Network Working Group
Request for Comments: 3425
Updates: 1035
Category: Standards Track

D. Lawrence
Nominum

November 2002

Obsoleting IQUERY

Отмена IQUERY

Статус документа

Этот документ содержит спецификацию стандартного протокола, предложенного сообществу Internet, и служит приглашением к дискуссии в целях развития и совершенствования протокола. Текущее состояние стандартизации протокола можно узнать из документа Internet Official Protocol Standards (STD 1). Документ может распространяться свободно.

Авторские права

Аннотация

Метод IQUERY для выполнения реверсного поиска в DNS, заданный в RFC 1035, не получил широкого распространения и обычно отключается там, где он реализован. То и другое отражает общий взгляд сообщества на неразумность данной концепции и предпочтительность широко распространённого подхода с запросами, использующими указатель (PTR), и записями обратного отображения. Этот документ обновляет RFC 1035.

1 - Введение

Как указано в RFC 1035 (параграф 6.4), операция IQUERY для запросов DNS применяется при поиске имён, связанных с данным значением. Значение указывается в разделе вопросов, а отклик помещается в раздел ответов в виде одного или нескольких триплетов тип-имя-класс (type, name, class).

Как отмечено в параграфе 6.4.3 [RFC1035], обработка реверсных запросов может вызывать на сервере достаточно высокую нагрузку. Серверу придётся выполнить исчерпывающий поиск в своей базе данных или поддерживать отдельную базу данных, в которой ключами служат значения основной базы данных. Оба этих подхода могут вызывать перегрузку ресурсов системы, особенно на серверах с полномочиями для миллионов имён. Пакеты откликов от таких мегасерверов могут быть чрезвычайно большими, легко достигая мегабайтных размеров. Например, использование IQUERY для поиска каждого домена, который передал полномочия одному из сервером имён крупного ISP может возвращать десятки тысяч триплетов в разделе ответов. Это можно легко использовать для атак с отказом в обслуживании.

Операторы серверов, в той или иной мере поддерживающих запросы IQUERY (например, серверов BIND 4), обычно предпочитают отключать такую поддержку. В основном это связано с ошибками в недостаточно протестированном коде или опасениями раскрыть слишком большие блоки имён из своих зон, например, в ответ на реверсные запросы MX.

Метод IQUERY в какой-то мере ущербен по сути, поскольку не позволяет указать запрашивающей стороне, куда ей следует обратиться за искомой информацией. Ответ на запросы будет сильно зависеть от запрошенного сервера. Иногда этот метод служит удобным инструментом диагностики, но видимо не настолько, чтобы операторы серверов захотели включить его или запросить реализацию метода там, где его нет.

Ни один из известных клиентов не применяет IQUERY для предоставления каких-либо значимых услуг. Единственная поддержка обратных отображений в Internet - это сопоставление адресов с именами, обеспечиваемое с помощью записей об указателях (PTR) в дереве in-addr.arpa, которое хорошо служит сообществу уже многие годы.

С учётом отмеченных факторов этот документ рекомендует официально отказаться от операции IQUERY для серверов DNS.

2 - Требования

Ключевое слово **следует** (SHOULD) в этом документе должно интерпретироваться в соответствии с BCP 14 (RFC 2119), а именно - могут быть причины для игнорирования определённого элемента, но при этом нужно понять и тщательно взвесить последствия такого отказа.

3 - Влияние на RFC 1035

Данный документ меняет определение кода операции (opcode) 1, исходно приведённое в параграфе 4.1.1 RFC 1035, и полностью переопределяет содержимое параграфа 6.4 в RFC 1035. Определение opcode 1 сейчас имеет вид

```
1               an inverse query (IQUERY) (obsolete)
```

Текст параграфа 6.4 в RFC 1035 признается устаревшим. Заявление о применимости операции IQUERY приведено ниже.

> Инверсные запросы с использованием операции IQUERY изначально были описаны как возможность поиска имён, связанных с определённой записью о ресурсе (Resource Record или RR). Реализация операции не была обязательной и не получила широкого распространения. Поэтому операция IQUERY признана устаревшей и в ответ на запрос IQUERY серверам имён **следует** возвращать отклик Not Implemented (не реализовано).

4 - Вопросы безопасности

Поскольку этот документ отменяет операцию, которая ранее была доступна, можно предположить, что кто-то мог применять её в качестве основы для правил защиты. Однако, поскольку наиболее логичным для такого правила в случае отсутствия отклика от сервера является отказ при проверке подлинности (полномочий), весьма маловероятно, что отменя поддержки IQUERY откроет какие-то «дыры» в защите.

Отметим, что при отказе от отмены IQUERY, защита откликов с помощью DNS Security (DNSSEC) становится крайне затруднительной без использования цифровых подписей «на лету».

5 - Взаимодействие с IANA

Код 1 для операции IQUERY следует окончательно вывести из употребления и не назначать новым операциям.

6 - Благодарности

Описанное здесь действие инициировал Olafur Gudmundsson. Matt Crawford, John Klensin, Erik Nordmark и Keith Moore внесли некоторые улучшения в формулировку обращения с устаревающей функциональностью, описанной как Internet Standard.

7 - Литература

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

[RFC2026] Bradner, S., "The Internet Standards Process — Revision 3", BCP 9, RFC 2026, October 1996.

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

8 - Адрес автора

David C Lawrence
Nominum, Inc.
2385 Bay Rd
Redwood City CA 94063
USA
Phone: +1.650.779.6042
EMail: tale@nominum.com

9 - Полное заявление авторских прав

Подтверждение

Финансирование функций RFC Editor обеспечено Internet Society.

Перевод на русский язык

Николай Малых

nmalykh@protokols.ru