Network Working Group
Request for Comments: 1995
Updates: 1035
Category: Standards Track

M. Ohta
Tokyo Institute of Technology

August 1996

Постепенный перенос зон в DNS

Incremental Zone Transfer in DNS

Статус документа

В этом документе описан предлагаемый стандарт протокола для сообщества Internet; документ служит приглашением к дискуссии в целях развития протокола. Информацию о текущем состоянии стандартизации протокола можно найти в документе "Internet Official Protocol Standards" (STD 1). Данный документ может распространяться свободно.

Аннотация

Этот документ вносит расширение для протоколов DNS, обеспечивающее поддержку механизма инкрементального перноса зон (IXFR[1]).

1. Введение

Для быстрого распространения изменений в базе данных DNS [STD13] требуется снизить величину задержки путем активного уведомления серверов об изменениях. Это достигается за счет добавления в DNS расширения NOTIFY [NOTIFY].

Текущий механизм полного переноса зон AXFR не обеспечивает эффективного способа распространения изменений в небольшой части зоны, поскольку с помощью этого механизма зоны переносятся целиком.

Постепенный перенос (IXFR), предложенный здесь, обеспечивает более эффективный механизм за счет того, что передается лишь измененная часть зоны.

В этом документе вторичные серверы, которые запрашивают перенос IXFR, называются клиентами IXFR, а первичные или вторичные серверы имен, которые отвечают на запросы переноса зон, называются серверами IXFR.

2. Краткое описание протокола

Если клиент IXFR, который явно имеет устаревшую версию зоны, полагает, что ему нужна новая информация о зоне (обычно по тайм-ауту обновления SOA или с помощью механизма NOTIFY), он передает сообщение IXFR, содержащее порядковый номер SOA для своей, предположительно устаревшей, копии зоны.

Серверу IXFR следует следует хранить новейшую версию зоны и различия между этой версией и несколькими ее предшественницами. При получении запроса IXFR с порядковым номером старой версии серверу IXFR нужно передать копию различий между устаревшей и текущей версией. Кроме того, сервер может выбрать перенос зоны целиком, как при обычной операции переноса зоны.

При обновлении зоны содержимое старой зоны следует сохранить в стабильной памяти до тех пор, пока не начнется использование новой версии, чтобы можно было отвечать на запросы IXFR (или AXFR). Иначе при аварии на сервере информация о недоступности данных может быть распространена между вторичными серверами, что приведет к несогласованности базы данных.

При получении запроса IXFR с тем же или более новым порядковым номером серверу следует передавать в ответ только порядковый номер текущей версии записи SOA, как это делается в случае AXFR.

Транспортировка запроса может осуществляться с помощью протокола UDP или TCP. Если запрос IXFR передается через UDP, сервер IXFR может попытаться ответить с помощью протокола UDP, если отклик целиком помещается в один пакет DNS. Если UDP не позволяет передать весь отклик в одном пакете, клиенту возвращается только запись SOA для текущей версии сервера, чтобы уведомить клиента о необходимости передачи запроса по протоколу TCP.

Таким образом, клиенту следует передавать первый запрос IXFR с использованием UDP. Если тип запроса не был распознан сервером, тому слеует попытаться использовать AXFR (предварительно передав по протоколу UDP запись SOA) для обеспечения совместимости с устаревшими версиями. Если отклик представляет собой один пакет или у сервера нет новой версии для данного клиента, обработка запроса на этом завершается. В остальных случаях следует предпринять попытку использования TCP IXFR.

Для обеспечения целостности серверам следует использовать контрольные суммы UDP для всех UDP-откликов. Осмотрительным клиентам следует игнорировать пакеты UDP с нулевым значением контрольной суммы и использовать взамен TCP IXFR.

Для IXFR агентство IANA выделило значение 251.

3. Формат запроса

Для запросов IXFR используются пакеты такого же формата, которые применяются для обычных запросов DNS, но тип запроса указывает IXFR и раздел authority содержит запись SOA для имеющейся у клиента версии зоны.

[1]Incremental zone transfer.

4. Формат отклика

Если инкрементальный перенос зоны недоступен, возвращается зона целиком. Первая и последняя записи RR в отклике являются записями SOA для данной зоны (т. е., поведение не отличается от переноса AXFR, но в качестве типа запроса используется IXFR).

Если доступен инкрементальный перенос, возвращается одна или несколько записей о различиях. В начале и в конце последовательности различий помещается запись SOA текущей версии зоны на сервере.

Каждая последовательность различий представляет собой одно обновление зоны (одно изменение порядкового номера SOA), состоящее из удаленных и добавленных записей RR. Первой RR из числа удаленный указывается старая запись SOA RR, а первой RR из числа добавленных - новая запись SOA RR.

При изменении RR сначала удаляются имеющиеся записи, а после этого добавляются измененные и новые.

Последовательности различий упорядочиваются от старых к новым. Таким образом, эти последовательности включают историю изменений, внесенных от известной клиенту IXFR версии до текущей версии на сервере.

Записи RR в инкрементальном переносе могут быть неполными. Т. е., при изменении множества однотипных RR передаваться будут только измененные записи.

Клиенту IXFR следует заменять старый номер версии новым только после завершения обработки всех изменений.

Отклик при инкрементальном переносе отличается от обычного отклика тем, что он начинается с двух записей SOA — сначала указывается SOA текущей версии сервера, а за ней - запись SOA заменяемой версии клиента.

5. Стратегия очистки

Сервер IXFR не обязан хранить все предшествующие версии, он может удалять их в любой момент. В общем случае обеспечивается компромисс между размером области хранения и возможностью использования IXFR.

Информацию о старых версиях следует очищать, если общий размер отклика IXFR будет превышать размер отклика AXFR. Исходя из того, что задачей IXFR является снижение издержек AXFR, такая стратегия представляется разумной. При такой стратегии объем требуемой для хранения памяти не будет превышать объем текущих данных зоны более, чем вдвое.

Информация, которая старше срока действия SOA, также может удаляться.

6. Объединение изменений

Сервер IXFR может собирать множество последовательностей различий в одну последовательность, отбрасывая данные о промежуточных изменениях.

Такой подход может обеспечивать преимущества при наличии большого числа версий, не все из которых оказались полезными. Например, если множество серверов ftp используют одно имя DNS и адрес IP, связанный с именем, меняется каждую минуту для распределения нагрузки между серверами, отслеживать всю историю изменений нет смысла.

Однако такое объединение может оказаться не столь полезным, если клиент IXFR имеет доступ к двум серверам IXFR с несогласованной консолидацией изменений. Текущая версия клиента IXFR, полученная от сервера A, может быть не известна серверу B. В таком случае B не сможет обеспечить инкрементальное обновление для неизвестной версии и придется переносить зону полностью.

Консолидация изменений является необязательной функцией. Клиент не может по отклику определить наличие или отсутствие консолидации.

Для обеспечения интероперабельности серверам IXFR, включая серверы без поддержки консолидации, не следует констатировать ошибку даже при получении от клиента IXFR запроса с неизвестным номером версии. В таких случаях следует предпринять попытку полного переноса зоны.

7. Пример

Ниже приведены три версии зоны с текущим порядковым номером 3.

```
      JAIN.AD.JP.          IN SOA NS.JAIN.AD.JP. mohta.jain.ad.jp. (
                                      1 600 600 3600000 604800)
                           IN NS  NS.JAIN.AD.JP.
      NS.JAIN.AD.JP.       IN A   133.69.136.1
      NEZU.JAIN.AD.JP.     IN A   133.69.136.5
```

Имя NEZU.JAIN.AD.JP. удалено, а JAIN-BB.JAIN.AD.JP. добавлено.

```
      jain.ad.jp.          IN SOA ns.jain.ad.jp. mohta.jain.ad.jp. (
                                      2 600 600 3600000 604800)
                           IN NS  NS.JAIN.AD.JP.
      NS.JAIN.AD.JP.       IN A   133.69.136.1
      JAIN-BB.JAIN.AD.JP.  IN A   133.69.136.4
                           IN A   192.41.197.2
```

Один из IP-адресов JAIN-BB.JAIN.AD.JP. изменен.

```
      JAIN.AD.JP.          IN SOA ns.jain.ad.jp. mohta.jain.ad.jp. (
                                      3 600 600 3600000 604800)
                           IN NS  NS.JAIN.AD.JP.
      NS.JAIN.AD.JP.       IN A   133.69.136.1
      JAIN-BB.JAIN.AD.JP.  IN A   133.69.136.3
                           IN A   192.41.197.2
```

На запрос IXFR

```
            +-------------------------------------------------+
Заголовок   | OPCODE=SQUERY                                   |
            +-------------------------------------------------+
Вопрос      | QNAME=JAIN.AD.JP., QCLASS=IN, QTYPE=IXFR        |
            +-------------------------------------------------+
Ответ       | <пусто>                                         |
            +-------------------------------------------------+
Полномочия  | JAIN.AD.JP.          IN SOA serial=1            |
            +-------------------------------------------------+
Дополнение  | <пусто>                                         |
            +-------------------------------------------------+
```

может быть дан отклик со следующим сообщением для полного переноса зоны:

```
            +-------------------------------------------------+
Заголовок   | OPCODE=SQUERY, RESPONSE                         |
            +-------------------------------------------------+
Вопрос      | QNAME=JAIN.AD.JP., QCLASS=IN, QTYPE=IXFR        |
            +-------------------------------------------------+
Ответ       | JAIN.AD.JP.          IN SOA serial=3            |
            | JAIN.AD.JP.          IN NS  NS.JAIN.AD.JP.      |
            | NS.JAIN.AD.JP.       IN A   133.69.136.1        |
            | JAIN-BB.JAIN.AD.JP.  IN A   133.69.136.3        |
            | JAIN-BB.JAIN.AD.JP.  IN A   192.41.197.2        |
            | JAIN.AD.JP.          IN SOA serial=3            |
            +-------------------------------------------------+
Полномочия  | <пусто>                                         |
            +-------------------------------------------------+
Дополнение  | <пусто>                                         |
            +-------------------------------------------------+
```

или с сообщением для инкрементального переноса:

```
            +-------------------------------------------------+
Заголовок   | OPCODE=SQUERY, RESPONSE                         |
            +-------------------------------------------------+
Вопрос      | QNAME=JAIN.AD.JP., QCLASS=IN, QTYPE=IXFR        |
            +-------------------------------------------------+
Ответ       | JAIN.AD.JP.          IN SOA serial=3            |
            | JAIN.AD.JP.          IN SOA serial=1            |
            | NEZU.JAIN.AD.JP.     IN A   133.69.136.5        |
            | JAIN.AD.JP.          IN SOA serial=2            |
            | JAIN-BB.JAIN.AD.JP.  IN A   133.69.136.4        |
            | JAIN-BB.JAIN.AD.JP.  IN A   192.41.197.2        |
            | JAIN.AD.JP.          IN SOA serial=2            |
            | JAIN-BB.JAIN.AD.JP.  IN A   133.69.136.4        |
            | JAIN.AD.JP.          IN SOA serial=3            |
            | JAIN-BB.JAIN.AD.JP.  IN A   133.69.136.3        |
            | JAIN.AD.JP.          IN SOA serial=3            |
            +-------------------------------------------------+
Полномочия  | <пусто>                                         |
            +-------------------------------------------------+
Дополнение  | <пусто>                                         |
            +-------------------------------------------------+
```

или с консолидированной информацией об изменениях:

```
            +-------------------------------------------------+
Заголовок   | OPCODE=SQUERY, RESPONSE                         |
            +-------------------------------------------------+
Вопрос      | QNAME=JAIN.AD.JP., QCLASS=IN, QTYPE=IXFR        |
            +-------------------------------------------------+
Ответ       | JAIN.AD.JP.          IN SOA serial=3            |
            | JAIN.AD.JP.          IN SOA serial=1            |
            | NEZU.JAIN.AD.JP.     IN A   133.69.136.5        |
            | JAIN.AD.JP.          IN SOA serial=3            |
            | JAIN-BB.JAIN.AD.JP.  IN A   133.69.136.3        |
            | JAIN-BB.JAIN.AD.JP.  IN A   192.41.197.2        |
            | JAIN.AD.JP.          IN SOA serial=3            |
            +-------------------------------------------------+
Полномочия  | <пусто>                                         |
            +-------------------------------------------------+
Дополнение  | <пусто>                                         |
            +-------------------------------------------------+
```

или (в случае переполнения пакета UDP) с сообщением:

```
            +-------------------------------------------------+
Заголовок   | OPCODE=SQUERY, RESPONSE                         |
            +-------------------------------------------------+
Вопрос      | QNAME=JAIN.AD.JP., QCLASS=IN, QTYPE=IXFR        |
            +-------------------------------------------------+
Ответ       | JAIN.AD.JP.          IN SOA serial=3            |
            +-------------------------------------------------+
Полномочия  | <пусто>                                         |
            +-------------------------------------------------+
Дополнение  | <пусто>                                         |
            +-------------------------------------------------+
```

8. Благодарности

Оригинальную идею IXFR предложили Anant Kumar, Steve Hotz и Jon Postel.

В развитие протокола и документации внесли вклад множество людей, включая Anant Kumar, Robert Austein, Paul Vixie, Randy Bush, Mark Andrews, Robert Elz и членов рабочей группы IETF DNSIND.

9. Литература

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

[STD13] Mockapetris, P., "Domain Name System", STD 13, (RFC 1034 и RFC 1035), November 1987.

10. Вопросы безопасности

Хотя в DNS существуют некоторые проблемы безопасности, в данном документе не содержится попыток решения этих проблем.

Надеемся, что этот документ не порождает новых проблем безопасности в современном протоколе DNS.

11. Адрес автора

Masataka Ohta

Computer Center

Tokyo Institute of Technology

2-12-1, O-okayama, Meguro-ku, Tokyo 152, JAPAN

Phone: +81-3-5734-3299

Fax: +81-3-5734-3415

EMail: mohta@necom830.hpcl.titech.ac.jp

Перевод на русский язык

Николай Малых

nmalykh@protokols.ru