Network Working Group
Request for Comments: 4592
Updates: 1034, 2672
Category: Standards Track

E. Lewis
NeuStar

July 2006

The Role of Wildcards in the Domain Name System

Роль шаблонов в DNS

Статус документа

В этом документе содержится спецификация стандарта для протокола, предложенного сообществу Internet. Документ служит приглашением к дискуссии в целях развития и совершенствования протокола. Текущее состояние стандартизации протокола вы можете узнать из документа Internet Official Protocol Standards (STD 1). Документ может распространяться без ограничений.

Аннотация

Этот документ обновляет определение шаблонов (wildcard) RFC 1034. Изменено взаимодействие CNAME с шаблонами, исключено условие ошибки, а также изменён текст некоторых определений, важных для шаблонов. Цель заключалась не в изменении шаблонов, а лишь в уточнении определения из RFC 1034.

Оглавление

1. Введение

В параграфах 4.3.2 и 4.3.3 RFC 1034 [RFC1034] описано создание ответов из специальных записей о ресурсах (resource record или RR), называемых шаблонами (wildcard). Определение в RFC 1034 неполно и оказалось путанным. В этом документе описывается создание шаблонов, дополняется их обсуждение и вносятся некоторые правки для

устранения несоответствий, приводящих к проблемам функциональной совместимости. Описание не расширяет спектр услуг, предусмотренных исходным определением.

Сохраняя дух и стиль исходных документов, этот документ не задаёт правил для реализаций DNS в части шаблонов. Намерение заключается лишь в описании того, что требуется для обеспечения функциональной совместимости без ограничения выбора для реализаций. Кроме того, учитывается необходимость минимизировать проблемы совместимости с прежними версиями, которые следуют определению из RFC 1034.

Документ посвящён концепции шаблонов, заданной в RFC 1034. Не принимается каких-либо допущений в части дополнительных средств синтеза RRSet и не обсуждаются альтернативы.

1.1. Мотивация

Многие реализации DNS так или иначе отклоняются от исходного определения шаблонов. Хотя очевидна необходимость уточнения исходного определения в свете отмеченного выше, толчком к созданию этого документа послужила потребность в разработке защитных расширений DNS [RFC4033]. Нечёткое определение шаблонов привело к путанице при создании аутентифицированных отказов.

Этот документ вносит лишь ограниченные изменения, документируя лишь те, которые признаны необходимыми на основе опыта, и сохраняя максимально возможную близость к исходному документу. Для подчёркивания того, что этот документ лишь разъясняет и уточняет, а не переопределяет шаблоны, приведены соответствующие фрагменты RFC 1034, позволяющие сравнить прежний и новый текст.

1.2. Исходное определение

Определение понятия шаблон включает документация алгоритма, с помощью которого сервер имён готовит отклик (параграф 4.3.2 в RFC 1034), и способ идентификации того, что запись или набор записей являются синтетическими данными (параграф 4.3.3).

Определение термина «шаблон» (wildcard) в параграфе 4.3.3 RFC 1034 приведено ниже.

> В предыдущем алгоритме использовалась специальная трактовка записей RR, у которых имена владельца начинаются с метки «*». Такие RR называют шаблонами. Шаблонные RR можно представлять, как инструкцию по синтезированию RR. При выполнении соответствующих условий сервер имён создаёт записи RR, для которых имя владельца совпадает с именем в запросе, а содержимое берётся из шаблонных RR.

Этот фрагмент следует алгоритму, в котором термин «шаблон» применён впервые. В определении понятие шаблона относится к записям о ресурсах, а при иных вариантах применения - к доменным именам, и служит для описания практики применения шаблонов при создании ответов. Отсюда ясно, что для обсуждения шаблонов требуется задать чёткую и недвусмысленную терминологию.

Упоминание использования шаблонов при подготовке отклика содержится в п. 3.c параграфа 4.3.2 (Алгоритм) в RFC 1034. В описании алгоритма термин wildcard не применяется и вместо него используется термин «метка *». Часть алгоритма, относящаяся к шаблонам, подробно разбирается в разделе 3 этого документа, а ниже приведён соответствующий фрагмент из параграфа «Алгоритм» в RFC 1034.

> c. Если для какой-либо метки сопоставление невозможно (т. е., соответствующей метки не существует), проверяется существование метки «*».

Областью действия этого документа является определение шаблонов в RFC 1034 и влияние обновлений документов, таких как DNS Security (DNSSEC). Дополнительные варианты синтеза ответов не рассматриваются (обратите внимание, что ссылок здесь не указанно, поскольку не известно ни одного документа, описывающего дополнительные схемы, хотя в почтовых конференциях они упоминались).

1.3. План документа

Документ решает 3 основных задачи:

- определение новых терминов;
- внесение незначительных изменений для исключения противоречивых понятий;
- описание действий при наличии шаблонов в некоторых записях о ресурсах.

1.3.1. Новые термины

Чтобы помочь разобраться, какие записи о ресурсах являются шаблонными, в параграфе 2.1.1 определяются два термина - «метка-звёздочка» (asterisk label) и «шаблонное доменное имя» (wildcard domain name). Для разъяснения роли шаблонов в работе алгоритма сервера имён из параграфа 4.3.2 в RFC 1034 в параграфе 3.3.1 определены термины «источник синтеза» (source of synthesis) и «ближайший включающий» (closest encloser). Совпадение меток (label match) определено в параграфе 3.2.

Новые термины служат для того, чтобы сделать обсуждение шаблонов более понятным, т прямого влияния на реализацию не оказывают.

1.3.2. Изменённый текст

Внешне изменено определение существования (existence). Это изменение не будет важно для реализаций и внесено для уточнения описаний. Изменение представлено в параграфе 2.2.3.

Представляется, что параграф 4.3.3 в RFC 1034 запрещает использовать две метки * имени владельца шаблона. Данные документ полностью снимает это ограничение. Изменение и его результаты указаны в параграфе 2.1.3.

Действия в случае, когда источник синтеза владеет CNAME RR, изменены на зеркальные, если в точности совпадающее имя владеет CNAME RR. Это дополняет п.3.c в параграфе 4.3.2 RFC 1034 и приведено в параграфе 3.3.3.

На реализации оказывает влияние лишь последнее изменение. Определение существования не меняет протокол, а изменение ограничений для имён вряд ли будет оказывать влияние, поскольку в RFC 1034 нет указаний, когда применять эти ограничения.

1.3.3. Рассмотрение специальных типов

В этом документе описывается семантика шаблонных RRSet для «интересных» типов, а также пустых нетерминальных шаблонов. Понимание этих ситуаций в контексте шаблонов (подстановок) было «затуманено», поскольку эти типы требуют особой обработки, когда они являются результатом точного совпадения. Это рассматривается в разделе 4. Приведённые обсуждения не влияют на реализацию, они охватывают имеющиеся знания о типах, но с большей детализацией.

1.4. Терминология стандартов

В этом документе не применяются уровни требований из [RFC2119]. Цитаты из RFC 1034 выделены смещением текста вправо. Ссылки на параграф 4.3.2 указывают параграф 4.3.2 Алгоритм в RFC 1034.

2. Синтаксис шаблонов

Для шаблонов применяется тот же синтаксис, как для других записей о ресурсах DNS, во всех классах и типах. Важной характеристикой является лишь имя владельца.

Поскольку шаблоны кодируются как записи о ресурсах с особыми именами, они включаются в перенос зон (включая инкрементный [RFC1995]), как обычные записи о ресурсах. Это свойство недооценивалось, пока в почтовых конференциях не прошло обсуждение других подходов к шаблонам.

2.1. Идентификация шаблонов

Для более точного описания шаблонов обсуждение начинается с доменных имён, появляющихся в качестве владельцев. Для этого нужна два новых термина «метка-звёздочка» (asterisk label) и «шаблонное доменное имя».

*2.1.1. Шаблонные доменные имена и метка **

Шаблонное доменное имя определено как имеющее начальную (левую или наименее значимую) метку в формате

```
0000 0001 0010 1010 (двоичный) = 0x01 0x2a (шестнадцатеричный)
```

Первый октет - это обычный тип и размер метки (1), а второй содержит код ASCII [RFC20] для символа *. Описательным именем такой метки служит asterisk label (метка-звёздочка).

В RFC 1034 шаблон определён как «запись о ресурсе, принадлежащая шаблонному доменному имени».

*2.1.2. * и другие символы*

Никакие значения меток, кроме указанного в параграфе 2.1.1, не применяются в качестве метки-звёздочки и имена меток, начинающиеся с другого символа, не могут быть именем шаблона. Такие метки, как the* и **, не являются метками-звёздочками и не могут служить началом шаблонных доменных имён.

2.1.3. Нетерминальные шаблонные доменные имена

В параграфе 4.3.3 сказано:

> ... Имя владельца шаблонной RR имеет форму *.<anydomain>, где <anydomain> может представлять собой любое доменное имя. В <anydomain> не следует включать другие метки «*» ...

Это ограничение отменяется. Исходная документация для него неполна, а ограничение не имеет смысла, как показал опыт эксплуатации.

Возможны три причины введения этого ограничения, но ни одну из них время не подтвердило. Одна из причин состоит в том, что ограничение подразумевает отсутствие субдоменов с шаблонами в доменном имени, но в указанной форме ограничение не препятствует использованию таких имён, как example.*.example.. Вторая причина заключается в том, что шаблонные доменные имена не должны быть пустыми нетерминальными элементами, но они не нарушают работу алгоритма из параграфа 4.3.2. «Вложенные» шаблонные доменные имена перестают быть неоднозначными после введения концепции ближайшего включающего (имени).

Шаблонные доменные имена могут иметь субдомены. Не требуется проверять субдомены на предмет наличия ещё одного символа * в каком-либо субдомене.

Шаблонные доменные имена могут быть пустыми нетерминальными элементами (см. ниже). В этом случае поиск, где встречается такое имя завершится как при любом совпадении с пустым нетерминальным элементом.

2.2. Правила существования

В определении шаблонов применяется понятие существования доменных имён. В параграфе 4.3.3 RFC 1034 сказано:

> Шаблоны RR не применимы в тех случаях, когда:
>
> - ...
> - имя в запросе или имя между шаблонным доменом и именем в запросе определённо существует ...

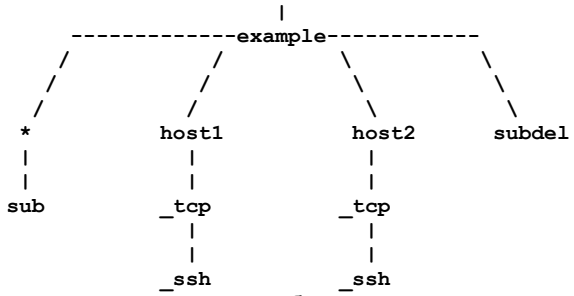
Поэтому понятие существования важно для понимания шаблонов. К сожалению, определение существования в RFC 1034 нечетко, поэтому в параграфах 2.2.2 и 2.2.3 оно рассматривается ещё раз.

2.2.1. Пример

Для иллюстрации понятия существования рассмотрим приведённую ниже полную зону.

```
$ORIGIN example.
example.                 3600 IN  SOA   <SOA RDATA>
example.                 3600     NS    ns.example.com.
example.                 3600     NS    ns.example.net.
*.example.               3600     TXT   "this is a wildcard"
*.example.               3600     MX    10 host1.example.
sub.*.example.           3600     TXT   "this is not a wildcard"
host1.example.           3600     A     192.0.2.1
_ssh._tcp.host1.example. 3600     SRV   <SRV RDATA>
_ssh._tcp.host2.example. 3600     SRV   <SRV RDATA>
subdel.example.          3600     NS    ns.example.com.
subdel.example.          3600     NS    ns.example.net.
```

Полезно рассмотреть также дерево доменных имён, показанное на рисунке.



Приведённые ниже запросы синтезированы из одного из шаблонов в зоне.

`QNAME=host3.example. QTYPE=MX, QCLASS=IN`

Ответом будет host3.example. IN MX ...

`QNAME=host3.example. QTYPE=A, QCLASS=IN`

Ответ будет указывать отсутствие ошибок и данных (no error, but no data), поскольку нет набора A RR в *.example.

`QNAME=foo.bar.example. QTYPE=TXT, QCLASS=IN`

Ответом будет foo.bar.example. IN TXT …, поскольку bar.example. не существует, но шаблон имеется.

Приведённые ниже отклики[1] не будут синтезированы из одного из шаблонов в зоне.

`QNAME=host1.example., QTYPE=MX, QCLASS=IN`

поскольку host1.example. существует.

`QNAME=sub.*.example., QTYPE=MX, QCLASS=IN`

поскольку sub.*.example. существует.

`QNAME=_telnet._tcp.host1.example., QTYPE=SRV, QCLASS=IN`

поскольку because _tcp.host1.example. существует (без данных).

`QNAME=host.subdel.example., QTYPE=A, QCLASS=IN`

поскольку subdel.example. существует (и является срезом зоны).

`QNAME=ghost.*.example., QTYPE=MX, QCLASS=IN`

поскольку *.example. существует.

Последний пример демонстрирует распространённое заблуждение о шаблонах. Шаблон «блокирует себя» в том смысле, что он не соответствует своим субдоменам. Т. е. *.example. не соответствует именам в зоне example. и не соответствует именам ниже *.example. Для охвата имён ниже *.example. требуется другое шаблонное доменное имя *.*.example., которое охватывает все субдомены, кроме своих.

2.2.2. Пустые нетерминальные элементы

Пустые нетерминальные элементы [параграф 7.16 в RFC2136] - это доменные имена, в которых нет записей о ресурсах, но имеются субдомены. В параграфе 2.2.1 _tcp.host1.example. является примером пустого нетерминального имени. Эти имена введены в тексте параграфа 3.1 RFC 1034:

> Пространство имён имеет структуру дерева. Каждый узел и ветвь (лист) дерева соответствуют набору ресурсов (который может быть пустым). DNS не различает внутренние узлы и ветви и здесь термин узел относится к обоим.

Слова «может быть пустым» в скобках указывают, что пустые нетерминальные элементы признаются явно и существуют.

Педантичное прочтение приведённого выше абзаца может привести к допущению существования всех возможных доменов, вплоть до предложенного ограничения размера доменного имени 255 октетами [RFC1035]. Например, www.example. может иметь A RR и, насколько это возможно практически, быть листом дерева домена. Но это может означать, что существует также sub.www.example., хотя и без данных. Таким образом, существуют все возможные домены вниз от корня.

Поскольку RFC 1034 в параграфе 4.3.1 определяет также «ошибку authoritative name, указывающая на то, что имени не существует», это, очевидно, не является целью исходного определения, что оправдывает необходимость обновлённого определения в следующем параграфе.

[1] В оригинале ошибочно сказано о запросах, см. https://www.rfc-editor.org/errata/eid46. *Прим. перев.*

2.2.3. Другое определение существования

Формулировка RFC 1034 заменяется приведёнными ниже абзацами.

> Пространство имён является древовидной структурой. Узлы дерева владеют хотя бы одним RRSet и/или имеют потомков, коллективно владеющих хотя бы одним RRSet. Узел может существовать без RRSet лишь при наличии у него потомков, владеющих RRSet, - такой узел называется пустым нетерминальным узлом.
>
> Узел без потомков является листом. Пустых узлов-листьев не существует.

Отметим, что на границе зоны доменное имя владеет данными, включая набор NS RR. В делегирующей зоне набор NS RR не является полномочным, но в данном случае это не имеет значения. Доменное имя владеет данными, следовательно, оно существует.

2.3. Когда шаблонное доменное имя не является специальным?

Когда доменное имя с шаблоном появляется в разделе запроса в сообщении, специальной обработки не происходит. Метка * в имени запроса соответствует лишь одной метке * в существующем дереве зоны, если применяется алгоритм из параграфа 4.3.2.

Когда шаблонное доменное имя появляется в данных записи о ресурсе, специальной обработки на происходит. Метка * в контексте буквально означает просто звёздочку.

3. Влияние шаблонных доменных имён на отклик

В параграфе 4.3.2 RFC 1034 описано влияние шаблонов на генерацию откликов. Здесь описывается алгоритм, которому сервер следует при создании отклика. Пункт 3.c этого алгоритма задаёт поведение для шаблонов.

Алгоритм из параграфа 4.3.2 не является псевдокодом, т. е. его не обязательно выполнять строго по порядку. Это лишь предлагаемый способ реализации требований. Поэтому подпункты a, b и c пункта 3 не обязательно реализовать в указанном порядке, если результат реализации кода соответствует спецификации протокола.

3.1. Этап 2

В параграфе 4.3.2 сказано:

> 2. Поиск доступных зон для зоны, которая является ближайшим предком QNAME. При нахождении такой зоны переход к п. 3, иначе - п. 4.

На этом этапе выбирается зона, наиболее подходящая для отклика. Важность этого этапа определяется тем, что этап 3 целиком выполняется в рамках одной зоны. Это важно при рассмотрении вопроса о возможности использования SOA RR для синтеза.

3.2. Этап 3

Этап 3 разделен на 3 части - a, b и c. Начало этапа очень важно и требует разъяснения.

> 3. Начало поиска соответствия (метка за меткой) в зоне. Процесс поиска может прерываться в нескольких случаях:

Слово «соответствие» здесь означает совпадение меток. В основе концепции лежит представление зоны в форме дерева существующих имён. Имя в запросе рассматривается как упорядоченная последовательность меток - путь от корня к владельцу желаемых данных (см. третий абзац в параграфе 3.1 RFC 1034).

Процесс сопоставления метки с именем в запросе завершается в точности одним из трёх вариантов (a, b, c) - имя найдено, находится ниже точки среза или не найдено. После выбора одного из вариантов остальные уже не рассматриваются (например, не следует выбирать п. c, а затем менять путь выполнения, чтобы закончить в п. b). Процесс сопоставления меток выполняется независимо от типа запроса (QTYPE).

Пункты a и b здесь не рассматриваются, поскольку они не связаны с синтезом записей. Пункт a относится к точному совпадению, приводящему к ответу, а пункт b' is a referral.

3.3. Пункт c

Контекст п. c заключается в том, что процесс сопоставления меток из имени в запросе приводит к ситуации, когда в дереве нет соответствующей метки (как будто поиск «упал с дерева» - fallen off the tree).

> c Если для какой-либо метки сопоставление невозможно (т. е., соответствующей метки не существует), проверяется существование метки «*».

Чтобы помочь в описании процесса поиска «существования метки *» был введён термин, указывающий последний соответствующий домен (узел). Он называется «ближайшим включающим» (closest encloser).

3.3.1. Ближайший включающий узел и источник синтеза

Ближайшим включающим является узел в дереве зоны имеющихся доменных имён, который имеет наибольшее совпадение меток с именем в запросе (последовательно вниз от корневой метки). Каждое совпадение является совпадением меток и метки расположены в одном порядке.

Ближайший включающий узел по определению является существующим в зоне узлом. Это может быть пустой нетерминальный узел и даже само доменное имя с шаблоном. Ни в коем случае нельзя использовать ближайший включающий узел при синтезе записей для текущего запроса.

Источник синтеза определяется в контексте процесса запроса как доменное имя с шаблоном, являющееся непосредственным потомком ближайшего включающего узла, при условии наличия такого доменного имени с шаблоном. Непосредственный потомок означает, что имя источника синтеза имеет вид

```
<asterisk label>.<closest encloser>.
```

Источник синтеза не гарантирует наличия RRSet для синтеза и может быть пустым нетерминальным узлом. Если источника синтеза не существует (нет в дереве домена), синтез по шаблону не выполняется и поиск альтернатив не производится.

Важно то, что для любого данного процесса поиска существует не более 1 места, где можно получить синтетические записи с шаблонами. Если источника синтеза нет, поиск прерывается без попыток найти другие шаблонные записи.

3.3.2. Примеры ближайшего включающего узла и источника синтеза

Для иллюстрации в таблице показаны на основе примера из параграфа 2.2.1 значения QNAME, ближайшие включающие имена и источники синтеза.

QNAME	*Ближайшее включающее имя*	*Источник синтеза*
host3.example.	example.	*.example.
_telnet._tcp.host1.example.	_tcp.host1.example.	нет
_dns._udp.host2.example.	host2.example.	нет
_telnet._tcp.host3.example.	example.	*.example.
_chat._udp.host3.example.	example.	*.example.
foobar.*.example.	*.example.	нет

3.3.3. Сопоставление типа

В RFC 1034 п. c завершается приведённым ниже текстом.

> Если метки «*» не существует, проверяется является ли искомое имя исходным QNAME в запросе или именем, полученным через CNAME. Если имя является исходным, в отклике указывается ошибка authoritative name и поиск завершается. В противном случае поиск заканчивается без констатации ошибки.
>
> Если метка «*» существует, записи RR на данном узле сопоставляются с QTYPE. При обнаружении соответствий записи копируются в раздел ответа, но в качестве владельца RR указывается QNAME, а не узел с меткой «*». Переход к п. 6.

Во втором абзаце рассматривается роль QTYPE в процессе поиска. На основе отзывов на реализации и сходстве пп. a и c этот абзац изменён путём добавления приведённого ниже текста в п. c перед инструкцией перехода к п. 6.

> Если данные в источнике синтеза являются CNAME, а QTYPE не соответствует CNAME, в раздел ответов копируется CNAME RR с заменой имени владельца на QNAME, заменой QNAME на каноническое имя в CNAME RR и возвратом к п. 1.

По сути, это тот же текст, что и в п. a для обработки CNAME RRSet.

4. Рассмотрение особых типов

В разделах 2 и 3 этого документа обсуждается синтез подстановок применительно именам в дереве домена и не учитывается влияние типов. В этом разделе рассматривается влияние шаблонов определённых типов с акцентом на более сложные для понимания типы, к каковым относятся SOA, NS, CNAME, DNAME, SRV, DS, NSEC, RRSIG, и none (пустые нетерминальные имена доменов с шаблоном).

4.1. SOA RRSet доменного имени с шаблоном

Шаблонное доменное имя, владеющее SOA RRSet, означает, что домен находится в корне зоны (вершина - apex). Домен не может быть источником синтеза, поскольку он, по определению, является узлом-потомком (ближайшего включающего узла) и вершина зоны размещается наверху зоны (zone apex is at the top of the zone).

Хотя доменное имя с шаблоном, владеющее SOA RRSet, не может быть источником синтеза, нет причин запрещать ему владеть SOA RRSet. Пример такой зоны приведён ниже.

```
$ORIGIN *.example.
@               3600 IN  SOA   <SOA RDATA>
                3600     NS    ns1.example.com.
                3600     NS    ns1.example.net.
www             3600     TXT   "the www txt record"
```

Запрос записи TXT для www.*.example. найдёт ответ the www txt record. Метка * становится значимой лишь при использовании п. 3.c из параграфа 4.3.2.

Чтобы это работало, требуется делегирование в родительской зоне example. (см. следующий параграф).

4.2. NS RRSet доменного имени с шаблоном

С появлением DNSSEC [RFC4033, RFC4034, RFC4035] семантика доменного имени с шаблоном, владеющего NS RRSet стала плохо определённой. Дилемма связана с конфликтом правил синтеза из п. c и тем фактом, что в результате синтезируется запись, для которой зона не имеет полномочий. В зоне, подписанной DNSSEC, механизмы управления подписями (создание и включение в сообщение) становятся неясными.

Основные момент обсуждения этой темы рабочей группой кратко изложены в параграфе 4.2.1. В результате обсуждения не было дано определения доменного имени с шаблоном, владеющего NS RRSet. Семантика останется неопределённой, по не возникнет явная необходимость такого определения и не будет задано направление дальнейших действий. На практике включение в зону шаблонных NS RRSet не одобряется, но и не запрещено.

4.2.1. Отброшенные принципы

До появления DNSSEC шаблонные доменные имена, владеющие NS RRSet представлялись работоспособными и встречались в системах, использующих реализации с поддержкой этого. Продолжать допустимость таких имён в спецификации DNSSEC нецелесообразно. Причина заключается в том, что синтез NS RRSet выполняется в зоне,

которая передала ответственность за имя. Такой «неуполномоченный» синтез не вызывает проблем для базового протокола DNS, но с принятой в DNSSEC моделью проверки подлинности DNS возникают проблемы.

Прямой запрет использования шаблонов типа NS тоже несостоятелен, поскольку в протоколе DNS не определена обработка «недействительных» данных. Реализация может отказаться загружать зону, но протокол этого не задаёт. Отсутствие определения осложняется необходимостью поддержки динамических обновлений [RFC2136] и переноса зон, а также загрузки на первичном сервере. Нужно также учитывать случаи, когда клиент (распознаватель, кэширующий сервер) получает в отклике шаблон типа NS.

С учётом сложности полного определения способов запрета таких записей, работа с имеющимися реализациями, которые разрешают такие записи, создаёт сегодня дополнительные проблемы. Имеются случаи использования доменных имён с шаблонами, владеющих NS RRSet.

Один из предложенных компромиссов предусматривал переопределение шаблонов типа NS, чтобы они не использовались при синтезе, но это не было принято, поскольку требовало существенного изменения работы по подписанию и проверке DNSSEC (DNSSEC отлавливает неполномочные данные).

Поскольку чёткого согласия по решению отмеченной дилеммы не было достигнуто и ясно, что шаблоны типа NS на практике являются большой редкостью, лучшим вариантом будет оставить этот вопрос открытым до поры.

4.3. CNAME RRSet доменного имени с шаблоном

Проблема с CNAME RRSet, принадлежащим доменному имени с шаблоном, побудила внести изменение (см. параграф 3.3.3) в последний абзац п. 3c алгоритма из параграфа 4.3.2.

4.4. DNAME RRSet доменного имени с шаблоном

Принадлежность DNAME [RFC2672] RRSet доменному имени с шаблоном представляет угрозу согласованности DNS и таких ситуаций следует избегать или отвергнуть их совсем. Такой набор DNAME RRSet представляет недетерминированный синтез правил, передаваемых в различные кэши. По мере непредсказуемого поступления с кэши разных правил согласованность кэшей теряется (слова «по мере поступления» здесь относятся к хранению в кэше записей, полученных в откликах рекурсивных или итеративных серверов). Предположим, например, что один кэш, отвечающий на рекурсивный запрос, получит запись

```
a.b.example. DNAME foo.bar.example.net.
```

а другой получит

```
b.example.  DNAME foo.bar.example.net.
```

созданные полномочным сервером из записи

```
*.example. DNAME foo.bar.example.net.
```

В спецификации DNAME нет чёткого указания о применении кэшированных записей DNAME для перезаписи запросов. В некоторых интерпретациях такая запись происходит, в других - нет. Если допустить возможность перезаписи, запросы для sub.a.b.example. A могут быть переписаны как sub.foo.bar.example.tld. A первым кэширующим сервером и как sub.a.foo.bar.example.tld. A - последующим. Согласованность теряется с кошмарным результатом.

Ещё одна рекомендация избегать применения шаблонных записей DNAME связана с наблюдением, что такая запись может создавать DNAME, принадлежащую sub.foo.bar.example. И foo.bar.example. В определении DNAME есть ограничение, в соответствии с которым не может существовать доменов ниже домена владельца DNAME, поэтому шаблонных записей DNAME следует избегать.

4.5. SRV RRSet доменного имени с шаблоном

Определение SRV RRset в RFC 2782 [RFC2782] содержит путаницу с термином Name (имя), как показано ниже.

> Формат SRV RR
>
> ...
>
> _Service._Proto.Name TTL Class SRV Priority Weight Port Target
>
> ...
>
> Имя (Name)
>
> Домен, на который указывает эта запись RR. Запись SRV RR уникальна в том, что искомое имя не является именем этой записи и пример в конце наглядно показывает это.

Не следует путать Name с именем владельца. Т. е. после удаления меток _Service и _Proto из имени владельца SRV RRSet оставшаяся часть может быть доменным именем с шаблоном, но это несущественно для SRV RRSet. Например, если запись SRV имеет вид

```
_foo._udp.*.example. 10800 IN SRV 0 1 9 old-slow-box.example.
```

.example является доменным именем с шаблоном и хотя это Name для записи SRV RR, значение не будет владельцем (доменного имени). Владельцем будет _foo._udp..example. - доменное имя без шаблона.

Запрос SRV RRSet для _foo._udp.bar.example. (класс IN) приведёт к совпадению с именем *.example. (в предположении отсутствия bar.example.), а не с показанной записью SRV. Если в *.example. Нет SRV RRSet, раздел ответов будет отражать это (будет пустым или CNAME RRset).

Путаница, вероятно, связана со смешением спецификации SRV RR и описания «примера использования».

4.6. DS RRSet доменного имени с шаблоном

Набор DS RRSet, принадлежащий доменному имени с шаблоном не имеет смысла и не приносит вреда. Это утверждение сделано в контексте неопределённости NS RRSet доменного имени с шаблоном. В точке без

делегирования DS RRSet не имеет значения (DNSKEY RRSet не будет использоваться для проверки DNSSEC). При наличии синтезированного DS RRSet он сам по себе не будет полезен, поскольку он существует в точке делегировани.

4.7. NSEC RRSet доменного имени с шаблоном

Шаблонные имена доменов в зоне с подписью DNSSEC будут иметь NSEC RRSet. Синтез таких записей будет выполняться лишь при точном соответствии запроса записи. Синтезированные NSEC RR не нанесут вреда, поскольку они не будут использоваться в негативном кэшировании или при генерации негативных откликов [RFC2308].

4.8. RRSIG доменного имени с шаблоном

Записи RRSIG будут присутствовать в шаблонном доменном имени в подписанной зоне и будут синтезироваться вместе с данными, искомыми запросом. Синтезированное имя владельца не вызывает проблем, поскольку число меток в RRSIG укажет проверяющему коду, что его следует игнорировать.

4.9. Пустое нетерминальное доменное имя с шаблоном

Если источником синтеза является пустое нетерминальное имя, отклик будет указывать отсутствие ошибки в коде возврата и не будут включать RRSet в разделе ответов.

5. Вопросы безопасности

Этот документ уточняет спецификации для увеличения вероятности добавления защиты в DNS. Функциональных дополнений документ не включает и лишь уточняет, что считается корректным для белее предсказуемой работы, повышения уровня безопасности и расширения DNS.

6. Литература

6.1. Нормативные документы

[RFC20] Cerf, V., "ASCII format for network interchange", RFC 20, October 1969.

[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.

[RFC1995] Ohta, M., "Incremental Zone Transfer in DNS", RFC 1995, August 1996.

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

[RFC2308] Andrews, M., "Negative Caching of DNS Queries (DNS NCACHE)", RFC 2308, March 1998.

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

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

[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.

6.2. Дополнительная литература

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

7. Вклад в разработку документа

Этот документ представляет работу большой группы и редактор лишь зафиксировал коллективный результат.

Комментарии к документу можно направлять редактору или в почтовую конференцию DNSEXT по адресу namedroppers@ops.ietf.org.

Адрес редактора

Edward Lewis
NeuStar
46000 Center Oak Plaza
Sterling, VA
20166, US
Phone: +1-571-434-5468
EMail: ed.lewis@neustar.biz

Полное заявление авторских прав

Интеллектуальная собственность

IETF не принимает какой-либо позиции в отношении действительности или объема каких-либо прав интеллектуальной собственности (Intellectual Property Rights или IPR) или иных прав, которые, как может быть заявлено, относятся к реализации или использованию описанной в этом документе технологии, или степени, в которой любая лицензия, по которой права могут или не могут быть доступны, не заявляется также применение каких-либо усилий для определения таких прав. Сведения о процедурах IETF в отношении прав в документах RFC можно найти в BCP 78 и BCP 79.

Копии раскрытия IPR, предоставленные секретариату IETF, и любые гарантии доступности лицензий, а также результаты попыток получить общую лицензию или право на использование таких прав собственности разработчиками или пользователями этой спецификации, можно получить из сетевого репозитория IETF IPR по ссылке http://www.ietf.org/ipr.

IETF предлагает любой заинтересованной стороне обратить внимание на авторские права, патенты или использование патентов, а также иные права собственности, которые могут потребоваться для реализации этого стандарта. Информацию следует направлять в IETF по адресу ietf-ipr@ietf.org.

Подтверждение

Финансирование функций RFC Editor обеспечено IETF Administrative Support Activity (IASA).

Перевод на русский язык

Николай Малых

nmalykh@protokols.ru