Network Working Group
Request for Comments: 1996
Updates: 1035
Category: Standards Track

P. Vixie
ISC

August 1996

Механизм быстрого уведомления об изменении зоны

A Mechanism for Prompt Notification of Zone Changes (DNS NOTIFY)

Статус документа

В этом документе содержится спецификация 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

В этом документе описан код операции NOTIFY для DNS, посредством которой ведущий (master) сервер извещает группу ведомых (slave) серверов о том, что хранящиеся на ведущем сервере данные изменились и ведомым серверам следует инициировать запрос для получения новой информации.

1. Обоснования и сфера документа

1.1. Медленное распространение новых и измененных данных в зоне DNS может быть обусловлено относительно большим периодом обновления для этой зоны. Преимущество редких обновлений состоит в том, что это снижает нагрузку на ведущий сервер. Но за это преимущество приходиться расплачиваться тем, что в течение достаточно продолжительного интервала после обновления зоны может сохраняться несогласованность между уполномоченными серверами (authority server) зоны.

1.2. DNS-транзакция NOTIFY позволяет ведущему серверу информировать ведомые об изменениях в зоне[1] и, тем самым, снизить задержку распространения информации без возникновения нежелательного роста нагрузки на ведущий сервер. Данная спецификация позволяет уведомлять ведомые серверы лишь об изменении SOA RR[2], но архитектура NOTIFY может быть расширена и на другие типы RR.

1.3. Документ умышленно включает множество ролевых определений - серверы Master (ведущий), Slave (ведомый) и Stealth (скрытый), их перечисление в NS RR, а также поле SOA MNAME. В этом смысле данный документ можно считать дополнением к [RFC1035].

2. Определения и инварианты

2.1. Определения используемых в документе терминов

Slave (ведомый)
Уполномоченный сервер, который использует перенос зоны для ее получения. Все ведомые серверы указываются в NS RR для данной зоны.

Master (ведущий)
Любой уполномоченный сервер, настроенный на то, чтобы играть роль источника информации при переносе зоны для одного или множества ведомых серверов.

Primary Master (первичный ведущий)
Ведущий сервер в корне графа зависимостей для переноса зоны. Первичный ведущий сервер зоны указывается в поле SOA MNAME, а также может указываться в NS RR. По определению для зоны существует только один первичный ведущий сервер.

Stealth (скрытый)
Похож на ведомый сервер, но не указывается в NS RR для данной зоны. Скрытый сервер, если явно не оговорено иное, будет устанавливать бит AA в откликах и способен функционировать в режиме ведущего. Скрытый сервер станет известен другим серверам только в том случае, когда у них имеются статические конфигурационные данные, указывающие на существование такого сервера.

Notify Set (набор [серверов] для уведомления)
Группа серверов, уведомляемых об изменениях в некой зоне. По умолчанию эта группа включает все серверы, указанные в NS RR, за исключением тех, которые указаны также в SOA MNAME. Некоторые реализации позволяют администратору сервера имен переписывать этот набор и добавлять в него элементы (например, скрытые серверы).

2.1.

Серверы зоны должны быть организованы в граф зависимости так, чтобы существовал единственных первичный ведущий сервер, а все остальные серверы должны использовать перенос AXFR или IXFR с первичного ведущего сервера или с какого-либо из ведомых, который является одновременно и ведущим. Не допускается наличие петель в графе зависимостей AXFR.

[1] Это можно рассматривать, как прерывание в противовес режиму опроса, обычно используемому в системе DNS.
[2] Resource Record - запись о ресурсе. *Прим. перев.*

3. Сообщение NOTIFY

3.1. Когда ведущий сервер обновляет одну или несколько RR, в которых могут быть заинтересованы ведомые серверы, ведущий сервер может передать измененные RR для имени, класса, типа и (необязательно) новые RDATA каждому ведомому серверу, используя протокол на основе операции NOTIFY.

3.2. NOTIFY использует формат сообщений DNS, хотя реально применяется только часть доступных полей. Поля, не рассматриваемые в данном документе, заполняются нулями (двоичными) и реализации должны игнорировать все сообщения, для которых данное условие не выполняется.

3.3. Сообщение NOTIFY похоже на QUERY в том, что в запросе флаг QR сброшен, а в отклике - установлен. Отклики не содержат полезной информации, но получение отклика ведущим сервером служит индикацией того, что ведомый сервер получил сообщение NOTIFY и ведущий сервер может удалить этот ведомый из очереди на повтор передачи для данного события NOTIFY.

3.4. Транспортным протоколом для транзакций NOTIFY будет UDP, если ведущий сервер не настроен на использование протокола TCP (например, в тех случаях, когда между ведущими и ведомыми серверами имеется межсетевой экран, который пропускает только трафик TCP, или измененная запись RR настолько велика, что не может быть передана в дейтаграмме UDP/DNS).

3.5. При использовании TCP оба сервера (ведущий и ведомый) должны продолжать нормальную работу в процессе этой транзакции, даже в тех случаях, когда это будет тормозить выполнение транзакции TCP. Запрос NOTIFY передается однократно и, если в течение разумного интервала не было получено отклика NOTIFY, говорят о таймауте.

3.6. При использовании UDP ведущий сервер периодически шлет ведомому запрос NOTIFY, пока не будет превышено число попыток («таймаут»), получено сообщение ICMP о недоступности порта или получен отклик NOTIFY от ведомого сервера с соответствующими значениями идентификатора запроса, QNAME, IP-адреса отправителя, и номером порта UDP на стороне отправителя.

Примечание

Интервал между попытками и общее число повторов следует делать конфигурационными параметрами, доступными администратору сервера имен. Возможна независимая установка параметров для каждой зоны. Разумными значениями являются интервал 60 секунд (или таймаут при использовании TCP) и максимальное число попыток - 5 (для UDP). Представляется разумным использование линейного или экспоненциального роста интервала повтора в зависимости от номера попытки.

3.7. Запрос NOTIFY имеет QDCOUNT > 0, ANCOUNT >= 0, AUCOUNT >= 0, ADCOUNT >=0. Если ANCOUNT > 0, раздел answer представляет незащищенное указание в новом наборе RRset для данного <QNAME,QCLASS,QTYPE>. Ведомый сервер, получивший такое указание, волен трактовать эквивалентность этого раздела answer своим локальным данным, как индикацию того, что не нужно выполнять других действий. Если ANCOUNT = 0 или ANCOUNT > 0 и раздел answer отличается от локальных данных ведомого сервера, последнему следует обратиться к известным ему ведущим серверav для получения новых данных.

3.8. Ни в коем случае не следует использовать раздел answer запроса NOTIFY для обновления локальных данных ведомого сервера, индикации необходимости переноса зоны или изменения значений таймеров обновления зоны для ведомого сервера.

Только условие «данные присутствуют и совпадают» моетт менять поведение ведомого сервера для случаев ANCOUNT > 0 и ANCOUNT = 0.

3.9. Данная версия спецификации NOTIFY не использует разделы authority и additional data, поэтому соответствующей данной спецификации реализации протокола следует устанавливать AUCOUNT = 0 и ADCOUNT = 0 при передаче запросов. В силу того, что в будущих версиях спецификации может быть (с обратной совместимостью) определено использование одного или обоих этих разделов, современным реализациям следует игнорировать эти разделы (но не все сообщение целиком), если AUCOUNT > 0 и/или ADCOUNT > 0.

3.10. Если ведомый сервер получает запрос NOTIFY от хоста, который не указан ведущим сервером для зоны, содержащейся в QNAME, ему следует игнорировать это сообщение и записать в системный журнал сообщение об ошибке.

Примечание

Это условие предполагает, что ведомые серверы, которые работают с многодомным ведущим сервером, должны знать адрес «ближайшего» к ним или всех интерфейсов ведущего сервера. В противном случае корректный запрос NOTIFY может быть получен с адреса, который не указан в списке ведущих серверов для этой зоны на данном ведомом сервере. В результате может произойти ошибка.

3.11. Единственным определенным в настоящий момент событием NOTIFY является изменение записи SOA RR. По завершению транзакции NOTIFY для QTYPE=SOA ведомому серверу следует поступать, как в том случае, когда для зоны, указанной в QNAME, истекло время обновления (интервал REFRESH, описанный в [RFC1035]), т. е., ему следует запросить у своих ведущих серверов записи SOA для зоны, указанной NOTIFY QNAME, и проверить значение порядкового номера (SOA SERIAL). Если полученное значение превышает локальное, следует инициировать перенос зоны (с помощью AXFR или IXFR).

Примечание

Поскольку при большой глубине графа зависимостей может существовать множество путей от первичного ведущего сервера к данному ведомому, возможно, что ведомый сервер получит NOTIFY от одного из своих ведущих, хотя некоторые из известных ему ведущих серверов этой зоны еще не обновили свои копии зоны. Следовательно, при введении запроса QUERY для SOA-записи зоны этот запрос следует направлять тому из известных ведущих серверов, от которого был получен запрос NOTIFY, а не какому-либо иному из ведущих

серверов. Это отличается от требований документа [RFC1035], в котором сказано, что по истечении интервала SOA REFRESH следует запрашивать поочередно все ведущие серверы зоны[1].

3.12. Если запрос NOTIFY получен ведомым сервером, который не поддерживает код операции NOTIFY, этот сервер будет возвращать сообщение NOTIMP (функция не реализована). Ведущему серверу при получении такого сообщения следует считать транзакцию NOTIFY завершенной для данного ведомого.

4. Детали и примеры

4.1. Сохранение данных о состоянии запросов при перезагрузке хоста не является обязательным, но будет весьма разумным способом выполнения транзакции SOA NOTIFY для каждой зоны, для которой сервер имеет полномочия, при первом запуске сервера.

4.2. Очевидно, что каждый ведомый сервер может получать несколько копий одного запроса NOTIFY - исходный запрос от первичного ведущего и по одному от каждого другого ведомого, который перенес обновленную зону и уведомляет об этом своих потенциальных партнеров. Протокол NOTIFY требует, чтобы серверы, работающие в режиме slave/master, передавали запрос только **после** того, как они обновят SOA RR или определят, что обновления не требуется, что на практике приводит к тому, что такие запросы могут передаваться только после успешного переноса зоны. Таким образом, за исключением случаев нарушения порядка доставки последний запрос NOTIFY, который получен любым ведомым сервером, будет указывать на самое свежее изменение. Поскольку ведомый сервер всегда запрашивает SOA и AXFR/IXFR только у известных ему ведущих серверов, он может повторять свой запрос QUERY для SOA после того, как каждый из его ведущих будет завершать обновление любой из зон.

4.3. Если ведущий сервер хочет предотвратить перенос с него обновленной зоны множеством ведомых серверов одновременно, он может задерживать на произвольное время передачу сообщения NOTIFY для каждого конкретного ведомого. Предполагается, что время задержки будет выбираться случайным образом, поэтому каждый ведомый сервер будет начинать свой перенос в разное время. Задержку в любом случае не следует делать больше SOA REFRESH.

Примечание

Для задания этой задержки следует использовать параметр, который может устанавливать каждый первичный ведущий сервер (возможно, независимо для каждой зоны). Случайные задержки в диапазоне от 30 до 60 секунд представляются подходящими для серверов, расположенных в одной локальной сети при умеренных размерах зон.

4.4. Ведомому серверу, получившему корректный запрос NOTIFY, следует откладывать действия, вызванные последующими сообщениями NOTIFY с такими же значениями <QNAME,QCLASS,QTYPE>, пока не будет завершена транзакция, вызванная первым сообщением NOTIFY. Такое отторжение дубликатов требуется для предотвращения избыточной нагрузки на ведущий сервер.

4.5 Обновление зоны на первичном ведущем сервере

Первичный ведущий сервер передает запрос NOTIFY всем серверам, указанным в его Notify Set. Запрос NOTIFY имеет следующие характеристики:

```
query ID:   (новое значение)
op:         NOTIFY (4)
resp:       NOERROR
flags:      AA
qcount:     1
qname:      (имя зоны)
qclass:     (класс зоны)
qtype:      T_SOA
```

4.6 Обновление зоны на ведомом сервере, который также служит ведущим

Как в примере параграфа 4.5 с единственным отличием в том, что Notify Set может отличаться от набора первичного ведущего сервера вследствие наличия локальных скрытых серверов.

4.7 Ведомый сервер получил от ведущего запрос NOTIFY

Когда ведомый сервер получает запрос NOTIFY от одного из своих локально заданных ведущих для зоны, указанной в QNAME, с QTYPE=SOA и QR=0, ему следует перейти в состояние, которое возникает при завершении отсчета для таймера обновления зоны. Сервер будет также возвращать отправителю запроса NOTIFY отклик NOTIFY со следующими характеристиками:

```
query ID:   (то же значение, что и в запросе)
op:         NOTIFY (4)
resp:       NOERROR
flags:      QR AA
qcount:     1
qname:      (имя зоны)
qclass:     (класс зоны)
qtype:      T_SOA
```

Этот отклик должен быть идентичен запросу NOTIFY, отличаясь от того лишь установленным битом QR. Идентификатор запроса (query ID) в отклике должен совпадать с одноименным полем вызвавшего отклик запроса.

4.8 Ведущий сервер получил от ведомого отклик NOTIFY

Когда ведущий сервер получает от ведомого отклик NOTIFY, он удаляет соответствующий запрос из очереди на повтор, завершая, тем самым, процесс уведомления этого сервера об изменении данной RR.

[1] В RFC 1035 не удалось обнаружить в явном или неявном виде такого требования. *Прим. перев.*

5. Вопросы безопасности

Мы верим, что использование NOTIFY не может порождать проблем безопасности за исключением описанных ниже.

1. Запрос NOTIFY с подставным адресом отправителя IP/UDP может заставить ведомый сервер передать ложные запросы SOA своим ведущим, что может позволить организовать DoS-атаку, если подставные запросы передаются достаточно часто.
2. Можно использовать подмену TCP[1] для инициирования ложных запросов SOA со стороны ведомого сервера или подмену UDP/DNS для форсирования переноса зоны.

6. Литература

[RFC1035] Mockapetris, P., "Domain Names - Implementation and Specification", STD 13, RFC 1035, November 1987.

[IXFR] Ohta, M., "Incremental Zone Transfer", RFC 1995, August 1996.

7. Адрес автора

Paul Vixie

Internet Software Consortium

Star Route Box 159A

Woodside, CA 94062

Phone: +1 415 747 0204

EMail: paul@vix.com

Перевод на русский язык

Николай Малых

nmalykh@protokols.ru

[1]TCP spoofing.