

Obsoleting IQUERY

Status of this Memo

This document specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the "Internet Official Protocol Standards" (STD 1) for the standardization state and status of this protocol. Distribution of this memo is unlimited.

Copyright Notice

Copyright (C) The Internet Society (2002). All Rights Reserved.

Abstract

The IQUERY method of performing inverse DNS lookups, specified in RFC 1035, has not been generally implemented and has usually been operationally disabled where it has been implemented. Both reflect a general view in the community that the concept was unwise and that the widely-used alternate approach of using pointer (PTR) queries and reverse-mapping records is preferable. Consequently, this document deprecates the IQUERY operation, declaring it entirely obsolete. This document updates RFC 1035.

1 - Introduction

As specified in RFC 1035 (section 6.4), the IQUERY operation for DNS queries is used to look up the name(s) which are associated with the given value. The value being sought is provided in the query's answer section and the response fills in the question section with one or more 3-tuples of type, name and class.

As noted in [RFC1035], section 6.4.3, inverse query processing can put quite an arduous burden on a server. A server would need to perform either an exhaustive search of its database or maintain a separate database that is keyed by the values of the primary database. Both of these approaches could strain system resource use, particularly for servers that are authoritative for millions of names.

Response packets from these megaservers could be exceptionally large, and easily run into megabyte sizes. For example, using IQUERY to find every domain that is delegated to one of the nameservers of a large ISP could return tens of thousands of 3-tuples in the question section. This could easily be used to launch denial of service attacks.

Operators of servers that do support IQUERY in some form (such as very old BIND 4 servers) generally opt to disable it. This is largely due to bugs in insufficiently-exercised code, or concerns about exposure of large blocks of names in their zones by probes such as inverse MX queries.

IQUERY is also somewhat inherently crippled by being unable to tell a requester where it needs to go to get the information that was requested. The answer is very specific to the single server that was queried. This is sometimes a handy diagnostic tool, but apparently not enough so that server operators like to enable it, or request implementation where it is lacking.

No known clients use IQUERY to provide any meaningful service. The only common reverse mapping support on the Internet, mapping address records to names, is provided through the use of pointer (PTR) records in the in-addr.arpa tree and has served the community well for many years.

Based on all of these factors, this document recommends that the IQUERY operation for DNS servers be officially obsoleted.

2 - Requirements

The key word "SHOULD" in this document is to be interpreted as described in BCP 14, RFC 2119, namely that there may exist valid reasons to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.

3 - Effect on RFC 1035

The effect of this document is to change the definition of opcode 1 from that originally defined in section 4.1.1 of RFC 1035, and to entirely supersede section 6.4 (including subsections) of RFC 1035.

The definition of opcode 1 is hereby changed to:

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

The text in section 6.4 of RFC 1035 is now considered obsolete. The following is an applicability statement regarding the IQUERY opcode:

Inverse queries using the IQUERY opcode were originally described as the ability to look up the names that are associated with a particular Resource Record (RR). Their implementation was optional and never achieved widespread use. Therefore IQUERY is now obsolete, and name servers SHOULD return a "Not Implemented" error when an IQUERY request is received.

4 - Security Considerations

Since this document obsoletes an operation that was once available, it is conceivable that someone was using it as the basis of a security policy. However, since the most logical course for such a policy to take in the face of a lack of positive response from a server is to deny authentication/authorization, it is highly unlikely that removing support for IQUERY will open any new security holes.

Note that if IQUERY is not obsoleted, securing the responses with DNS Security (DNSSEC) is extremely difficult without out-on-the-fly digital signing.

5 - IANA Considerations

The IQUERY opcode of 1 should be permanently retired, not to be assigned to any future opcode.

6 - Acknowledgments

Olafur Gudmundsson instigated this action. Matt Crawford, John Klensin, Erik Nordmark and Keith Moore contributed some improved wording in how to handle obsoleting functionality described by an Internet Standard.

7 - References

- [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 - Author's Address

David C Lawrence
Nominum, Inc.
2385 Bay Rd
Redwood City CA 94063
USA

Phone: +1.650.779.6042
EMail: tale@nominum.com

9 - Full Copyright Statement

Copyright (C) The Internet Society (2002). All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.

