Internet Engineering Task Force (IETF)
Request for Comments: 6672
Obsoletes: 2672
Updates: 3363
Category: Standards Track
ISSN: 2070-1721

S. Rose
NIST
W. Wijngaards
NLnet Labs

June 2012

DNAME Redirection in the DNS

Перенаправление DNAME в DNS

Аннотация

Запись DNAME обеспечивает перенаправление для субдерева доменных имён в DNS, т. е. все имена с соответствующим суффиксом перенаправляются в другую часть DNS. Этот документ отменяет исходную спецификацию RFC 2672, а также обновляет документ о представлении адресов IPv6 в DNS (RFC 3363).

Статус документа

Документ относится к категории Internet Standards Track.

Документ является результатом работы IETF[1] и представляет согласованный взгляд сообщества IETF. Документ прошёл открытое обсуждение и был одобрен для публикации IESG[2]. Дополнительную информацию о стандартах Internet можно найти в разделе 2 в RFC 5741.

Информацию о текущем статусе документа, ошибках и способах обратной связи можно найти по ссылке http://www.rfc-editor.org/info/rfc6672.

Оглавление

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

1. Введение

DNAME - это запись о ресурсе DNS, исходно определённая в RFC 2672 [RFC2672]. DNAME обеспечивает перенаправления части дерева имён DNS в другую часть дерева имён DNS.

DNAME RR и CNAME RR [RFC1034] заставляют поиск (потенциально) возвращать данные, соответствующие доменному имени, отличному от запрошенного. Различие между этими типами записей состоит в том, что CNAME RR направляет поиск данных для владельца на (одно) другое имя, а DNAME RR направляет поиск данных для потомков владельца имени на соответствующие имена в (одном) другом узле дерева.

Примером может служить поиск в зоне (см. п. 3 в параграфе 4.3.2 RFC 1034 [RFC1034]) доменного имени foo.example.com с обнаружением в example.com записи DNAME, указывающей, что все запросы ниже example.com перенаправляются в example.net. Процесс поиска возвращается к п. 1 с запросом нового имени foo.example.net. Если в запросе было имя www.foo.example.com, новый запрос будет содержать www.foo.example.net.

Этот документ является пересмотром исходной спецификации DNAME из RFC 2672 [RFC2672]. Запись DNAME была предназначена для решения задачи поддержки сопоставления адресов с именами в контексте смены сетевых адресов. При тщательной настройке смена адресов в сети не ведёт к смене полномочных серверов, содержащих отображения адресов на имена. Практическим примером является делегирование реверсного пространства бесклассовых адресов.

Другим применением DNAME являются псевдонимы в пространстве имён. Например, администратор зоны может пожелать, чтобы ветви дерева DNS содержали одну информацию. Примеры включают варианты punycode [RFC3492] для доменных пространств.

Этот пересмотр спецификации DNAME не меняет формат передачи и обработку записей DNAME. Здесь также рассмотрены проблемы, которые могут возникать при использовании DNAME.

1.1. Уровни требований

Ключевые слова **необходимо** (MUST), **недопустимо** (MUST NOT), **требуется** (REQUIRED), **нужно** (SHALL), **не следует** (SHALL NOT), **следует** (SHOULD), **не нужно** (SHOULD NOT), **рекомендуется** (RECOMMENDED), **возможно** (MAY), **необязательно** (OPTIONAL) в данном документе интерпретируются в соответствии с RFC 2119 [RFC2119].

2. Запись DNAME

2.1. Формат

Записи DNAME RR имеют мнемоническое имя DNAME и десятичный код типа 39. Записи не зависят от класса адреса. Элемент RDATA состоит из одного поля <target>, содержащего полное доменное имя, которое **должно** передаваться в несжатой форме [RFC1035] [RFC3597]. Поле <target> **должно** присутствовать и использует формат представления доменных имён [RFC1035]. Формат представления RR показан ниже.

```
<owner> <ttl> <class> DNAME <target>
```

Влияние DNAME RR заключается в подстановке вместо поля <target> имя владельца записи в качестве суффикса домена. Эта подстановка применяется ко всем именам, размещённым в иерархии ниже имени владельца DNAME RR, для каждой DNAME RR, найденной в процессе распознавания, что разрешает достаточно длинные цепочки DNAME RR.

Детали процесса подстановки, методы предотвращения конфликтов записей о ресурсах и правила для особых случаев рассматриваются в последующих параграфах.

2.2. Подстановка DNAME

Если при выполнении п. 3 алгоритма из параграфа 4.3.2 в RFC 1034 [RFC1034]: «Начало поиска соответствия (метка за меткой) в зоне» обнаруживается узел, владеющий записью DNAME, выполняется подстановка DNAME. Искомое имя может быть именем из исходного запроса, результатом следования CNAME или найденной ранее записи DNAME. Как и при поиске CNAME или набора записей NS, обработка DNAME происходит до нахождения желаемого доменного имени.

Подстановка DNAME выполняется путём замены суффиксных меток искомого имени, совпадающих с именем владельца DNAME, строкой меток из поля RDATA. Во всех случаях совпадающие метки заканчиваются меткой корня. Заменяются только метки целиком. Общие и частные случаи приведены в таблице примеров ниже. QNAME в таблице указывает имя в запросе, владельцем DNAME является владелец доменного имени, а target указывает цель записи DNAME. Результатом является имя, полученное при подстановке DNAME в имя из запроса. Отсутствие совпадений говорит, что запрос не соответствует DNAME, подстановка не выполняется и может возвращаться сообщение об

ошибке (если нет иного результата). Каждая строка таблицы содержит пример подстановки, cyc и shortloop содержат петли.

Таблица 1. Примеры подстановки DNAME.

QNAME	*Владелец DNAME*	*target*	*Результат*
com.	example.com.	example.net.	Нет совпадений
example.com.	example.com.	example.net.	[1]
a.example.com.	example.com.	example.net.	a.example.net.
a.b.example.com.	example.com.	example.net.	a.b.example.net.
ab.example.com.	b.example.com.	example.net.	Нет совпадений
foo.example.com.	example.com.	example.net.	foo.example.net.
a.x.example.com.	x.example.com.	example.net.	a.example.net.
a.example.com.	example.com.	y.example.net.	a.y.example.net.
cyc.example.com.	example.com.	example.com.	cyc.example.com.
cyc.example.com.	example.com.	c.example.com.	cyc.c.example.com.
shortloop.x.x.	x.	.	shortloop.x.
shortloop.x.	x.	.	shortloop.

Записи DNAME могут создавать петли, аналогично CNAME, а также эти записи могут создавать петли совместно и даже одна краевая запись DNAME может формировать петлю. Распознавателям и серверам следует соблюдать осторожность при выделении ресурсов для запроса, но следует учитывать возможность наличия достаточно длинных цепочек DNAME. Администраторам содержимого зон следует принимать меры против возникновения петель при использовании перенаправлений DNAME и DNAME/CNAME.

В результате подстановки доменное имя может стать слишком длинным. Предположим, например, что целевое имя DNAME RR содержит 250 октетов (множество меток). Тогда при входящем QNAME размером более 5 октетов размер результата будет больше 255 октетов. В таких случаях сервер возвращает RCODE YXDOMAIN [RFC2136]. Запись DNAME и её подпись (если зона подписана) включаются в ответ, как подтверждение кода YXDOMAIN (6).

2.3. Совпадение имени владельца DNAME с QNAME

В отличие от CNAME RR, запись DNAME RR перенаправляет имена DNS, подчинённые имени владельца, а само имя владельца DNAME не перенаправляется. Доменному имени, владеющему записью DNAME, разрешено иметь другие типы записей о ресурсах, исключая DNAME, CNAME и другие типы, имеющие ограничения на сосуществование с ним.

При совпадении QTYPE с типом или типами, также принадлежащими имени владельца, отклик исходит от имени владельца. Например, для QTYPE типа ANY будут возвращены (доступные) типу по имени владельца, а не цели.

DNAME RR **недопустимо** присутствовать с тем же именем владельца, что и NS RR, если имя владельца не является вершиной зоны. Если это не вершина, NS RR указывает точку делегирования и DNAME RR должна появляться ниже среза зоны в вершине дочерней зоны.

Если запись DNAME присутствует на вершине зоны, там все равно требуются записи SOA и NS. Такую запись DNAME нельзя использовать для полного отражения зоны, поскольку она не отражает вершину зоны.

Приведённые правила позволяют запрашивать записи DNAME через кэш, совместимый с RFC 1034 [RFC1034] и не знающий о DNAME.

2.4. Имена вслед за записью DNAME и ниже её

Недопустимо существование записей о ресурсах в любом из субдоменов владельца DNAME RR. Для получения содержимого для имён, подчинённых имени владельца должно применяться перенаправление DNAME, запрашивающее результирующую цель. Сервер **может** отказаться загружать зону, имеющую данные в субдомене доменного имени, владеющего DNAME RR. Если сервер загружает зону, имена ниже DNAME RR будут скрыты, как описано в параграфе 7.18 RFC 2136 [RFC2136]. Кроме того, сервер должен отказаться загружать зону, подчинённую владельцу записи DNAME в родительской зоне. Вопросы динамического обновления обсуждаются в параграфе 5.2.

DNAME является одноэлементным (singleton) типом, т. е. для каждого имени разрешена лишь одна запись DNAME. Владелец имени DNAME может иметь лишь одну DNAME RR и для этого имени не может существовать CNAME RR. Эти правила гарантируют, что для доменного имени существует лишь одно перенаправление, что избавляет от путаницы. Сервер должен отказываться от загрузки зон, нарушающих эти правила.

2.5. Сжатие записи DNAME

Имя владельца DNAME может быть сжато, как и любое другое имя владельца. Целевое имя DNAME RDATA **недопустимо** передавать в сжатой форме и оно **должно** приводиться к нижнему регистру (downcased) для проверки DNSSEC.

Хотя в прежней спецификации DNAME [RFC2672] (отменена этим документом) говорилось о сигнализации, позволяющей сжимать целевое имя, такая сигнализация не была задана.

В RFC 2672 (отменен этим документом) сказано, что версия расширенного DNS (Extended DNS или EDNS) имеет средства для понимания сжатия DNAME и целевых имён DNAME. Этот документ отменяет эти слова, поскольку для DNAME отсутствует сигнализация EDNS.

3. Обработка

3.1. Создание CNAME

При подготовке отклика сервер, выполняющий подстановку DNAME, во всех случаях включает в раздел ответа соответствующую DNAME RR. Такие случаи указаны ниже.

[1] Результат зависит от QTYPE и при QTYPE = DNAME результатом будет example.com., в иных случаях совпадения не будет.

1. DNAME применяется как инструкция для подстановки.
2. Запись DNAME соответствует QTYPE, а имя владельца совпадает с QNAME.

Если имя владельца совпадает с QNAME, а QTYPE совпадает с другим типом, принадлежащим ему, DNAME не включается в ответ.

Если DNAME применяется в качестве инструкции подстановки, синтезируется запись CNAME RR со сроком действия (Time to Live или TTL), равным сроку действия DNAME RR, и включается в раздел ответов. Именем владельца CNAME является QNAME из запроса. В спецификации DNSSEC ([RFC4033] [RFC4034] [RFC4035]) сказано, что синтезированную запись CNAME не требуется подписывать. В подписанной DNAME имеется поле RRSIG и проверяющий распознаватель может сравнить CNAME с записью DNAME и подтвердить подпись DNAME RR.

Серверы **должны** быть способны отвечать на запрос для синтезированной записи CNAME. Как и другие типы запросов, этот запрос вызывает DNAME, сервер синтезирует запись CNAME и помещает её а раздел ответов. Если рассматриваемый сервер является кэшем, TTL синтезированной записи CNAME **следует** делать равным декрементированному TTL кэшированной записи DNAME.

Распознаватели **должны** быть способны обрабатывать синтезированные CNAME с TTL = 0 или совпадающим с TTL соответствующей записи DNAME (поскольку некоторые старые реализации полномочных серверов устанавливают в синтезированных CNAME TTL = 0). Нулевое значение TTL означает, что CNAME можно отбросить сразу после обработки ответа.

3.2. Серверный алгоритм

Ниже приведён пересмотренный вариант серверного алгоритма из параграфа 4.1 в RFC 2672.

1. Устанавливается или сбрасывается значение доступности рекурсии в зависимости от готовности сервера имён предоставлять рекурсивные услуги. Если рекурсия доступна и запрошена битом RD в запросе, выполняется переход к п. 5, иначе - к п. 2.
2. Поиск в доступных зонах для зоны, являющейся ближайшим предком QNAME. При нахождении такой зоны выполняется п. 3, иначе - п. 4.
3. Сопоставление метки за меткой вниз по этой зоне. Сопоставление может прерываться как указано ниже.

   A. Полное совпадение QNAME означает, что узел найден.

      Если данные узла являются CNAME, а QTYPE не соответствует CNAME, копия CNAME RR помещается в раздел ответа отклика, QNAME меняется на каноническое имя в CNAME RR и выполняется возврат к п. 1. В иных случаях все RR, соответствующие QTYPE, копируются в раздел ответов с переходом к п. 6.

   B. Если соответствие выводит за пределы полномочных данных, это будет ссылка (referral). Такое происходит при наличии узла с NS RR, маркирующими срез по нижней части зоны.

      NS RR для субзоны копируются в раздел полномочий (authority) отклика. Все доступные адреса помещаются в дополнительный раздел с использованием склеивающих RR, если адреса недоступны из полномочных данных или кэша. Переход к п. 4.

   C. Если для какой-либо метки сопоставление невозможно (соответствующей метки нет), проверяется наличие у последней соответствующей метки записи DNAME.

      Если запись DNAME в этой точке существует, она копируется в раздел ответов. Если подстановка её <target> для её <owner> в QNAME приводит к превышению допустимого размера <domain-name>, устанавливается RCODE = YXDOMAIN [RFC2136] и выполнение завершается (выход). В иных случаях выполняется подстановка и обработка продолжается. Сервер **должен** синтезировать запись CNAME, как описано выше, и включить её в раздел ответов. Возврат к п. 1.

      Если записи DNAME нет, проверяется наличие метки *. Если такой метки нет, проверяется совпадение искомого имени с исходным QNAME из запроса или именем, которое было найдено по CNAME или DNAME. При совпадении с исходным именем в отклике устанавливается ошибка полномочного имени и обработка завершается, в иных случаях обработка завершается без ошибки. При наличии метки * RR этого узла сопоставляются с QTYPE. При совпадении запись копируется в раздел ответов с указанием владельцем RR имени QNAME, а не узла с меткой *. Если данные узла с меткой * - это CNAME и QTYPE не соответствует CNAME, запись CNAME RR копируется в раздел ответов отклика с заменой владельца имени на QNAME, сменой QNAME на каноническое имя в CNAME RR и возвратом к п. 1. В иных случаях выполняется п. 6.
4. Сопоставление с кэшем. При нахождении QNAME в кэше все присоединённые к нему RR, соответствующие QTYPE, копируются в раздел ответов. Если QNAME не найдено в кэше, но имеется запись DNAME у предка владельца QNAME, эта запись DNAME копируется в раздел ответов. Если не было делегирования из полномочных данных, выбирается лучшее из кэша и помещается в раздел authority. Переход к п. 6.
5. Применяется локальный распознаватель или копия его алгоритма для ответа на запрос. Результат сохраняется в разделе ответов отклика, включая любые промежуточные CNAME и DNAME.
6. Предпринимается попытка добавить другие RR, которые могут быть полезны в дополнительный раздел запроса с использованием только локальных данных. Обработка завершается (выход).

Отметим, что будет не более 1 предка с DNAME, как описано в п. 4, если только данные какой-либо зоны не нарушают ограничение на потомков (no-descendants) из раздела 3. Реализация может воспользоваться этим ограничениемЮ останавливая поиск на этапе 3c или 4 при обнаружении записи DNAME.

3.3. Шаблоны

Применять DNAME с шаблонами не рекомендовано в [RFC4592]. Таким образом, **не следует** использовать DNAME вида *.example.com.

Взаимодействие между подстановкой шаблона и перенаправлением из DNAME является неопределенным. Из-за неопределённости обработки проверяющие распознаватели DNSSEC могут оказаться не в состоянии проверить DNAME с шаблоном.

Сервер **может** выдавать предупреждение о неопределённом поведении при загрузке DNAME с шаблоном. Сервер **может** отвергать загрузку зоны или динамические обновления.

3.4. Восприятие и промежуточное хранение

Кэширующие рекурсивные серверы имён могут сталкиваться с данными в именах ниже имени владельца DNAME RR из-за изменений на полномочном сервере, если в кэше имеются данные до и после изменения. Эта конфликтная ситуация является переходной фазой, которая завершается по тайм-ауту старых данных. Кэширующий сервер имён может хранить как старые, так и новые данные и относится к каждым из них, как будто других не существует, а также отбрасывать старые данные или длинные доменные имена. При любом подходе согласованность восстанавливается по истечении срока действия (TTL) старых данных.

Рекурсивные серверы имён с кэшированием **должны** синтезировать CNAME от имени клиентов.

Если рекурсивный сервер имён с кэшированием встречает подтверждённую DNSSEC запись DNAME RR, которая противоречит находящимся в кэше сведениям (за исключением записей CNAME), ему **следует** кэшировать DNAME RR, но **можно** кэшировать запись CNAME, полученную вместе с DNAME, в соответствии с правилами для CNAME. Если DNAME RR невозможно подтвердить через DNSSEC (т. е. это не BOGUS, но проверка не возможна), рекурсивному серверу с кэшированием **не следует** кэшировать DNAME RR, но **можно** кэшировать полученную с ней запись CNAME в соответствии с правилами для CNAME.

3.4.1. Алгоритм распознавателя

Ниже представлена пересмотренная версия алгоритма распознавателя, описанного в параграфе 4.2 RFC 2672.

1. Проверяется возможность получить ответ из локальных данных или синтезировать его из кэшированного DNAME. Если ответ найден, он возвращается клиенту.
2. Определяется наилучший сервер для запроса.
3. Запросы передаются, пока не будет возвращён отклик.
4. Анализируется полученный отклик.
   A. Если отклик отвечает на вопрос или указывает ошибку имени, данные из него кэшируются и возвращаются клиенту.
   B. Если отклик указывает лучшее делегирование другим серверам, данные делегирования кэшируются и происходит возврат к п. 2.
   C. Если отклик указывает CNAME и не является ответом, CNAME кэшируется, в CNAME RR значение SNAME меняется на каноническое имя и происходит возврат к п. 1.
   D. Если отклик указывает DNAME и не является ответом, DNAME кэшируется (после подтверждения DNSSEC, если клиент является проверяющим распознавателем). Если замена целевого имени DNAME именем владельца ведёт к превышению допустимого для доменного имени размера SNAME, приложению возвращается зависящая от реализации ошибка. Иначе выполняется подстановка и возврат к п. 1.
   E. Если отклик говорит об отказе сервера или содержит странные сведения, сервер удаляется из SLIST с возвратом к п. 3.

4. Рассмотрение DNAME в других документах

В параграфе 10.3 [RFC2181] при рассмотрении записей MX и NS затрагивается перенаправление с помощью CNAME, но это относится и к DNAME. В параграфе 10.3 (Записи MX и NS) [RFC2181] сказано:

> Доменное имя, используемое в качестве значения записи NS или части значения записи MX не должно быть псевдонимом. Это не просто разъяснение – использование псевдонима в любой из указанных позиций не обеспечит корректной работы и не приведёт к ожидаемым результатам. Это доменное имя должно иметь в качестве значения по крайней мере одну адресную запись. В настоящее время в качестве таких значений могут использоваться записи типа A, однако в будущем могут появиться другие типы, дающие адресную информацию. Это также может быть RR другого типа, но ни в коем случае не CNAME RR.

DNAME RR рассматриваются в разделе 4 RFC 3363, посвящённом A6 и DNAME. Вступительная посылка этого раздела явно ошибочна, а значит неверен и основанный на ней вывод. В частности, [RFC3363] запрещает применять DNAME в реверсном дереве IPv6. На основе накопленного опыта [RFC3363] пересматривается с отменой всех ограничений на наличие DNAME RR в этих зонах [RFC6434]. Это существенно повысит управляемость реверсного дерева IPv6. Изменения явно указаны ниже. Соответствующий абзац [RFC3363] заменяется приведённым ниже текстом и применение DNAME RR в реверсном дереве больше не запрещается.

> Проблемы применения DNAME в дереве реверсного отображения тесно связаны с необходимостью использовать в основном дереве фрагментированные A6. Поэтому, переводя RFC 2874 в статус экспериментального, этот документ предполагает, что использование DNAME RR в реверсном дереве будет отменено.

5. Другие проблемы, связанные с DNAME

При использовании DNAME следует учитывать описанные в последующих параграфах аспекты.

5.1. Канонические имена хостов не могут быть ниже владельца DNAME

Имена целей в записях MX, NS, PTR, SRV [RFC2782] должны быть каноническими именами хостов. Это означает невозможность перенаправления CNAME или DNAME в процессе поиска DNS адресных записей хостов. Этот вопрос рассматривается в параграфе 10.3 RFC 2181 [RFC2181] и в параграфе 2.4 RFC 1912 [RFC1912]. Записи SRV рассмотрены на стр. 4 RFC 2782 [RFC2782].

В итоге получается, что имя, указанное в записи PTR не может размещаться ниже DNAME, хотя поиск PTR может включать DNAME. Это относится и к записям NS, SRV, MX. Например, punycode [RFC3492] меняет для зоны использование DNAME, записи NS, MX, SRV и PTR, указывающие эту зону, должны использовать в своих RDATA имена, которые не являются псевдонимами. Тогда требуется, чтобы подстановка DNAME уже была применена к доменным имена в данных MX, NS, PTR, SRV. Это будут канонические имена хостов.

5.2. Динамическое обновление и DNAME

Записи DNAME в зоне можно добавлять, изменять и удалять с помощью транзакций динамического обновления. Добавление в зону DNAME RR закрывает все доменные имена, которые могли существовать пол добавленной DNAME.

Если сообщение динамического обновления пытается добавить DNAME, с именем владельца которой уже связана запись CNAME, сервер **должен** игнорировать DNAME. Если с этим именем уже связана запись DNAME, она заменяется новой DNAME. В остальных случаях запись DNAME добавляется в зону. Если добавляется запись CNAME, с именем владельца которой уже связана запись DNAME, эта запись CNAME **должна** игнорироваться. Аналогичное поведение имеет место и при динамическом обновлении имени владельца CNAME RR [RFC2136].

5.3. DNSSEC и DNAME

В последующих параграфах рассматривается поведение реализаций, поддерживающих DNSSEC и DNAME (синтез).

5.3.1. Подписанные DNAME и синтезированные CNAME без подписи

В любом отклике подписанная DNAME RR указывает нетерминальное перенаправление запроса. В разделе ответов может (не обязательно) быть синтезированная сервером запись CNAME, но такие записи никогда не подписываются. Для валидатора DNSSEC достаточно проверки DNAME RR и корректности синтеза CNAME.

5.3.2. Бит DNAME в битовой карте NSEC

В любом негативно отклике NSEC или NSEC3 [RFC5155] **следует** проверять битовую карту типа, чтобы убедиться в отсутствии записи DNAME, которую можно применить. Если бит DNAME установлен и имя в запросе является субдоменом ближайшего включающего имени, которое заявлено, это указывает, что следовало выполнить подстановку DNAME, но это не было сделано, как задано.

5.3.3. Действенность цепочек DNAME

Отклик может содержать цепочку перенаправлений DNAME и CNAME, которая может завершаться позитивным или негативным (нет имени или данных) откликом. Каждый шаг цепочки ведёт к добавлению записей о ресурсах в раздел ответов или полномочий отклика. Бит AD (Authentic Data - аутентичные данные) может быть установлен лишь при безопасности каждого шага. Если любой из шагов является ложным, вся цепочка становится фальшивой.

5.3.4. Валидаторы должны понимать DNAME

Ниже приведены примеры, показывающие, почему валидаторы DNSSEC **должны** понимать DNAME. В примерах опущены или сокращены записи SOA, NSEC, отвергающие шаблоны, и другие данные, не связанные с обсуждением.

5.3.4.1. Отклик с ошибкой непригодного имени, вызванной DNAME в битовой карте

```
;; Заголовок: QR AA RCODE=3(NXDOMAIN)
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096

;; Вопрос
foo.bar.example.com. IN A
;; Полномочия
bar.example.com. NSEC dub.example.com. A DNAME RRSIG NSEC
bar.example.com. RRSIG NSEC [действительная подпись]
```

Если это полцченный отклик, только понимание того, что бит DNAME в битовой маске NSEC указывает, что foo.bar.example.com нужно перенаправлять по DNAME. Валидатор может увидеть, что это фиктивный ответ (BOGUS) злоумышленника, собравшего имеющиеся записи DNS для создания вносящего путаницу ответа. Если бы бит DNAME не был установлен в показанной выше записи NSEC, ответ был бы подтверждён как отклик об ошибке имени.

5.3.4.2. Действительный отклик об ошибке имени с DNAME в битовой карте

```
;; Заголовок: QR AA RCODE=3(NXDOMAIN)
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096

;; Вопрос
cee.example.com. IN A
;; Полномочия
bar.example.com. NSEC dub.example.com. A DNAME RRSIG NSEC
bar.example.com. RRSIG NSEC [действительная подпись]
```

Этот отклик имеет такие же записи NSEC, как в первом примере, но с таким именем в запросе (cee.example.com), ответ подтверждается, поскольку cee не перенаправляется по DNAME в bar.

5.3.4.3. Отклик с синтезированной записью CNAME

```
;; Заголовок: QR AA RCODE=0(NOERROR)
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096

;; Вопрос
foo.bar.example.com. IN A
;; Ответ
bar.example.com. DNAME bar.example.net.
bar.example.com. RRSIG DNAME [действительная подпись]
foo.bar.example.com. CNAME foo.bar.example.net.
```

Показанный выше отклик включает синтезированную запись CNAME, которая не имеет подписи, поскольку сервер не подписывает онлайн. Такому отклику нельзя доверять, поскольку атакующий может изменить его на foo.bar.example.com CNAME bla.bla.example. Запись DNAME включает подпись, поэтому изменить её не удастся. Валидатор должен проверить подпись DNAME, а затем рекурсивно распознать её для запроса записи A для имени foo.bar.example.net.

6. Примеры использования DNAME в зоне

Ниже приведено несколько примеров использования DNAME в зоне. Примеры не охватывают всех вариантов.

6.1. Переименование организации

Если организация с доменным именем FROBOZZ.EXAMPLE.NET становится частью организации с доменом ACME.EXAMPLE.COM, она может облегчить переход, поместив в старой зоне записи вида

```
frobozz.example.net.  DNAME    frobozz-division.acme.example.com.
                      MX       10       mailhub.acme.example.com.
```

Отклик на расширенный рекурсивный запрос для www.frobozz.example.net будет содержать в разделе ответов запись DNAME, приведённую выше и соответствующие RR для www.frobozz-division.acme.example.com.

Если организация хочет иметь псевдонимы для имён с разным написанием или на другом языке, примени тот же способ. Отметим, что MX RR на вершине зоны не перенаправляется и должна повторяться в целевой зоне. Отметим также, что службы в mailhub и www.frobozz-division.acme.example.com. должны распознавать и обрабатывать эти псевдонимы.

6.2. Бесклассовое делегирование коротких префиксов

Бесклассовую схему делегирования in-addr.arpa [RFC2317] можно расширить на префиксы короче 24 битов с помощью записи DNAME. Например, префикс 192.0.8.0/22 можно делегировать с помощью показанных ниже записей.

```
$ORIGIN 0.192.in-addr.arpa.
8/22    NS      ns.slash-22-holder.example.com.
8       DNAME   8.8/22
9       DNAME   9.8/22
10      DNAME   10.8/22
11      DNAME   11.8/22
```

Типичная запись результирующей реверсной зоны для хоста с адресом 192.0.9.33 может иметь вид

```
$ORIGIN 8/22.0.192.in-addr.arpa.
33.9    PTR     somehost.slash-22-holder.example.com.
```

Замечания в [RFC2317] относительно выбора символа / применимы и здесь.

6.3. Поддержка смены сетевых адресов

Если бы смена адресов IPv4 в сетях происходила часто, поддержку делегирования адресного пространства можно было бы упростить применяя записи DNAME вместо NS, как показано ниже.

```
$ORIGIN new-style.in-addr.arpa.
189.190           DNAME    in-addr.example.net.

$ORIGIN in-addr.example.net.
188               DNAME    in-addr.customer.example.com.

$ORIGIN in-addr.customer.example.
1                 PTR      www.customer.example.com
2                 PTR      mailhub.customer.example.com.
; ...
```

Это позволит сменить адресный блок 190.189.0.0/16, выделенный провайдеру example.net, без необходимости менять данные зоны, описывающие использование этого блока провайдером и его клиентами.

Смена адресов в сетях IPv4 в настоящее время является тяжёлой задачей и обновление DNS является лишь малой частью работы, поэтому ценность приведённой выше схемы невелика. Однако есть надежда, что механизм смены адресов IPv6 будет иным и механизм DNAME может оказаться полезным.

7. Взаимодействие с IANA

Код записи DNAME с десятичным значением 39 исходно включён [RFC2672] в таблице реестра DNS Resource Record (RR) http://www.iana.org/assignments/dns-parameters. Агентство IANA обновило реестр записей о ресурсах DNS для типа 39, указав в нем этот документ.

8. Вопросы безопасности

DNAME перенаправляет запросы, что может влиять на безопасность в зависимости от политики и состояния защиты зоны с DNAME и зоны перенаправления. Для проверяющих распознавателей к результат определяется самым слабым звеном цепочки перенаправлений CNAME и DNAME. Если проверяющий распознаватель воспринимает шаблонные DNAME, возникают проблемы безопасности. Поскольку обработка шаблонных DNAME недетерминирована, а CNAME, подставленные сервером, не имеют подписи, распознаватель может выбрать результат, отличающийся от предусмотренного сервером, и, соответственно, попасть не в тот пункт назначения. Ни в каких случаях не рекомендуется применять записи DNAME с шаблонами [RFC4592]. Проверяющий распознаватель **должен** понимать записи DNAME, согласно [RFC4034]. Иллюстрация этого представлена в примерах параграфа 5.3.4.

9. Благодарности

Авторы документа признательны Matt Larson за начало работы по решению проблем, связанных с типом DNAME RR. Авторы также благодарны Paul Vixie, Ed Lewis, Mark Andrews, Mike StJohns, Niall O'Reilly, Sam Weiler, Alfred Hoenes, Kevin Darcy за рецензии и комментарии к документу.

10. Литература

10.1. Нормативные документы

[RFC1034] Mockapetris, P., "Domain names - concepts and facilities", STD 13, RFC 1034, November 1987.

[RFC1035] Mockapetris, P., "Domain names - implementation and specification", STD 13, RFC 1035, November 1987.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2136] Vixie, P., Thomson, S., Rekhter, Y., and J. Bound, "Dynamic Updates in the Domain Name System (DNS UPDATE)", RFC 2136, April 1997.

[RFC2181] Elz, R. and R. Bush, "Clarifications to the DNS Specification", RFC 2181, July 1997.

[RFC2317] Eidnes, H., de Groot, G., and P. Vixie, "Classless IN-ADDR.ARPA delegation", BCP 20, RFC 2317, March 1998.

[RFC2782] Gulbrandsen, A., Vixie, P., and L. Esibov, "A DNS RR for specifying the location of services (DNS SRV)", RFC 2782, February 2000.

[RFC3597] Gustafsson, A., "Handling of Unknown DNS Resource Record (RR) Types", RFC 3597, September 2003.

[RFC4033] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "DNS Security Introduction and Requirements", RFC 4033, March 2005.

[RFC4034] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Resource Records for the DNS Security Extensions", RFC 4034, March 2005.

[RFC4035] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Protocol Modifications for the DNS Security Extensions", RFC 4035, March 2005.

[RFC4592] Lewis, E., "The Role of Wildcards in the Domain Name System", RFC 4592, July 2006.

[RFC5155] Laurie, B., Sisson, G., Arends, R., and D. Blacka, "DNS Security (DNSSEC) Hashed Authenticated Denial of Existence", RFC 5155, March 2008.

10.2. Дополнительная литература

[RFC1912] Barr, D., "Common DNS Operational and Configuration Errors", RFC 1912, February 1996.

[RFC2672] Crawford, M., "Non-Terminal DNS Name Redirection", RFC 2672, August 1999.

[RFC3363] Bush, R., Durand, A., Fink, B., Gudmundsson, O., and T. Hain, "Representing Internet Protocol version 6 (IPv6) Addresses in the Domain Name System (DNS)", RFC 3363, August 2002.

[RFC3492] Costello, A., "Punycode: A Bootstring encoding of Unicode for Internationalized Domain Names in Applications (IDNA)", RFC 3492, March 2003.

[RFC6434] Jankiewicz, E., Loughney, J., and T. Narten, "IPv6 Node Requirements", RFC 6434, December 2011.

Приложение A. Отличия от RFC 2672

A.1. Изменения в поведении сервера

Ниже перечислены основные изменения в поведении сервера по сравнению с исходной спецификацией DNAME.

- Правила подстановки DNAME уточнены в параграфе 2.2.
- Опция EDNS для сигнализации понимания и сжатия DNAME не была задана и этот документ указывает, что метода сигнализации не существует (параграф 2.5).
- В поле TTL синтезированных CNAME RR устанавливается TTL из DNAME, а не 0 (параграф 3.1).
- Рекурсивные кэширующие серверы **должны** выполнять синтез CNAME от имени клиентов (параграф 3.4).
- Пересмотренный алгоритм сервера представлен в параграфе 3.2.
- Правила для сообщений динамического обновления, добавляющих DNAME или CNAME RR в зону, где уже имеются CNAME или DNAME, детализированы в параграфе 5.2.

A.2. Изменения в поведении клиента

Ниже перечислены основные изменения в поведении клиента по сравнению с исходной спецификацией DNAME.

- Клиенты **должны** быть способны воспринимать синтезированные CNAME RR с TTL = 0 или TTL из DNAME RR, сопровождающей CNAME RR.
- Клиентам с поддержкой DNSSEC **следует** кэшировать DNAME RR и **можно** кэшировать синтезированные CNAME RR, полученные в том же отклике. Таким клиента **следует** также проверять битовую карту типа NSEC/NSEC3, чтобы убедиться в необходимости перенаправления DNAME. Распознаватели DNSSEC **должны** понимать DNAME (параграф 5.3).
- Пересмотренный алгоритм клиента представлен в параграфе 3.4.1.

Адреса авторов

Scott Rose
NIST
100 Bureau Dr.
Gaithersburg, MD 20899
USA
Phone: +1-301-975-8439
Fax: +1-301-975-6238
EMail: scott.rose@nist.gov

Wouter Wijngaards
NLnet Labs
Science Park 140
Amsterdam 1098 XH
The Netherlands
Phone: +31-20-888-4551
EMail: wouter@nlnetlabs.nl

Перевод на русский язык

Николай Малых

nmalykh@protokols.ru