Internet Engineering Task Force (IETF) E. Lewis
Request for Comments: 5936 NeuStar, Inc.
Updates: 1034, 1035 A. Hoenes, Ed.
Category: Standards Track TR-Sys
ISSN: 2070-1721 June 2010

Протокол переноса зон DNS (AXFR)

DNS Zone Transfer Protocol (AXFR)

Тезисы

Стандартные средства протокола DNS[1] для поддержки согласованности уполномоченных серверов зон включают три механизма. Уполномоченный перенос AXFR[2] является одним из механизмов, определенных в RFC 1034 и RFC 1035.

Определение AXFR оказалось недостаточно детализировано, что заставляло разработчиков реализаций протокола вносить свои допущения, осложняющие взаимодействие. Тем нечто здесь дано точное определение механизма взаимодействия AXFR.

Статус документа

Этот документ содержит проект стандарта Internet (Internet Standards Track).

Документ является результатом работы IETF[3] и представляет собой согласованное мнение членов (сообщества) IETF. Документ был представлен для публичного обсуждения и одобрен для публикации IESG[4]. Дополнительную информацию о стандартах Internet можно найти в разделе 2 документа RFC 5741.

Информацию о текущем состоянии этого документа, обнаруженных ошибках и способах обратной связи можно найти по ссылке http://www.rfc-editor.org/info/rfc5936.

Оглавление

1. Введение....2
1.1. Определения терминов....2
1.2. Сфера действия документа....2
1.3. Контекст....3
1.4. Связь с исходной спецификацией AXFR....3
2. Сообщения AXFR....3
2.1. Запрос AXFR....4
2.1.1. Значения заголовка....4
2.1.2. Раздел Question....5
2.1.3. Раздел Answer....5
2.1.4. Раздел Authority....5
2.1.5. Раздел Additional....5
2.2. Отклик AXFR....5
2.2.1. Значения заголовка....6
2.2.2. Раздел Question....7

[1]Domain Name System - система доменных имен.
[2]Authoritative Transfer.
[3]Internet Engineering Task Force - комиссия по решению инженерных задач Internet.
[4]Internet Engineering Steering Group - комиссия по инженерным разработкам Internet.

2.2.3. Раздел Answer....7
2.2.4. Раздел Authority....7
2.2.5. Раздел Additional....7
2.3. Разрыв соединения TCP....7
3. Содержимое зоны....7
3.1. Включаемые записи....7
3.2. Записи Delegation....7
3.3. Склеивающие записи....8
3.4. Сжатие имен....9
3.5. Скрытые имена....9
4. Транспорт....9
4.1. TCP....9
4.1.1. Клиент AXFR - TCP....10
4.1.2. Сервер AXFR - TCP....10
4.2. UDP....10
5. Проверка полномочий....10
6. Целостность зоны....11
7. Совместимость с ранними версиями....11
7.1. Сервер....11
7.2. Клиент....11
8. Вопросы безопасности....11
9. Согласование с IANA....11
10. Поддержка других языков....12
11. Благодарности....12
12. Литература....12
12.1. Нормативные документы....12
12.2. Дополнительная литература....13

1. Введение

Стандарт DNS для поддержки согласованности между серверами зон включает три элемента. Уполномоченный перенос (AXFR) определен в документах Domain Names - Concepts and Facilities [RFC1034] (далее, RFC 1034) и Domain Names - Implementation and Specification [RFC1035] (далее, 1035). Перенос изменений в зоне (IXFR[1]) определен в документе Incremental Zone Transfer in DNS [RFC1995]. Механизм для своевременного уведомления о внесенных в зону изменениях (NOTIFY) определен в документе Mechanism for Prompt Notification of Zone Changes (DNS NOTIFY) [RFC1996]. Целью этих механизмов является обеспечение набора серверов DNS, являющихся уполномоченными для данной зоны.

В этом документе заново дается спецификация механизма AXFR, широко используемого в Internet, с учетом современных требований к стандартам Internet. Следовательно, данный документ является обновлением RFC 1034 b RFC 1035.

1.1. Определения терминов

Ключевые слова **необходимо** (MUST), **недопустимо** (MUST NOT), **требуется** (REQUIRED), **нужно** (SHALL), **не нужно** (SHALL NOT), **следует** (SHOULD), **не следует** (SHOULD NOT), **рекомендуется** (RECOMMENDED), **возможно** (MAY), **необязательно** (OPTIONAL) в данном документе должны интерпретироваться в соответствии с документом «Key words for use in RFCs to Indicate Requirement Levels» [BCP14].

Термины «новый/новее» и «старый/старше» применительно к DNS относятся к реализациям, выпущенным после и до публикации данного документа, соответственно.

Термин «реализация DNS общего назначения» относится к программам DNS, разработанным для повсеместного использования. К таким программам относятся преобразователи (resolver) и серверы, свободно распространяющиеся в форме библиотек или автономных приложений. К таким программам относятся также фирменные (proprietary) реализации, используемые только для поддержки предлагаемых услуг DNS.

Термин «заказная реализация DNS» относится к специализированным реализациям DNS. Такие реализации включают программы, использующие сообщения DNS в формате, не соответствующем всему диапазону функциональности DNS.

Термины «сессия AXFR», «сервер AXFR» и «клиент AXFR» определены в первом параграфе раздела 2, после описания контекста.

1.2. Сфера действия документа

Полномочные серверы имен для данной зоны могут использовать различные механизмы для обеспечения согласованности содержимого обслуживаемых серверами зон. Например, существуют реализации DNS, которые собирают ответы из данных, хранящихся в реляционных базах данных (а не в файлах зон) и применяют не относящиеся к DNS механизмы синхронизации экземпляров баз данных. Некоторые из таких решений (не-DNS) обеспечивают тот или иной способ взаимодействия с другими серверами. Однако только механизмы AXFR, IXFR и NOTIFY определены для протокола DNS в качестве механизмов обеспечения согласованности множества серверов имен и только эти механизмы стандартизованы IETF.

Этот документ не относится к несогласованным DNS. Существуют приложения DNS, в которых серверы для зоны предназначены быть несогласованными. Для таких конфигураций описанные здесь механизмы согласования будут неприемлемы.

Реализации DNS не обязаны поддерживать AXFR, IXFR и NOTIFY, но им следует обеспечивать те или иные механизмы поддержки согласованности серверов. Реализация DNS общего назначения будет, очевидно, поддерживать AXFR (а также IXFR и NOTIFY), но заказные реализации DNS могут существовать и без AXFR.

[1] Incremental Zone Transfer - инкрементальный перенос зоны.

1.3. Контекст

Кроме описания самих механизмов существует еще контекст, в котором рассматривается работа этих механизмов. В исходной спецификации AXFR (а также IXFR и NOTIFY) вопросам безопасности и конфиденциальности (приватности) было уделено незначительное внимание. С момента исходного определения AXFR были добавлены опции доступа ко всему содержимому зоны. В этом документе базовые механизмы будут рассматриваться отдельно от прав на использование этих механизмов.

1.4. Связь с исходной спецификацией AXFR

Этот документ концентрируется на определении AXFR. Какие-либо усилия по обновлению спецификации механизмов IXFR и NOTIFY оставлены для других документов.

Исходная «спецификация» субпротокола AXFR «размазана» по RFC 1034 и RFC 1035. В параграфе 2.2 RFC 1035 (стр. 5) описан сценарий, для которого предназначен AXFR. В параграфе 4.3.5 RFC 1034 описаны стратегии сертификации зоны в общем виде и правила для выполнения полного переноса зоны с помощью AXFR; пятый абзац этого параграфа содержит очень краткое описание протокола AXFR. В параграфе 5.5 RFC 2181 исправлены существенные изъяны предшествующей спецификации. В параграфе 3.2.3 RFC 1035 выделен код для AXFR QTYPE (см. параграф 2.1.2 ниже). В параграфе 4.2 RFC 1035 обсуждается использование транспортного уровня в DNS и даны краткие разъяснения по поводу неприемлемости транспорта UDP для AXFR; в последнем абзаце параграфа 4.2.2 приведено детальное описание управления соединениями TCP для AXFR. Параграф 6.3 в RFC 1035 задает поведение сервера при изменении данных зоны в процессе переноса зоны с использованием AXFR.

Этот документ обновляет спецификацию AXFR. Здесь полностью описаны форматы записей и правила обработки для AXFR, что является существенным расширением абзаца 5 в параграфе 4.3.5 RFC 1034, детализированы вопросы транспорта для AXFR с заменой поведения, описанного в параграфе 4.2.2 RFC 1035. Кроме того, в документе рассматриваются вопросы совместимости с более ранними версиями, вопросы управления/политики, а также специфичные для AXFR вопросы безопасности. Целью настоящего документа является определение AXFR для современной среды DNS.

2. Сообщения AXFR

Сессия AXFR включает запросное сообщение AXFR и последовательность сообщений-откликов AXFR в ответ на этот запрос. В данном документе клиентом AXFR называется отправитель запроса AXFR, а сервером AXFR — отвечающая на запрос сторона (термины master - ведущий, slave - ведомый, primary - первичный, secondary - вторичный не имеют значения в контексте определения AXFR). Термин «сессия» без дополнительных пояснений относится к сессии AXFR.

Важно принимать во внимание, что определение AXFR ограничено транспортом TCP [RFC0793] (см. раздел 4). Организация процесса AXFR имеет унаследованные особенности, которые достаточно сложно перенести на транспорт UDP [RFC0768].

Базовый формат сообщения AXFR соответствует формату сообщений DNS, определенному в разделе 4 (MESSAGES) RFC 1035 [RFC1035] и обновленному в следующих документах:

- «базовая» спецификация DNS:
  - «A Mechanism for Prompt Notification of Zone Changes (DNS NOTIFY)[1]» [RFC1996];
  - «Dynamic Updates in the Domain Name System (DNS UPDATE)[2]» [RFC2136];
  - «Clarifications to the DNS Specification[3]» [RFC2181];
  - «Extension Mechanisms for DNS (EDNS0)[4]» [RFC2671];
  - «Secret Key Transaction Authentication for DNS (TSIG)[5]» [RFC2845];
  - «Secret Key Establishment for DNS (TKEY RR)[6]» [RFC2930];
  - «Obsoleting IQUERY[7]» [RFC3425];
  - «Handling of Unknown DNS Resource Record (RR) Types[8]» [RFC3597];
  - «HMAC SHA (Hashed Message Authentication Code, Secure Hash Algorithm) TSIG Algorithm Identifiers[9]» [RFC4635];
  - «Domain Name System (DNS) IANA Considerations[10]» [RFC5395];
- последующие дополнения, связанные с защитными расширениями DNS (DNSSEC):
  - «DNS Security Introduction and Requirements[11]» [RFC4033];
  - «Resource Records for the DNS Security Extensions[12]» [RFC4034];

[1]Механизм быстрого уведомления об изменении зоны.
[2]Динамическое обновление DNS.
[3]Разъяснения к спецификации DNS.
[4]Механизмы расширения для DNS.
[5]Аутентификация с помощью секретных ключей для DNS.
[6]Организация секретных ключей для DNS.
[7]Вывод (отвод) запросов.
[8]Обработка неизвестных типов записей DNS.
[9]Идентификаторы HMAC SHA алгоритма TSIG.
[10]DNS – согласование с IANA.
[11]Безопасность DNS - введение и требования.
[12]Записи RR для защитных расширений DNS.

- «Protocol Modifications for the DNS Security Extensions[1]» [RFC4035];
- «Use of SHA-256 in DNSSEC Delegation Signer (DS) Resource Records (RRs)[2]» [RFC4509];
- «DNS Security (DNSSEC) Hashed Authenticated Denial of Existence» [RFC5155];
- «Use of SHA-2 Algorithms with RSA in DNSKEY and RRSIG Resource Records for DNSSEC» [RFC5702];
- «Clarifications and Implementation Notes for DNSSECbis» [DNSSEC-U].

В этих документах содержится информация о синтаксисе и семантике сообщений DNS. Они не связаны непосредственно с AXFR, но будут полезны для понимания того, что будет передаваться с помощью AXFR.

Для удобства ниже воспроизведено краткое описание заголовков сообщений DNS из [RFC5395] и реестра IANA для параметров DNS [DNSVALS].

В документе используются имена полей, показанные на рисунке. Имена разделов в сообщениях DNS начинаются с заглавных букв для удобства восприятия (например, раздел Additional).

Ограничение размера сообщений DNS из [RFC1035] для работы DNS по протоколу UDP (и расширения с помощью механизма EDNS0, описанного в [RFC2671]), не относятся к AXFR, как объяснено в разделе 4. Верхняя граница размера сообщения DNS при работе по протоколу TCP ограничивается только кадрированием TCP, определенным в параграфе 4.2.2 RFC 1035, которое задает двухоктетное поле размера сообщения, трактуемое, как целое число без знака. Таким образом, размер сообщения ограничен 65535 октетами. Это ограничение не меняется в EDNS0.

Отметим, что бит TC (отсечение) никогда не устанавливается сервером AXFR и не рассматривается (не читается) клиентом AXFR.

```
  0  1  2  3  4  5  6  7  8  9 10 11 12 13 14 15
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|                      ID                       |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|QR|   OpCode  |AA|TC|RD|RA| Z|AD|CD|   RCODE   |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|                  QDCOUNT/ZOCOUNT                |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|                  ANCOUNT/PRCOUNT                |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|                  NSCOUNT/UPCOUNT                |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|                    ARCOUNT                      |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
```

2.1. Запрос AXFR

Запрос AXFR передается клиентом, когда у того возникает причина для такого запроса. Это может быть запланированное или инициированное событием действие по обслуживанию зоны (см. параграф 4.3.5 RFC 1034 и документ DNS NOTIFY [RFC1996], соответственно), а также в результате выполнения команды оператора (например, для отладки).

2.1.1. Значения заголовка

Ниже приведены значения полей заголовка сообщения DNS для запроса AXFR.

ID — выбирается клиентом (примечание a);

QR — **должно** иметь значение 0 (Query - запрос);

OPCODE — **должно** иметь значение 0 (Standard Query - стандартный запрос);

Флаги:

- AA — n/a (см. примечание b);
- TC — n/a (см. примечание b);
- RD — n/a (см. примечание b);
- RA — n/a (см. примечание b);
- Z — mbz (см. примечание c);
- AD — n/a (см. примечание b);
- CD — n/a (см. примечание b);

RCODE — **должно** иметь значение 0 (No error - нет ошибок);

QDCOUNT — число записей в разделе Question; **должно** иметь значение 1;

ANCOUNT — число записей в разделе Answer; **должно** иметь значение 0;

NSCOUNT — число записей в разделе Authority; **должно** иметь значение 0;

ARCOUNT — число записей в разделе Additional (см. примечание d).

Примечания.

a) Устанавливается любое значение, которое клиент еще не использовал для этого сервера. Каких-то специальных рекомендаций по выбору значения этого поля нет (отмена данного AXFR осуществляется только путем управления соединением TCP — см. раздел 4. Транспорт).

Сервер **должен** ответить, используя сообщения с таким же значением в поле ID, что позволяет клиенту использовать множество совпадающих во времени транзакций через одно соединение TCP (см. примечание a в параграфе 2.2.1).

b) n/a - говорит, что данное поле не имеет значения в контексте запросных сообщений AXFR. Для клиентов **рекомендуется** устанавливать в таких полях значение 0. Сервер **должен** игнорировать такие поля.

[1]Изменения протокола для защитных расширений DNS.
[2]Использование SHA-256 в записях DS RR.

c) mbz - клиент **должен** установить для этого поля значение 0, а сервер **должен** игнорировать поле.

d) Клиент **должен** указать в этом поле количество записей о ресурсах, включенных в раздел Additional. При отсутствии явных спецификаций новых RR[1] для передачи в разделе Additional запроса AXFR, это поле **может** принимать значения 0, 1 или 2 (см. параграф 2.1.5. Раздел Additional).

2.1.2. Раздел Question

Раздел Question запроса AXFR **должен** соответствовать требованиям параграфа 4.1.2 RFC 1035 и содержать одну RR со следующими значениями:

QNAME имя запрашиваемой зоны;

QTYPE AXFR (= 252), тип псевдо-RR для переноса зоны [DNSVALS];

QCLASS класс запрашиваемой зоны [DNSVALS].

2.1.3. Раздел Answer

Раздел Answer **должен** быть пустым.

2.1.4. Раздел Authority

Раздел Authority **должен** быть пустым.

2.1.5. Раздел Additional

В настоящее время определены два типа записей, которые могут появляться в разделе Additional дапросов и откликов AXFR - защита транзакций EDNS и DNS. Будущие спецификации определений RR, которые могут передаваться в разделе Additional нормальных транзакций DNS, должны явно указывать их использование с AXFR, если таковое желательно.

Клиент **может** включить одну запись OPT [RFC2671]. Если сервер не поддерживает EDNS0, клиент **должен** передавать этот раздел без записи OPT, когда возникает повтор. Однако протокол не определяет явной индикации отсутствия поддержки сервером EDNS0, что требует предположений со стороны клиента. Зачастую сервер будет возвращать код ошибки FormErr(1), которая может быть связана с записью OPT. Отметим, что на момент подготовки этого документа лишь поле EXTENDED-RCODE в OPT RR являлось значимым в контексте AXFR; будущие спецификации флагов EDNS и/или опций EDNS должны описывать их использование в контексте AXFR, если таковое применимо.

Клиент **может** включить одну запись аутентификации и целостности транзакции (в настоящее время это записи TSIG [RFC2845] или SIG(0) [RFC2931]). Если сервер показал, что он не понимает запись и ошибка действительно вызвана записью, клиенту, возможно, не следует повторять попытку. Удаление данных защиты следует выполнять с пониманием возможных последствий.

В общем случае, если клиент AXFR уверен в том, что сервер AXFR не поддерживает тот или иной механизм, клиенту **не следует** пытаться работать с сервером с помощью такого механизма (или просто не следует использовать этот сервер). Клиент может проверить возможности сервера с помощью конфигурационных установок или иным (пока не определенным) способом.

Спектр записей, которые **могут** включаться в раздел Additional может изменяться с течением времени. Если меняется существующая запись (как OPT RR для EDNS) или создается новая запись в разделе Additional, новое определение должно включать обсуждение допустимости использования и влияния этой записи на AXFR. Будущие записи для размещения в разделе Additional могут давать эффект, «ортогональный» AXFR и, поэтому, могут передаваться в сессии, как «непрозрачные» данные. В таких случаях «мудрая» реализация должна быть способна передать эти записи без нарушения работы.

2.2. Отклик AXFR

Отклик AXFR будет включать одно или множество сообщений. Специальный случай закрытия сервером соединения TCP без возврата отклика AXFR описан в параграфе 2.3.

Отклик AXFR, передающий содержимое зоны, будет состоять из последовательности сообщений DNS (последовательность может включать 1 сообщение). В таких последовательностях первое сообщение **должно** начинаться с записи SOA для зоны, а последнее **должно** включать такую же запись SOA. В остальные сообщения последовательности **недопустимо** включать записи SOA. Сервер AXFR **должен** копировать раздел Question из соответствующего запроса AXFR в раздел Question первого сообщения отклика. Для последующих сообщений **можно** включать ту же копию раздела Question или оставлять раздел пустым.

Протокол AXFR трактует содержимое зоны, как неупорядоченное множество RR. За исключением требования включения SOA RR в первое и последнее сообщения, никаких других требований к порядку передачи RR или их группировке не предъявляется. Хотя серверы обычно пытаются передавать связанные между собой RR (например, записи одного набора Rrset или наборы Rrset одного имени) в виде непрерывной группы сообщений или в одном сообщении (если поволяет размер сообщения). Этого не требуется и клиент **должен** принимать отличные от SOA записи в любом порядке и с любой группировкой. Каждую RR **следует** передавать однократно и клиент AXFR **должен** игнорировать все полученные дубликаты RR.

В каждое сообщение отклика AXFR **следует** включать достаточное число RR с целью минимизации служебного трафика, вплоть до максимального числа записей, помещающегося в сообщение DNS (принимая во внимание содержимое других разделов, как описано ниже).

[1]Resource record - запись о ресурсах.

Некоторые клиенты AXFR могут ожидать наличия в каждом сообщении единственной записи RR. Для взаимодействия с такими клиентами сервер **может** ограничить размер сообщений одной записью RR. Поскольку не существует способа автоматического детектирования таких клиентов, для них обычно требуется настройка параметров сервера вручную.

Для индикации ошибки в отклике AXFR сервер AXFR передает одно сообщение DNS с указанием обнаруженной ошибки, содержащим код отклика, значение которого соответствует ошибке. Такое сообщение прерывает сессию AXFR; оно **должно** содержать копию раздела Question из запроса AXFR в своем разделе Question, но включение завершающей записи SOA не требуется.

Сервер AXFR может передать множество сообщений отклика AXFR до передачи сообщения, указывающего на ошибку.

2.2.1. Значения заголовка

Ниже перечислены значения полей заголовка сообщений DNS в откликах AXFR.

ID	**должно** копироваться из запроса (см. примечание a);
QR	**должно** быть значение 1 (Response — отклик);
OPCODE	**должно** быть значение 0 (Standard Query - стандартный запрос);
Флаги:	
AA	обычно 1 (см. примечание b);
TC	**должно** быть значение 0 (Not truncated - без отсечения);
RD	**рекомендуется** копировать значение из запроса; **можно** установить 0;
RA	**следует** установить 0 (см. примечание c);
Z	mbz (см. примечание d);
AD	mbz (см. примечание d);
CD	mbz (см. примечание d);
RCODE	см. примечание e);
QDCOUNT	в первом сообщении **должно быть** значение 1; в последующих сообщениях **должно** быть значение 0 или 1; д**олжно** иметь значение 1, если RCODE показывает ошибку;
ANCOUNT	(см. примечание f).
NSCOUNT	**должно** быть значение 0;
ARCOUNT	(см. примечание g).

Примечания.

a) Поскольку поведение некоторых старых реализаций отличается от желаемого сегодня, требование для этого поля детализировано дополнительно. Новые серверы DNS **должны** устанавливать в этом поле значение ID из запроса AXFR в каждом сообщении отклика AXFR для данной сессии. Клиенты AXFR **должны** быть способны управлять сессиями со множеством одновременных запросов (AXFR или другие запросы DNS). Клиентам **следует** отбрасывать отклики, которые не соответствуют по значению ID ни одному из незавершенных запросов.

   Пока клиент не уверен, что сервер будет устанавливать в поле ID отклика значение ID из запроса, клиенту **не рекомендуется** вводить новые запросы до завершения переноса зоны. Клиент **может** проверить возможности сервера по конфигурационным установкам.

b) Если RCODE = 0 (нет ошибок), флаг AA **должен** иметь значение 1. Для всех остальных значений RCODE флаг AA **должен** устанавливаться в соответствии с правилами для конкретного кода ошибки. При возникновении сомнений **рекомендуется** устанавливать значение 1. Клиенту AXFR **рекомендуется** игнорировать это значение.

c) Серверу **рекомендуется** устанавливать значение 0, клиент **должен** игнорировать это значение.

   Сервер **может** устанавливать это значение в соответствии с локальной политикой в части рекурсивного обслуживания, но это может вызывать неоднозначную интерпретацию отклика, поскольку AXFR не может использовать рекурсию. Клиент **может** зафиксировать политику сервера в части рекурсии на основе этого значения, но **не следует** делать вывод о том, что отклик AXFR был получен с использованием рекурсии, даже в том случае, когда в запросе было установлено RD = 1.

d) mbz - сервер **должен** установить значение 0, а клиент **должен** игнорировать это поле.

e) При отсутствии ошибок сервер **должен** установить для этого поля значение NoError(0). Если сервер не является полномочным для запрашиваемой зоны, ему **следует** устанавливать значение NotAuth(9). (напоминание: см. соответствующий реестр IANA [DNSVALS]). Если клиент получает в отклике любое другое значения, он **должен** действовать в соответствии с указанной ошибкой. Например, некорректно сформированный запрос AXFR или присутствие записи OPT, переданной старому серверу, будет приводить к возврату значения FormErr(1). Это значение не устанавливается, как часть специфической для AXFR обработки отклика. Ситуация аналогична и для других значений, указывающих на ошибку.

f) Значение счетчика ответных записей **должно** быть равно числу записей в разделе AXFR Answer. Когда сервер уверен, что клиент будет воспринимать только отклики с одной RR, это поле **должно** иметь значение 1. Сервер **может** обрести уверенность в ограниченных возможностях клиента из конфигурационных данных.

g) Сервер **должен** указывать в этом поле количество записей RR, помещаемых в раздел Additional. При отсутствии явных спецификаций новых записей RR, которые будут передаваться в разделе Additional сообщений с откликами AXFR поле **может** иметь значение 0, 1 или 2. См. параграф 2.1.5, где описаны применимые в настоящее время RR и параграф 2.2.5, где дополнительно рассматриваются вопросы, связанные с серверами AXFR.

2.2.2. Раздел Question

В первом сообщении отклика этот раздел **должен** содержать копию одноименного раздела из запроса. В последующих сообщениях раздел **может** содержать эту же копию или оставаться пустым. Однако в сообщениях отклика, содержащие информацию об ошибке (см. параграф 2.2), этот раздел **должен** включать копию раздела из запроса. Содержимое этого раздела **может** служить для определения контекста сообщения (имени переносимой зоны).

2.2.3. Раздел Answer

Раздел Answer **должен** заполняться содержимым зоны. Представление этого содержимого описано в разделе 3.

2.2.4. Раздел Authority

Раздел Authority **должен** быть пустым.

2.2.5. Раздел Additional

Содержимое этого раздела **должно** соответствовать рекомендациям для записей OPT, TSIG и SIG(0) или других записей, которые могут быть определены в будущем. К этому разделу применимо также содержимое параграфа 2.1.5. К откликам AXFR применимы приведенные ниже соображения.

> Если клиент представляет запись EDNS OPT RR в запросе AXFR и сервер также включает в отклик EDNS, ему **следует** включить запись OPT RR в первое сообщение отклика и **можно** включать ее в последующие сообщения (см. параграф 2.2); спецификации опций EDNS, которые будут передаваться в записи OPT RR могут вносить более строгие требования.
>
> Если клиент представляет запись защиты транзакции (в настоящее время TSIG или SIG(0)) и сервер поддерживает выбранный клиентом метод, сервер **должен** включить соответствующую запись в сообщения отклика AXFR, согласно принятым для выбранного метода правилам.

2.3. Разрыв соединения TCP

Если клиент AXFR передает запрос через соединение TCP, а это соединение разрывается по любой причине, клиент AXFR **должен** считать сеанс AXFR прерванным. Идентификатор сообщения (ID) **можно** снова использовать в новом соединении даже в тех случаях, когда запрос и сервер будут те же.

Применительно к разорванному соединению клиенту **следует** попытаться определить причину разрыва — действие сети или решение сервера AXFR. Такое определение не всегда точно. Способ реагирования выбирает клиент, но ему **не следует** бесконечно повторять попытки или увеличивать частоту попыток.

Разработчикам серверов AXFR следует принимать во внимание упомянутую выше дилемму, когда соединение разрывается при незавершенной обработке запроса. Для таких ситуаций сервер должен принимать во внимание возможность злоупотребления со стороны клиента AXFR.

3. Содержимое зоны

Задачей сессии AXFR является запрос и передача содержимого зоны для того, чтобы предоставить клиенту AXFR возможность корректно реконструировать зону, существующую на основном сервере для данного порядкового номера зоны. Слово «существует» в данном случае относится к видимому извне поведению - содержимое зоны, которое будет обрабатываться (передаваться клиентам) не является копией содержимого файла зоны или используемой сервером базы данных и для обеспечения согласованности клиенту следует выполнить подобающую обработку полученных данных.

С течением времени определение зоны было расширено от статического набора записей до динамически обновляемого набора и, потенциально, до непрерывно регенерируемого набора записей (например, RR, синтезируемые «на лету» из набора правил или в результате просмотра базы данных).

3.1. Включаемые записи

В раздел Answer откликов **должны** включаться записи RR для зоны с данным порядковым номером. Определение того, что относится к зоне, приведено в RFC 1034 (параграф 4.2, «Деление базы данных на зоны» и, в частности, параграф 4.2.1 «Технические вопросы») и дополнительно разъяснено в разделе 6 RFC 2181.

Зоны, для которых на практике нецелесообразно перечислять всю зону для порядкового номера, не подходят для переноса AXFR. Типичным (но не единственным) случаем такой зоны является зона, состоящая из откликов, генерируемых по результатам запросов к базе данных и/или конструируемая на основе меняющихся данных.

3.2. Записи Delegation

В параграфе 4.2.1 RFC 1034 сказано (обратите внимание, что слово «следует» не выделено, поскольку документ был выпущен до разработки [BCP14] - см. параграф 1.1):

> Записям RR, которые описывают срезы, ... следует совпадать с соответствующими RR наверху узла субзоны.

Это утверждение вступает в противоречие с выбором записей NS, включаемых в перенос зоны.

Фраза «которые описывают срезы» относится к набору NS и применима к склеивающим записям. Это не означает идентичности записей для точки среза и апекса (вершины) зоны идентичны. Например, запись SOA может присутствовать только на вершине зоны. Приведенное здесь рассмотрение ограничено набором NS и склеивающих записей, как «описывающих срезы».

Для записей DNSSEC имеются отдельные спецификации, относящиеся к расположению этих записей на срезе и вершине зоны. Эти спецификации были введены в параграфах 5.3 и 6.2 RFC 2181 (изначальная спецификация DNSSEC), которые, фактически, отошли в достояние истории. Современный набор документов DNSSEC (см. список в разделе 2 выше) полностью указывают местоположение записей DNSSEC(bis), а в параграфе 3.1.5 RFC 4035 введено требование по их трактовке в AXFR; дополнительная запись NSEC3, определенная позднее в RFC 5155, ведет себя идентично NSEC RR в контексте AXFR.

По сути:

- DS RRSet присутствует только на родительской стороне среза зоны и содержит полномочные данные для родительской, но не дочерней зоны;
- DNSKEY RRSet присутствует только на вершине подписанной зоны и является полномочной частью данных обслуживаемой зоны;
- независимые наборы RRSIG RRSet присутствуют только в подписанной родительской части среза зоны и на вершине подписанной зоны; эти данные полномочны для соответствующей зоны; простые запросы для записей RRSIG могут возвращать оба набора, если один тот же сервер является полномочным для родительской и дочерней зон (в параграфе 3.1.5 RFC 4035 описаны различия между этими RR); эта кажущаяся неопределенность не возникает для AXFR, поскольку каждый такой набор RRSIG RRset относится к одной зоне;
- различные записи NSEC [RFC4034] (или NSEC3 [RFC5155]) могут одинаково появляться на родительской стороне среза и на вершине зоны; каждая такая запись относится в точности к одной из этих зон и включается в AXFR для этой зоны.

Одна из проблем заключается в том, что в некоторые моменты записи NS могут различаться для точки среза родительской зоны и вершины зоны. Иногда это является результатом ошибки, а в других случаях может быть частью происходящего в серверах имен изменения. Протокол DNS достаточно устойчив к несоответствиям вплоть до отсутствия (но не включая его) показанной родителем записи NS, ссылающейся на сервер, способный обслуживать дочернюю зону. Эта устойчивость явилась одним из качеств, которые обеспечили успех DNS. Тем не это состояние является ошибочным и требуется принять меря, чтобы это состояние было замечено (если оно не запланировано).

Другой проблемой является то, что сервер AXFR может быть полномочным для набора зон, который отличается от набора зон, на которые распространяются полномочия клиента AXFR. Может оказаться, что сервер AXFR полномочен для обеих половин несогласованной точки среза, а клиент имеет полномочия только для родительской стороны среза.

При рассмотрении ситуации, когда записи NS в точке среза не соответствуют полномочному набору возникает вопрос, может ли сервер AXFR возвращать набор записей NS, который находится в переносимой зоне или в полномочном месте.

Отклик AXFR **должен** содержать набор записей NS точки среза, зарегистрированный с зоной где он согласуется или не согласуется с полномочным набором. Слова «зарегистрированный с» могут трактоваться достаточно широко вплоть до включения данных, находящихся в файле зоны для конкретного порядкового номера (в среде файла зоны), или любых данных, сконфигурированных для наличия в зоне (базе данных) статически или динамически.

Эти требования обусловлены перечисленными ниже причинами.

1) Сервер AXFR может оказаться не способным определить несоответствие локальным данным, следовательно, требование соответствия значительно увеличивает объем работы и усложняет поиск данных. От полномочного сервера не следует требовать выполнения любых запросов.
2) При переносе несогласованных записей NS от сервера, который полномочен как для среза, так и для вершины зоны, к клиенту, который не является полномочным ни для среза, ни для вершины, будет возникать ошибка. Например, уполномоченный администратор может вручную запросить AXFR и проверить результат на предмет наличия несоответствий (в противном случае полномочных для обеих половин сервер всегда будет давать ответ из более полномочного набора, скрывая ошибку).
3) Несогласованный набор записей NS может указывать на проблему в регистрационной базе данных.
4) Это требование нужно для обеспечения гарантии того, что при отыскании заданной пары (зона, порядковый номер) с помощью AXFR будет возвращаться один и тот же набор записей, независимо от выбора полномочного сервера для переноса зоны.

Если серверу AXFR было разрешено отвечать с полномочным NS RRset дочерней зоны вместо NS RRset родительской зоны в зоне, которая будет передаваться, набор возвращаемых данных может меняться в зависимости от того, является ли этот сервер полномочным и для дочерней зоны.

Свойства для данной пары зона-порядковый номер соответствуют одному точно определенному набору записей, который требуется для корректной работы протоколов инкрементального переноса типа IXFR [RFC1995]. Например, клиент может получить зону с одного сервера AXFR и потом воспользоваться инкрементальным обновлением по IXFR с другого сервера. Если эти серверы по-разному трактуют содержимое зоны, у клиента могут возникнуть попытки добавить уже имеющиеся записи или удалить записи, которых нет.

3.3. Склеивающие записи

Как сказано в предыдущем параграфе, RFC 1034 (параграф 4.2.1) содержит руководство и обоснование для включения склеивающих записей, как части отклика AXFR. И, как было отмечено в предыдущем параграфе данного документа,

даже при отсутствии согласованности между адресом в склеивающей записи и полномочной копией адреса сервера имен, склеивающая запись, запрашиваемая, как часть зоны с данным порядковым номером, должна быть включена.

Это относится к склеивающим записям для всех семейств адресов [IANA-AF].

Отклик AXFR **должен** включать подходящие склеивающие записи, как зарегистрированные с зоной. Интерпретация слов «зарегистрированные с», использованная в предыдущем параграфе, применима и здесь. Несоответствие склеивающих записей вполне допустимо.

3.4. Сжатие имен

Сжатие имен в сообщениях DNS описано в RFC 1035 (параграф 4.1.4, Message compression[1]). Отмеченная здесь проблема относится к комментарию, приведенному в параграфе 3.1 (Name space specifications and terminology[2]) RFC 1034, который гласит:

> При получении доменного имени или метки следует[3] сохранять регистр символов.

Поскольку основной целью AXFR является обеспечение клиенту возможности обслуживать то же самое содержимое зоны, которое хранится на сервере, в отличие от обычных откликов DNS, в которых предполагается сохранение регистра символов в запросе, для реального переноса зон требуется сохранять регистр символов меток в содержимом зоны. По этой причине сжатие имен в сообщении AXFR **следует** выполнять так, чтобы регистр символов сохранялся в отличие от того, как компрессия выполняется для «обычных» откликов DNS. Т. е., несмотря на то, что при сравнении доменных имен принимается a=A, при сравнении в целях компрессии для AXFR принимается, что «a» не равно «A». Отметим, что это отличается от обычного определения сравнения имен в протоколе DNS и представляет новую трактовку требований к серверам AXFR.

Правила сжатия имен для RDATA в сообщениях AXFR **должны** соответствовать спецификациям Handling of Unknown DNS Resource Record (RR) Types[4] [RFC3597] и, в частности, параграфа 4 Domain Name Compression[5].

3.5. Скрытые имена

Операции динамического обновления [RFC2136] и в особенности их взаимодействие с DNAME [RFC2672] могут давать побочный эффект в виде «сокрытия» имен в зоне. 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[6]».

Скрытые имена **должны** включаться в отклики AXFR. Клиент AXFR **должен** быть способен идентифицировать и обработать скрытые имена. Основанием для этого требования является быстрое восстановление для случаев ошибочного выполнения динамической операции.

4. Транспорт

Сессии AXFR в настоящее время ограничены использованием протокола TCP, как указано в параграфе 4.3.5 RFC 1034:

> Поскольку точность имеет существенное значение, для запросов AXFR должен использоваться протокол TCP или другие протоколы с гарантированной доставкой.

Требование использовать протокол TCP содержится также в параграфе 6.1.3.2 документа «Требования к хостам Internet - Прикладные и служебные протоколы» [RFC1123].

Наиболее распространенным сценарием для клиента AXFR является организация соединения TCP с сервером AXFR, передача запроса AXFR, получение отклика AXFR и закрытие (разрыв) соединения. Однако вариации этого простого сценария доступны и даже желательны - например, передача запроса для записи SOA через соединение TCP и повторное использование существующего TCP для других запросов.

Следовательно, допущение о том, что соединение TCP предназначено для одной сессии AXFR, является некорректным. Такое ложное допущение может приводить к тому, что реализация будет препятствовать организации множества одновременных переносов или использованию открытого соединения для новых запросов.

С первых дней использования DNS операторы, имеющие множество полномочных серверов имен для общего набора зон считают желательной организацию одновременного переноса для множества серверов - это позволяет серверу имен не ждать, пока завершится операция переноса зоны с другим сервером имен. RFC 1035 не исключает такую возможность, но унаследованные реализации не всегда способны эффективно выполнять множество одновременных переносов через одно соединение TCP. Сохранившиеся экземпляры таких унаследованных реализаций требуют от новых реализаций клиентов общего назначения поддерживать старые модели поведения для одновременных транзакций DNS и сессий AXFR через одно соединение TCP.

4.1. TCP

В исходном определении присутствовало спорное неявное (возможно, непреднамеренное) предположение, что соединение TCP используется для одной и только одной сессии AXFR. Проявлением этого является отсутствие явного требования копировать раздел Question и или идентификатор сообщения в отклики, отсутствие явного упорядочения информации в откликах AXFR и отсутствие явного указания на продолжение переноса зоны в следующем сообщении.

Целью приведенного ниже руководства является повышение производительности обмена AXFR, а также рекомендации по взаимодействию со старыми программами. Повышение производительности включает возможность

---

[1] Сжатие сообщений.
[2] Спецификации и терминология пространства имен.
[3] Термин «следует» не выделен шрифтом, поскольку процитированный документ выпущен до [BCP14].
[4] Обработка неизвестных типов RR.
[5] Сжатие доменных имен.
[6] В оригинале «occluded». *Прим. перев.*

мультиплексного обмена сообщениями DNS, включая сеансы переноса зон. Рекомендации по взаимодействию со старыми программами в общем случае относятся к новым клиентам AXFR. В обратной ситуации (взаимодействие старого клиента AXFR с новым сервером AXFR) сервер может функционировать в рамках старой спецификации.

4.1.1. Клиент AXFR - TCP

Клиент AXFR **может** запросить соединение с сервером AXFR по любой причине. Клиенту AXFR **следует** завершать соединение, если он не видит необходимости использовать это соединение в течение достаточно продолжительного времени. Сервер AXFR не обязан поддерживать бездействующие соединения - ответственность за разрыв соединения лежит на клиенте. Решение об отсутствии необходимости принимает клиент AXFR (клиент DNS). Если соединение используется для множества сессий, известно о продолжении сессии или имеются трафик других запросов/откликов, предполагаемый или передаваемый через открытое соединение, это говорит о наличии необходимости.

Клиент AXFR может отказаться от доставки зоны только посредством разрыва соединения. Однако это действие повлечет за собой также прерывание всех прочих операций, выполняемых с использованием данного соединения. Другого механизма прерывания отклика AXFR не существует.

При удаленном (относительно клиента) закрытии соединения TCP (по инициативе сервера или в результате событий в сети) клиент AXFR **должен** прервать все оставшиеся сессии и транзакции, не относящиеся к AXFR. Восстановление после такого разрыва не всегда просто. Если разрыв произошел в результате случайности, разумно просто попытаться заново организовать соединение. Если разрыв был вызван продолжающимся отказом, клиенту AXFR неразумно тратить слишком много ресурсов на попытки восстановить соединение. Если же соединение было разорвано в соответствии с политикой сервера AXFR (это может возникать при работе со старыми серверами AXFR), клиенту AXFR нет смысла повторять попытки организации соединения. К сожалению не существует способа различить три описанных выше ситуации (а именно, сбой, отказ, политика), поэтому не остается других методов, кроме эвристических. Это достаточно типичная ситуация для клиентов основанных на явных соединениях протоколов, когда они не получают адекватной информации об ошибках.

Клиент AXFR **может** использовать уже созданное соединение TCP для начала сессии AXFR. Использование существующих соединений **рекомендуется** (можно использовать соединения, через которые передается трафик, отличный от AXFR). Если в таком случае клиент AXFR не может подобающим образом дифференцировать отклики (например, по причине отсутствия в откликах идентификатора запроса) или соединение разрывается удаленной стороной, клиенту AXFR **не следует** пытаться заново организовать соединение с соответствующим сервером AXFR, пока этот сервер AXFR не будет обновлен (такие события не отражаются в протоколе DNS).

4.1.2. Сервер AXFR - TCP

Сервер AXFR **должен** быть способен обрабатывать множество сессий AXFR через одно соединение TCP одновременно с обслуживанием других запросов/откликов через это же соединение.

При удаленном разрыве соединения TCP сервер AXFR **должен** прервать все организованные через это соединение сессии AXFR. Операций по восстановлению соединения выполнять не требуется — это прерогатива клиента AXFR.

Локальная политика **может** требовать разрыва соединения TCP. Такие действия **следует** выполнять в качестве реакции на превышение предельных значений)типа числа остающихся открытыми соединений). Разрыв соединения в ответ на подозрительное с точки зрения безопасности событие **следует** выполнять только в крайних случаях, когда сервер уверен в своих действиях. В ответ на отдельный запрос зоны, не находящейся на сервере AXFR, **следует** возвращать подходящий код отклика без разрыва соединения.

4.2. UDP

Добавление EDNS0 и приложений, которым требуется множество мелких зон (например, web-хостинг и некоторые сценарии ENUM) делает желательной поддержку сессий AXFR на основе протокола UDP. Однако некоторые аспекты сеансов AXFR не удается легко перенести на транспорт UDP.

Следовательно, данный документ не меняет требование RFC 1035 в этой части - сессии AXFR на основе протокола UDP не определены спецификацией.

5. Проверка полномочий

Администратор зоны имеет полномочия ограничивать AXFR-доступ к зоне. Это не было предусмотрено в исходном варианте DNS, но возникло в процессе развития протокола DNS. Ограничения на использование AXFR могут быть обусловлены разными причинами, включая желание (а в некоторых случаях - требования законодательства) сохранить полное содержимое зоны в тайне или снизить нагрузку на серверы, связанную с обработкой AXFR. Можно считать эти доводы спорными, но данный документ, исходя из опыта использования протокола с момента публикации RFC 1035, подтверждает фактическое требование для создания механизмов, ограничивающих доступ AXFR.

Реализациям DNS **следует** обеспечивать меры по ограничению сессий AXFR указанным кругом клиентов.

Реализациям **следует** предоставлять доступ по адресам IP или диапазонам адресов, не принимая во внимание, что адрес отправителя может быть подставным. Предоставление доступа по адресам в комбинации с технологиями VPN[1] [RFC2764] или VLAN[2] обеспечивает достаточно эффективное ограничение.

Реализациям общего назначения **рекомендуется** поддерживать контроль доступа на базе методов Secret Key Transaction Authentication for DNS (TSIG) [RFC2845] и/или DNS Request and Transaction Signatures (SIG(0)s) [RFC2931].

Реализациям общего назначения **следует** разрешать доступ для всех запросов AXFR. Т. е., оператору должна обеспечиваться возможность ввода любого запроса AXFR.

[1]Virtual Private Network - виртуальная частная сеть.
[2]Virtual LAN - виртуальная ЛВС.

Реализациям общего назначения **не следует** поддерживать по умолчанию политику AXFR «разрешено всем» (open to all). Например, по умолчанию перенос может быть разрешен только для адресов, указанных администраторами DNS для размещенных на сервере зон.

6. Целостность зоны

Клиент AXFR **должен** гарантировать, что для обслуживания зоны будет использоваться только успешно перенесенная копия. Предшествующее описание и практика реализации привели к созданию двухэтапной модели процедуры синхронизации зоны - по триггеру (например, при просмотре записи SOA обнаружено изменение порядкового номера SOA или получен запрос DNS NOTIFY [RFC1996]) инициируется сессия AXFR в результате чего данные зоны сохраняются в базе данных (этот .тап требуется в любом случае для обеспечения гарантии корректного перезапуска сервера); по завершении операции AXFR и некоторых проверок этот набор данных «загружается», становится доступным для «атомных» операций обслуживания зоны и помечается, как «корректный» для использования при следующем запуске сервера DNS; при обнаружении любой ошибки эти данные **должны** быть удалены и клиент AXFR **должен** продолжать использование прежней версии зоны, если он делал это ранее. Видимое извне поведение реализации клиента AXFR **должно** быть эквивалентно описанной здесь двухэтапной модели.

Если клиент AXFR отвергает данные, полученные в сессии AXFR, ему **следует** запомнить порядковый номер и **можно** попытаться запросить ту же зону снова. Причина повторения запроса для того же номера может быть обусловлена тем, что отказ от восприятия данных мог быть связан с деталями реализации конкретного сервера AXFR для зоны и при запросе данных у другого сервера AXFR для этой зоны проблема может не возникнуть. При наличии у оператора зоны такой возможности защита может быть обеспечена с использованием выделенных каналов (физических или логических на основе VPN) между полномочными серверами. Однако в некоторых случаях у оператора зоны нет иной возможности организации сессий AXFR, кроме глобальной публичной сети Internet.

Кроме защиты соединений TCP реализациям DNS **следует** обеспечивать возможность использования TSIG[1] [RFC2845] и/или SIG(0)[2] [RFC2931], чтобы клиенты AXFR могли проверить содержимое. Эти методы **могут** также применяться для проверки полномочий.

7. Совместимость с ранними версиями

Описание совместимости с более ранними версиями весьма затруднительно по причине «расплывчатости» исходного определения. В этом параграфе приведены некоторые советы по обеспечению такой совместимости, заимствованные большей частью из предшествующих параграфов.

Совместимость с более ранними версиями не является обязательной, но она обеспечивает повышение уровня интероперабельности. Для заказных реализаций вопроса совместимости обычно не возникает. Для реализаций общего назначения важность совместимости с более ранними версиями определяется требованиями интероперабельности.

К сожалению, необходимость смены поведения для обеспечения совместимости с более старыми версиями невозможно тем или иным способом детектировать и отразить в конфигурационном файле. Реализациям **следует** в своей документации предупреждать операторов о необходимости периодического пересмотра клиентов и серверов AXFR, поскольку старые программы время от времени обновляются.

7.1. Сервер

Сервер AXFR имеет возможность реагировать на «способности» клиентов AXFR, за исключением возможности выяснить, способен ли клиент воспринимать сообщения AXFR, содержащие множество записей. Такая ограниченность клиента не может быть обнаружена, поэтому ее следует указывать в конфигурационном файле.

Реализация сервера AXFR **может** на уровне отдельного клиента AXFR задавать необходимость передачи по одной записи в сообщении - в таких случаях по умолчанию **следует** передавать множество записей в сообщении.

7.2. Клиент

Клиент AXFR имеет возможность при запросе сервера AXFR попытаться воспользоваться другими функциями (т. е., теми, которые не рассматриваются в этом документе).

Попытку ввести множество запросов DNS через соединение TCP для сеанса AXFR **следует** прерывать, если прерывается исходный запрос, **следует** также принимать во внимание возможность разрыва соединения сервером AXFR сразу же по выполнении исходного (вызвавшего организацию соединения) переноса зоны.

8. Вопросы безопасности

Этот документ содержит разъяснения для механизмов, предложенных в RFC 1034 и RFC 1035, не добавляя новых проблем безопасности. Документ RFC 3833 [RFC3833] полностью посвящен вопросам безопасности DNS - в параграфе 4.3 проведено разграничение вопросов безопасности при переносе зон и угроз, предотвращаемых с помощью DNSSEC.

Вопросы, касающиеся проверки полномочий (авторизации), лавинных атак и целостности сообщений, рассмотрены в разделе 5 «Проверка полномочий», параграфе 4.1 «TCP», и разделе 6 «Целостность зоны».

9. Согласование с IANA

Агентство IANA добавило ссылку на данный RFC в строку AXFR (252) субреестра Resource Record (RR) TYPEs[3] в реестре Domain Name System (DNS) Parameters[4].

---

[1]Secret Key Transaction Authentication for DNS (TSIG) - Аутентификация транзакций DNS с помощью секретного ключа.
[2]DNS Request and Transaction Signatures - подписи для запросов и транзакций DNS.
[3]Типы записей о ресурсах.
[4]Параметры DNS.

10. Поддержка других языков

Протокол AXFR прозрачен для части содержимого зон DNS, в которой может рассматриваться вопрос поддержки отличных от английского языков[1]. Предполагается, что для меток DNS и доменных имен вопросы использования других языков решены в документе Internationalizing Domain Names in Applications (IDNA) [RFC3490] или более современных его вариантах.

11. Благодарности

Ранние черновые варианты этого документа редактировал Andreas Gustafsson. В последней черновой версии документа присутствовал текст:

> Множество людей внесло свой вклад и предоставило комментарии к черновым вариантам этого документа. Неполный список таких людей включает Bob Halley, Dan Bernstein, Eric A. Hall, Josh Littlefield, Kevin Darcy, Robert Elz, Levon Esibov, Mark Andrews, Michael Patton, Peter Koch, Sam Trenholme, Brian Wellington.

К последней черновой версии документа свои комментарии предоставили:

> Mark Andrews, Paul Vixie, Wouter Wijngaards, Iain Calder, Tony Finch, Ian Jackson, Andreas Gustafsson, Brian Wellington, Niall O'Reilly, Bill Manning и другие члены рабочей группы DNSEXT. Значимые комментарии со стороны IETF были получены, прежде всего, от Subramanian Moonesamy, Chris Lonvick, Vijay K. Gurbani.

Edward Lewis выполнял функции редактора этого документа в течение двух лет.

12. Литература

Все упомянутые ниже RFC, равно как и все остальные документы серии RFC, доступны на сайте RFC Editor по адресу http://www.rfc-editor.org.

12.1. Нормативные документы

[BCP14] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC0793] Postel, J., "Transmission Control Protocol", STD 7, RFC 793, September 1981.

[RFC0768] Postel, J., "User Datagram Protocol", STD 6, RFC 768, August 1980.

[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.

[RFC1123] Braden, R., Ed., "Requirements for Internet Hosts - Application and Support", STD 3, RFC 1123, October 1989.

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

[RFC1996] Vixie, P., "A Mechanism for Prompt Notification of Zone Changes (DNS NOTIFY)", RFC 1996, August 1996.

[RFC2136] Vixie, P., Ed., 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.

[RFC2671] Vixie, P., "Extension Mechanisms for DNS (EDNS0)", RFC 2671, August 1999.

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

[RFC2845] Vixie, P., Gudmundsson, O., Eastlake 3rd, D., and B. Wellington, "Secret Key Transaction Authentication for DNS (TSIG)", RFC 2845, May 2000.

[RFC2930] Eastlake 3rd, D., "Secret Key Establishment for DNS (TKEY RR)", RFC 2930, September 2000.

[RFC2931] Eastlake 3rd, D., "DNS Request and Transaction Signatures (SIG(0)s)", RFC 2931, September 2000.

[RFC3425] Lawrence, D., "Obsoleting IQUERY", RFC 3425, November 2002.

[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.

[RFC4509] Hardaker, W., "Use of SHA-256 in DNSSEC Delegation Signer (DS) Resource Records (RRs)", RFC 4509, May 2006.

[RFC4635] Eastlake 3rd, D., "HMAC SHA (Hashed Message Authentication Code, Secure Hash Algorithm) TSIG Algorithm Identifiers", RFC 4635, August 2006.

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

[RFC5395] Eastlake 3rd, D., "Domain Name System (DNS) IANA Considerations", BCP 42, RFC 5395, November 2008.

[RFC5702] Jansen, J., "Use of SHA-2 Algorithms with RSA in DNSKEY and RRSIG Resource Records for DNSSEC", RFC 5702, October 2009.

[1] Точнее, отличных от ASCII наборов символов. *Прим. перев.*

12.2. Дополнительная литература

[DNSVALS] IANA Registry "Domain Name System (DNS) Parameters", http://www.iana.org/.

[IANA-AF] IANA Registry "Address Family Numbers", http://www.iana.org/.

[RFC2764] Gleeson, B., Lin, A., Heinanen, J., Armitage, G., and A. Malis, "A Framework for IP Based Virtual Private Networks", RFC 2764, February 2000.

[RFC3490] Faltstrom, P., Hoffman, P., and A. Costello, "Internationalizing Domain Names in Applications (IDNA)", RFC 3490, March 2003.

[RFC3833] Atkins, D. and R. Austein, "Threat Analysis of the Domain Name System (DNS)", RFC 3833, August 2004.

[DNSSEC-U] Weiler, S. and D. Blacka, "Clarifications and Implementation Notes for DNSSECbis", Work in Progress, March 2010.

Адреса авторов

Edward Lewis

46000 Center Oak Plaza

Sterling, VA 20166

US

EMail: ed.lewis@neustar.biz

Alfred Hoenes, редактор

TR-Sys

Gerlinger Str. 12

Ditzingen D-71254

Germany

EMail: ah@TR-Sys.de

Перевод на русский язык

Николай Малых

nmalykh@protocols.ru