакции (определение из параграфа 6.1.1 [RFC6891]). Используется EDNS.

Owner

Имя домена, в котором найдена RR (параграф 3.6 в [RFC1034]). Зачастую используется термин owner name.

[1]В оригинале приведена искаженная цитата из RFC 2181 (см. здесь). *Прим. перев.*
[2]Public Suffix List.

Имена полей SOA

В документах DNS, включая определения этого документа, часто указывают поля RDATA записей о ресурсах SOA по именам этих полей. Это поля, определенные в параграфе 3.3.13 [RFC1035]. Именами (в порядке размещения в SOA RDATA) являются MNAME, RNAME, SERIAL, REFRESH, RETRY, EXPIRE и MINIMUM.

Отметим, что значение поля MINIMUM изменено в разделе 4 [RFC2308] и в соответствии с новым определением поле MINIMUM указывает лишь «TTL для негативных откликов». В этом документе используются имена полей вместо их описаний.

TTL

Максимальное «время жизни» записи для ресурса. «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.[1]» (цитата из раздела 8 [RFC2181]).

TTL «задает временной интервал, в течение которого запись может кэшироваться прежде, чем снова возникнет необходимость обращения к источнику данных.» (цитата из параграфа 3.2.1 [RFC1035]) Также это значение «задает временной интервал (в секундах), в течение которого запись может кэшироваться до ее отбрасывания» (цитата из параграфа 4.1.3 [RFC1035]). Несмотря на то, что это значение определено для записи ресурса, TTL в каждой записи RRset должно иметь одинаковое значение ([RFC2181], параграф 5.2).

Причина того, что TTL называется максимальным временем жизни, заключается в том, что операторы кэширования могут сокращать это время в соответствии со своими целями (например, политика может запрещать значение TTL выше нокого порога). Если запись удаляется из кэша при незавершенном сроке жизни, значение на деле становится нулевым. Некоторые серверы игнорируют TTL в части RRset (например, когда полномочные данные имеют слишком малое время жизни TTL), хотя это противоречит RFC 1035.

Имеется также концепция «TTL по умолчанию» для зоны, и это значение может быть конфигурационным параметром серверных программ. Оно часто применяется по умолчанию для всего сервера, а принятое по умолчанию значение для зоны указывают с помощью директивы $TTL в файле зоны. Директива $TTL была добавлена в формат первичного файла [RFC2308].

Class independent

Запись для ресурса, синтаксис и семантика которой одинаковы для каждого класса DNS. Тип записи для ресурса, который не является независимым от класса, имеет разные значения в зависимости от класса DNS для записи или его значение не определено за пределами класса IN (класс 1, Internet).

5. Серверы и клиенты DNS

В этом разделе определены термины, используемые для систем, действующих как клиенты и/или серверы DNS.

Resolver - распознаватель

Программа, «получающая от сервера имен информацию в ответ на запрос клиента» (цитата из параграфа 2.4 в [RFC1034]). «Распознаватель размещается на одной машине с запрашивающей его услуги программой, но ему могут потребоваться услуги размещающихся на других хостах серверов имен» (цитата из параграфа 5.1 в [RFC1034]). Программа распознавания запрашивает имя, тип и класс, получая их в отклике. Логическая функция называется распознаванием (resolution). На практике этот термин обычно относится к тому или иному конкретному типу распознавателя (некоторые из них определены ниже) и трактовка термина зависит от контекста.

Stub resolver - оконечный распознаватель

Распознаватель, не способный самостоятельно выполнить все преобразования. Оконечный распознаватель обычно зависит от рекурсивного распознавателя для фактического выполнения функций преобразования. Оконечные распознаватели рассмотрены, но не определены полностью в параграфе 5.3.1 [RFC1034], полное определение дано в параграфе 6.1.3.1 [RFC1123].

Iterative mode - итерационный режим

Режим преобразования сервера, когда он получает запросы DNS и отвечает на них ссылкой на другой сервер. В параграфе 2.3 [RFC1034] это описано как: «сервер указывает клиенту другой сервер, который способен ответить на запрос клиента». Распознаватель, работающие в итерационном режиме иногда называют итерационными распознавателями.

Recursive mode - рекурсивный режим

Режим преобразования сервера, когда он получает запросы DNS и отвечает на них записями из локального кэша или передает запросы другому серверу для получения окончательных ответов на исходные запросы. В параграфе 2.3 [RFC1034] это описано как: «первый сервер транслирует (передает) запрос клиента другому серверу». Сервер, работающий в рекурсивном режиме, может рассматриваться как сервер, включающий серверную (отвечает на запросы) и распознающую (выполняет преобразование) стороны. Системы, работающие в таком режиме, обычно называют рекурсивными серверами, а иногда - рекурсивными распознавателями. Хотя строгое различие между ними состоит в том, что один отправляет запросы другому рекурсивному серверу, а другой - нет, на практике невозможно заранее знать, будет ли сервер выполнять также рекурсию, поэтому термины считаются взаимозаменяемыми.

Full resolver - полный распознаватель

Этот термин применяется в [RFC1035], но не определен там. В RFC 1123 определен «полносервисный распознаватель» (full-service resolver), который может (не обязательно) быть полным распознавателем [RFC1035]. Этот термин не определен должным образом в каком-либо RFC.

Full-service resolver - полнофункциональный распознаватель

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

Priming

Механизм, используемый распознавателем для определения куда отправлять запросы до того, как что-либо появится в кэше распознавателя. Чаще всего это выполняется на основе конфигурационных параметров, содержащих список полномочных серверов для корневой зоны.

Negative caching - кэширование негативных откликов.

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

[1]Отметим, что в [RFC1035] ошибочно указано, что это целое число со знаком. Ошибка исправлена в [RFC2181].

Authoritative server - полномочный сервер

«Сервер, которому содержимое зоны DNS известно из локальных источников и поэтому он может отвечать на запросы для этой зоны, не обращаясь к другим серверам.» (цитата из раздела 2 в [RFC2182]). Это система, которая отвечает на запросы DNS информацией о зонах, для которых она настроена отвечать с флагом AA в заголовке отклика, имеющим значение 1. Это сервер, имеющий полномочия для одной или множества зон DNS. Отметим, что полномочный сервер может отвечать на запросы без передачи ему полномочий родительской зоны. Полномочные серверы также предоставляют «рефералов», обычно для дочерних зон, делегированных ими. Эти «рефералы» имеют бит AA = 0 и приходят со ссылочными данными в разделе Authority и (если нужно) Additional.

Authoritative-only server - сервер, выполняющий лишь функции полномочного

Сервер имен, который обслуживает лишь полномочные данные и игнорирует запросы на рекурсию. Он «обычно не генерирует запросов от себя. Вместо этого он отвечает на нерекурсивные запросы от итерационных распознавателей, ищущих информацию для обслуживаемых этим сервером зон» (цитата из параграфа 2.4 [RFC4697]).

Zone transfer - перенос зоны

Действие клиента, запрашивающего копию зоны, и полномочного сервера, передающего требуемую информацию (см. описание зон в разделе 6). Имеется два базовых стандартных способа переноса зон - AXFR (Authoritative Transfer - полномочный перенос) для копирования всей зоны (описан в [RFC5936] и IXFR (Incremental Transfer - инкрементный перенос) для копирования лишь измененных частей зоны (описан в [RFC1995]). Многие системы применяют нестандартные способы переноса зон, выходящие за рамки протокола DNS.

Secondary server - вторичный сервер

«Уполномоченный сервер, который использует перенос зоны для ее получения» (цитата из параграфа 2.1 в [RFC1996]). В [RFC2182] вторичные серверы описаны подробно. Хотя в ранних RFC для DNS, таких как [RFC1996], применялся термин slave (ведомый), сейчас общепринятым является термин secondary. Вторичные серверы рассмотрены также в [RFC1034].

Slave server - ведомый сервер

См. secondary server.

Primary server - первичный (основной) сервер

«Любой уполномоченный сервер, настроенный на то, чтобы играть роль источника информации при переносе зоны для одного или множества [ведомых] серверов» (цитата из параграфа 2.1 в [RFC1996]) или (более конкретно) «полномочный сервер, настроенный быть источником данных AXFR или IXFR для одного или множества [вторичных] серверов» (цитата из [RFC2136]). Хотя в ранних RFC для DNS, таких как [RFC1996], применялся термин master (ведущий), сейчас общепринятым является термин primary. Первичные серверы рассмотрены также в [RFC1034].

Master server - ведущий сервер

См. primary server.

Primary master - первичный ведущий сервер

«Первичный ведущий сервер зоны указывается в поле SOA MNAME, а также может указываться в NS RR» (цитата из параграфа 2.1 в [RFC1996]). [RFC2136] определяет primary master 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 для зоны существует только один первичный ведущий сервер». Идея первичного ведущего сервера применяется только в [RFC2136] и сочтена архаичной в других частях DNS.

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 - спрятанный ведущий сервер

Скрытый сервер, который является ведущим для переноса зон. «В этой схеме первичный сервер имен, который обрабатывает обновления, недоступен для обычных хостов Internet и не указывается в NS RRset.» (цитата из параграфа 3.4.3 в [RFC6781]) В более раннем RFC [RFC4641] сказано, что имя скрытого ведущего сервера указывается в поле SOA RR MNAME, хотя в некоторых настройках это имя совсем не присутствует в общедоступных DNS. Скрытый ведущий сервер может быть вторичным или первичным ведущим.

Forwarding - пересылка

Процесс, в котором один сервер передает запрос DNS с RD=1 другому серверу для преобразования (resolve). Пересылка является функцией распознавателей DNS и отличается от простой ретрансляции запросов вслепую. [RFC5625] не дает конкретного определения пересылки, но подробно описывает функции системы, которые нужно поддерживать для пересылки. Пересылающие системы иногда называют DNS proxy, но этот термин еще не определен (даже в [RFC5625]).

Forwarder - пересылающий сервер

В разделе 1 [RFC2308] пересылающий сервер описан как: «Сервер имен, используемый для преобразования (resolve) запросов взамен прямого использования цепочки полномочных серверов имен.» Далее в [RFC2308] сказано: «Обычно пересылающий сервер имеет более качественный доступ в Internet или поддерживает кэш большего размера, разделяемый множеством распознавателей имен.» Такое определение представляется указывающим, что пересылающие серверы обычно обращаются с запросами лишь к полномочным серверам. Однако в современной практике эти серверы часто размещаются между оконечным распознавателем и рекурсивными серверами. В [RFC2308] не сказано, является ли пересылающий сервер лишь итерационным или может быть полнофункциональным распознавателем.

Policy-implementing resolver - реализующий правила распознаватель

Работающий в рекурсивном режиме распознаватель, который меняет некоторые возвращаемые ответы на основе критериев политики, таких как предотвращение доступа к вредоносным сайтам или нежелательному содержимому. В общем случае оконечный распознаватель не имеет представления, реализуют ли восходящие распознаватели такую политику, а в случае ее реализации не знает точных правил изменения ответов. В некоторых случаях оконечный распознаватель выбирает реализующий правила распознаватель с явным намерением применять эти правила. В других случаях правила вводятся без уведомления пользователей оконечного распознавателя.

Open resolver - открытый распознаватель

Полнофункциональный распознаватель, который воспринимает и обрабатывает запросы от любого (или почти любого) оконечного распознавателя. Иногда применяется термин public resolver (общедоступный распознаватель), хотя этот термин чаще применяется к открытым распознавателям, которые действительно открыты по сравнению с подавляющим большинством некорректно настроенных распознавателей, которые заявлены открытыми.

View - представление

Конфигурация сервера DNS, позволяющая ему предоставлять разные ответы в зависимости от атрибутов запроса. Обычно представления различаются по IP-адресу источника запроса, но могут различаться также по IP-адресу получателя, типу запроса (например, AXFR), его рекурсивности и т. п. Представления часто используются для возврата большего числа имен или различных адресов при запросе изнутри защищенной сети по сравнению с внешними запросами. Представления являются нестандартизованной частью DNS, но широко распространены в серверных программах.

Passive DNS - пассивный DNS

Механизм для сбора больших объемов данных DNS путем хранения откликов от серверов DNS. Некоторые из таких систем собирают также запросы DNS, связанные с откликами, это может вызывать вопросы, связанные с приватностью. Пассивные базы данных DNS могут служить для ответов на исторические вопросы о зонах DNS, например, какие записи были доступны для них и в какое время (в прошлом). Пассивные базы данных DNS позволяют вести поиск сохраненных записей по ключам, которые отличаются от простых имен, например, «найти все имена, которые имеют запись типа A с определенным значением».

Anycast

«Технология, позволяющая сделать определенный 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])

6. Зоны

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

Zone - зона

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

Child - потомок

«Элемент записи, которые имеет полномочия для домена, полученные 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 «родительский сервер имен» был определен в [RFC882] как «сервер имен, имеющий полномочия для места в пространстве доменных имен, где будет содержаться новый домен» (отметим, что [RFC882] был отменен [RFC1034] и [RFC1035]). В [RFC819] приседено некоторое описание связей между родителями и потомками.

Origin - источник

(a) «Доменное имя, появляющееся наверху зоны (сразу под срезом, отделяющим зону от ее родителя) называется «источником зоны». Имя зоны совпадает с именем домена в источнике зоны.» (цитата из раздела 6 в [RFC2181]). Сейчас термины origin (источник) и apex (вершина зоны, см. ниже) часто используются взаимозаменяемо.

(b) Имя домена, в котором указывается относительное доменное имя в файлах зоны. Обычно рассматривается в контексте $ORIGIN, который является управляющей записью, определенной в параграфе 5.1 [RFC1035] как часть первичного файла зоны. Например, если $ORIGIN имеет значение «example.org.», строка первичного файла www является фактически записью для «www.example.org.».

Apex - вершина

Точка в дереве у владельца SOA и соответствующего полномочного NS RRset. Используется также термин zone apex. [RFC4033] определяет его как «имя на дочерней стороне среза зоны». Apex можно рассматривать как описание структуры дерева в теории данных, а origin является названием того же понятия при реализации в файле зоны. Однако различие поддерживается не всегда и можно встретиться с толкованиями, противоречащими этому определению. [RFC1034] использует термин «верхний узел зоны» (top node of the zone) как синоним apex, но этот термин не получил широкого распространения. Сейчас термины origin (источник, см. выше) и apex (вершина зоны) часто используются взаимозаменяемо.

Zone cut - срез зоны

Точка разделения между двумя зонами, где источник 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]; отметим, что это определение является лишь остенсивным, т. е. демонстрацией на примере). В параграфе 4.2 [RFC1034] используется термин cuts в качестве среза зоны.

Delegation - передача полномочий

Процесс, с помощью которого создается отдельная зона в пространстве имен под вершиной данного домена. Передача полномочий происходит при добавлении NS RRset в родительскую зону для дочернего источника. По сути передача происходит на срезе зоны. Термин также часто служит существительным, которое обозначает новую зону, созданную фактом передачи полномочий.

Glue records - склеивающие записи

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

Более позднее определение говорит, что склеивающие записи включают «имена сервером 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 сегодня склеивание иной раз трактуется с учетом этого более широкого определения, контекст определения [RFC2181] предполагает, что оно относится к склеиванию в самом документе и не обязательно за его пределами.

In-bailiwick - внутренний (в сфере охвата)

(a) Прилагательное для описания сервера имен, чье имя является подчиненным или (в редких случаях) совпадает с именем источника зоны. Серверы in-bailiwick требуют склеивающей записи в родительской зоне (в смысле первого определения склеивающей записи, приведенного выше).

(b) Данные, для которых сервер является полномочным или имеет полномочия для родителя владельца имени. Эта трактовка термина обычно применяется при рассмотрении релевантности склеивающих записей в отклике. Например, сервер для родительской зоны example.com может отвечать со склеивающими записями для

ns.child.example.com. Поскольку зона child.example.com является потомком example.com, склеивающие записи являются in-bailiwick.

Out-of-bailiwick

Антоним для in-bailiwick.

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 [RFC1034]). Отмечено, что это определение может непреднамеренно включать любые записи NS, присутствующие в зоне, включая те, которые не могут быть полномочными, поскольку они идентичны NS RR ниже среза зоны. Это показывает неоднозначность понятия полномочных данных, поскольку записи NS на родительской стороне полномочно указывают делегирование, хотя сами полномочными не являются.

Root zone - корневая зона

Зона, вершина которой имеет пустую метку. Называется также корнем DNS (DNS root).

Empty non-terminals - пустые нетарминальные имена

«Доменные имена, не владеющие записями о ресурсах, но имеющие субдомены с такими записями» (цитата из параграфа 2.2.2 в [RFC4592]). Типичным примером служат записи SRV - в имени _sip._tcp.example.com домен _tcp.example.com вероятно не будет иметь RRset, но _sip._tcp.example.com имеет (по меньшей мере) SRV RRset.

Delegation-centric zone - ориентированная на делегирование зона

Зона, состоящая в основном из передачи полномочий дочерним зонам. Это отличается от зон, которые могут включать делегирование дочерним зонам, но имеют также множество записей о ресурсах для самой зоны и/или дочерних зон. Этот термин применяется в [RFC4956] и [RFC5155], но не определен там.

Wildcard - шаблон

[RFC1034] определяет шаблон, но это определение вызвало путаницу среди разработчиков. Для RR, начинающихся с метки «*» применяется специальная обработка. «Такие RR называют шаблонами. Шаблонные RR можно представлять, как инструкцию по синтезированию RR.» (цитата из параграфа 4.3.3 в [RFC1034]). Расширенное обсуждение шаблонов, включая более четкие определения, приведено в [RFC4592].

Occluded name - скрытое имя

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

Fast flux DNS - быстрое изменение DNS

Это «происходит, когда домен, найденый в DNS, использует записи A для множества адресов IP и каждая имеет очень малый срок действия (Time-to-Live - TTL). Это означает, что домен возвращает разные адреса IP на корткий период времени.» (цитата из параграфа 1.1.5 в [RFC6561] с исправленной опечаткой). Это часто применяется для распространения вредоносных программ. Поскольку адреса меняются быстро, обнаружение всех хостов затруднительно. Следует отметить, что этот метод работает и с записями AAAA, на на момент написания документа такое использование было редким в Internet.

7. Модель регистрации

Registry - регистрация, реестр

Административный процесс зоны, позволяющий регистрировать в ней имена. Этот термин часто применяется только к организациям, выполняющим регистрацию в больших, ориентированных на делегирование зонах (таких как TLD), но формально сторона, принимающая решения о включении в зону, является оператором реестра зоны. Это определение registry с точки зрения DNS, для некоторых зон правила, определяющие включение в зону могут задаваться выщестоящими зонами, а не оператором реестра.

Registrant - регистрант

Человек или организация, от чьего имени имя в зоне зарегистрировано в реестре. Во многих зонах регистрант сам управляет зоной, но в TLD это зачастую не так.

Registrar - регистратор

Сервис-провайдер, выступающий посредником между регистрантом и реестром. Это требуется не для всех регистраций, но в общем случае регистраторы вовлечены в регистрации для TLD.

EPP

Расширяемый протокол предоставления (EPP[1]), который обычно применяется для обмена регистрационными данными между реестрами и регистраторами. EPP определен в [RFC5730].

WHOIS

Протокол, определенный в [RFC3912], который часто применяется для запросов к базам данных регистрации. Данные WHOIS часто используются для связывания регистрационных данных (таких как контакты управления зоной) с доменными именами. Термин «данные WHOIS» часто служит синонимом для базы данных реестра, хотя эта база может обслуживаться другими протоколами, например, RDAP. Протокол WHOIS используется также с реестрами адресов IP.

RDAP

Протокол доступа к регистрационным данным (RDAP[2]), определенный в [RFC7480], [RFC7481], [RFC7482], [RFC7483], [RFC7484] и [RFC7485]. Протокол и формат данных RDAP предназначены для замены WHOIS.

DNS operator - оператор DNS

Сторона, отвечающая за работу серверов DNS. Для полномочных серверов зон регистрант может быть оператором DNS для себя или это может делать регистратор от его имени, а также может применяться сторонний оператор. Для некоторых зон функции регистрации выполняются оператором DNS и другими сторонами, определяющими разрешенное содержимое зоны.

8. Базовые термины DNSSEC

Большинство терминов DNSSEC определено в [RFC4033], [RFC4034], [RFC4035] и [RFC5155]. Термины, которые вызвали путаницу в сообществе DNS, выделены здесь.

[1]Extensible Provisioning Protocol.
[2]Registration Data Access Protocol.

DNSSEC-aware и DNSSEC-unaware - понимающие и не понимающие DNSSEC

Эти два термина, применяемые в некоторых RFC, не были определены формально. Однако в разделе 2 [RFC4033] определено множество типов распознавателей и проверяющих узлов, включая «не проверяющий корректность знающий о защите оконечный распознаватель» (non-validating security-aware stub resolver), «не проверяющий оконечный распознаватель» (non-validating stub resolver), «знающий о защите сервер имен» (security-aware name server), «знающий о защите рекурсивный сервер имен» (security-aware recursive name server), «знающий о защите распознаватель» (security-aware resolver), «знающий о защите оконечный распознаватель» (security-aware stub resolver) и security-oblivious 'anything'" (отметим, что термин проверяющий распознаватель - validating resolver, используемый в некоторых связанных с DNSSEC локументах, тоже не определен).

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 было отмечено, что сама зона на деле не подписана, но все относящиеся к делу RRset в зоне подписаны. Тем не менее, если зона, которую следует подписывать, содержит не подписанные (или исключенные) RRset, эти RRset будут считаться поддельными и вся зона будет требовать иной обработки.

Следует также отметить, что с момента публикации [RFC6840] записи NSEC больше не требуются для подписанных зон и вместо этого подписанная зона может включать записи NSEC3. В [RFC7129] приведено дополнительное обоснование и некий контекст для механизмов NSEC и NSEC3, применяемых DNSSEC для предоставления аутентифицированных откликов об отсутствии (denial-of-existence response).

Unsigned zone – не подписанная зона

Раздел 2 в [RFC4033] определяет это как «зону, которая не подписана». В разделе 2 [RFC4035] приведено другое определение: «Зона, не включающая записи [корректно созданные открытый ключ DNS (DNSKEY), сигнатуру RR (RRSIG), записи NSEC и (не обязательно) DS] в соответствии с указанными правилами». Важно отметить, что в конце параграфа 5.2 [RFC4035] указана другая ситуация, где зона считается не подписанной: «Если распознаватель не поддерживает ни одного алгоритма, заданного в DS RRset, он не может проверить путь аутентификации к дочерней зоне. Поэтому распознавателю **следует** считать дочернюю зону не подписанной.»

NSEC

«Запись NSEC позволяет защищенному 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]). Говоря кратко, запись NSEC обеспечивает аутентифицированную информацию об отсутствии.

«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 RFC 4034).

NSEC3

Как и NSEC, запись NSEC3 обеспечивает аутентифицированый отклик об отсутствии, однако записи NSEC3 смягчают перечисление зон и поддерживают Opt-Out. Записи NSEC3 определены в [RFC5155].

Отметим, что в [RFC6840] сказано, что [RFC5155] «сейчас считается частью семейства документов DNS Security, описанного в разделе 10 [RFC4033]». Это означает, что некоторые определения из более ранних RFC, где упоминаются лишь записи NSEC, вероятно следует относить к NSEC и NSEC3.

Opt-out

«Флаг Opt-Out указывает, что NSEC3 RR может содержать неподписанную передачу полномочий.» (цитата из параграфа 3.1.2.1 в [RFC5155]). Opt-out решают проблему высокой стоимости защиты передачи полномочий в незащищенную зону. При использовании Opt-Out имена, которые являются незащищенным делегированием (и пустые не-терминалы, выводимые лишь из незащищенного делегирования), не требуют записи NSEC3 или соответствующих ей записей RRSIG. Записи NSEC3 с Opt-Out не способны подтвердить или опровергнуть наличие незащищенного делегирования (адаптировано из параграфа 5.1 в [RFC7129]).

Zone enumeration - перечисление зон

«Практика раскрытия всего содержимого зоны путем последовательных запросов.» (цитата из параграфа 1.3 в [RFC5155]). Называется также прохождением зон (zone walking). Перечисление зоны отличается от предсказания содержимого зоны, где предсказатель использует большой словарь возможных меток и передает для них последовательные запросы или сопоставляет содержимое записей NSEC3 с таким словарем.

Key signing key (KSK) - ключ подписи ключей

Ключи DNSSEC, служащие «лишь для подписи DNSKEY RRset вершины.» (цитата из параграфа 3.1 в [RFC6781]).

Zone signing key (ZSK) - ключ подписи зоны

«Ключи DNSSEC, которые могут применяться для подписи всех RRset в зоне, требующих подписи и не являющихся DNSKEY Rrset вершины зоны.» (цитата из параграфа 3.1 в [RFC6781]). Отметим, что роли KSK и ZSK не являются взаимоисключающими, один ключ может служить одновременно KSK и ZSK. Отметим также, что ZSK иногда применяют для подписывания DNSKEY Rrset вершины.

Combined signing key (CSK) - комбинированный ключ подписи

«В случаях, когда ключи KSK и ZSK не различают, т. е. один ключ служит KSK и ZSK, говорят об однотипной схеме подписи (Single-Type Signing Scheme).» (цитата из параграфа 3.1 в [RFC6781]). Этот ключ иногда называют комбинированным ключом подписи (combined signing key или CSK). Это операционная практика (не протокол), которая определяет, что конкретный ключ является ZSK, KSK или CSK.

Secure Entry Point (SEP) - защищенная точка входа

Флаг в DNSKEY RDATA, который «может служить для различения ключей, предназначенных быть защищенными точками входа в зону при построении цепочек доверия, т. е. они указываются (будут указываться) родительскими DS RR или будут настроены как доверенные привязки. Поэтому предлагается устанавливать флаг SEP для ключей, служащих KSK, а не для ключей, используемых как ZSK, а в случаях, когда KSK и ZSK не различаются (т. е. для схемы с однотипными подписями), предлагается устанавливать флаг SEP для всех ключей.» (цитата из параграфа 3.2.3 в [RFC6781]). Отметим, что флаг SEP является лишь подсказкой и его наличие или отсутствие не может служить основанием для отказа от применения данной DNSKEY RR в качестве KSK или ZSK при проверке.

DNSSEC Policy (DP) - политика DNSSEC

Оператор, который «устанавливает требования безопасности и реализуемые стандарты в зоне с подписью DNSSEC.» (цитата из раздела 2 в [RFC6841]).

DNSSEC Practice Statement (DPS) - заявление о практике DNSSEC

«Документ о раскрытии практики, который может поддерживать и дополнять документы политики DNSSEC (при их наличии) и указывает, как управление данной зоной реализует процедуры и элементы управления на верхнем уровне.» (цитата из раздела 2 в [RFC6841]).

9. Состояния DNSSEC

Проверяющий распознаватель может определить, что отклик имеет одно из 4 состояний: secure (защищенный), insecure (незащищенный), bogus (подделка) или indeterminate (неопределенное). Эти состояния определены в [RFC4033] и [RFC4035], хотя определения несколько различаются. Данный документ не пытается согласовать эти определения и не заявляет о необходимости такого согласования.

Ниже приведены определения из раздела 5 в [RFC4033].

Проверяющий распознаватель может определять 4 перечисленных ниже состояния.

Secure - защищенное
Проверяющий распознаватель имеет доверенную привязку или цепочку доверия или способен проверить все подписи в отклике.

Insecure - незащищенное
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 незащищенными. Проверяющий распознаватель может иметь локальное правило для маркировки части доменного пространства, как незащищенной.

Bogus - подделка
Проверяющий распознаватель имеет доверенную привязку и защищенное 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 - неопределенное
Нет доверенной привязки, которая показывает, что определенная часть дерева защищена. Это состояние принимается по умолчанию.

Ниже приведены определения из параграфа 4.3 в [RFC4035].

Защищенный распознаватель **должен** быть способен различать перечисленные ниже случаи.

Secure - защищенное
RRset, для которого распознаватель способен построить цепочку подписанных записей DNSKEY и DS RR от даверенной защитной привязки (security anchor) до RRset. В этом случае набору RRset следует быть подписанным и для него выполняется проверка подписи, описанная выше.

Insecure - незащищенное
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.

Bogus - подделка
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.

Indeterminate - неопределенное
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.

10. Вопросы безопасности

Приведенные в этом документе определения не меняют состояния безопасности для DNS.

11. Литература

11.1. Нормативные документы

[RFC882] Mockapetris, P., "Domain names: Concepts and facilities", RFC 882, DOI 10.17487/RFC0882, November 1983, <http://www.rfc-editor.org/info/rfc882>.

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

[RFC1035] Mockapetris, P., "Domain names - implementation and specification", STD 13, RFC 1035, DOI 10.17487/RFC1035, November 1987, <http://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, <http://www.rfc-editor.org/info/rfc1123>.

[RFC1996] Vixie, P., "A Mechanism for Prompt Notification of Zone Changes (DNS NOTIFY)", RFC 1996, DOI 10.17487/RFC1996, August 1996, <http://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, <http://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, <http://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, <http://www.rfc-editor.org/info/rfc2182>.

[RFC2308] Andrews, M., "Negative Caching of DNS Queries (DNS NCACHE)", RFC 2308, DOI 10.17487/RFC2308, March 1998, <http://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, <http://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, <http://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, <http://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, <http://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, <http://www.rfc-editor.org/info/rfc5155>.

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

[RFC5936] Lewis, E. and A. Hoenes, Ed., "DNS Zone Transfer Protocol (AXFR)", RFC 5936, DOI 10.17487/RFC5936, June 2010, <http://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, <http://www.rfc-editor.org/info/rfc6561>.

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

[RFC6781] Kolkman, O., Mekking, W., and R. Gieben, "DNSSEC Operational Practices, Version 2", RFC 6781, DOI 10.17487/RFC6781, December 2012, <http://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, <http://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, <http://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, <http://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, <http://www.rfc-editor.org/info/rfc7344>.

11.2. Дополнительная литература

[DBOUND] IETF, "Domain Boundaries (dbound) Working Group", 2015, <https://datatracker.ietf.org/wg/dbound/charter/>.

[RFC819] Su, Z. and J. Postel, "The Domain Naming Convention for Internet User Applications", RFC 819, DOI 10.17487/RFC0819, August 1982, <http://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, <http://www.rfc-editor.org/info/rfc952>.

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

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

[RFC4641] Kolkman, O. and R. Gieben, "DNSSEC Operational Practices", RFC 4641, DOI 10.17487/RFC4641, September 2006, <http://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, <http://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, <http://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, <http://www.rfc-editor.org/info/rfc4956>.

[RFC5625] Bellis, R., "DNS Proxy Implementation Guidelines", BCP 152, RFC 5625, DOI 10.17487/RFC5625, August 2009, <http://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, <http://www.rfc-editor.org/info/rfc5890>.

[RFC5891] Klensin, J., "Internationalized Domain Names in Applications (IDNA): Protocol", RFC 5891, DOI 10.17487/RFC5891, August 2010, <http://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, <http://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, <http://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, <http://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, <http://www.rfc-editor.org/info/rfc6055>.

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

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

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

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

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

[RFC7482] Newton, A. and S. Hollenbeck, "Registration Data Access Protocol (RDAP) Query Format", RFC 7482, DOI 10.17487/RFC7482, March 2015, <http://www.rfc-editor.org/info/rfc7482>.

[RFC7483] Newton, A. and S. Hollenbeck, "JSON Responses for the Registration Data Access Protocol (RDAP)", RFC 7483, DOI 10.17487/RFC7483, March 2015, <http://www.rfc-editor.org/info/rfc7483>.

[RFC7484] Blanchet, M., "Finding the Authoritative Registration Data (RDAP) Service", RFC 7484, DOI 10.17487/RFC7484, March 2015, <http://www.rfc-editor.org/info/rfc7484>.

[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, <http://www.rfc-editor.org/info/rfc7485>.

Благодарности

Авторы выражают благодарность всем авторам связанных с DNS документов RFC. Комментарии Tony Finch, Stephane Bortzmeyer, Niall O'Reilly, Colm MacCarthaigh, Ray Bellis, John Kristoff, Robert Edmonds, Paul Wouters, Shumon Huque, Paul Ebersman, David Lawrence, Matthijs Mekking, Casey Deccio, Bob Harold, Ed Lewis, John Klensin, David Black и многих других членов рабочей группы DNSOP оказали существенную помощь при подготовке данного документа.

Адреса авторов

Paul Hoffman

ICANN

Email: paul.hoffman@icann.org

Andrew Sullivan

Dyn

150 Dow Street, Tower 2

Manchester, NH 03101

United States

Email: asullivan@dyn.com

Kazunori Fujiwara

Japan Registry Services Co., Ltd.

Chiyoda First Bldg. East 13F, 3-8-1 Nishi-Kanda

Chiyoda-ku, Tokyo 101-0065

Japan

Phone: +81 3 5215 8451

Email: fujiwara@jprs.co.jp

Перевод на русский язык

Николай Малых

nmalykh@gmail.com