INTERNET-DRAFT
draft-lewis-axfr-over-udp-00.txt
Edward Lewis
NeuStar, Inc.
February 2008
Updates: 1034, 1035 (if approved) Intended status: Standards Track

DNS Zone Transfer Protocol (AXFR) over the User Datagram Protocol (UDP)

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with Section 6 of BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

This Internet-Draft will expire on September 1, 2008.

Copyright Notice

Copyright (C) The IETF Trust (2008).

Abstract

The Domain Name System's Authoritative Transfer (AXFR) use of the User Datagram Protocol (UDP) as a transport protocol is defined.

1 Introduction

The Domain Name System's [RFC1034] [RFC1035] Authoritative Transfer (AXFR) use of the User Datagram Protocol [RFC0768] (UDP) as a transport protocol is defined. A more thorough description of AXFR is "DNS Zone Transfer Protocol (AXFR)" [DRAFT07]. This definition builds upon that definition, including terminology, scope, applicability, etc.

Comments on this draft ought to be addressed to the editor or to namedroppers@ops.ietf.org.

1.1 Definition of Terms

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in "Key words for use in RFCs to Indicate Requirement Levels" [BCP14].

1.2 Scope

This definition extends AXFR to make use of UDP. This is an optional extension to the DNS protocol. Adherence to the requirements here is needed only to claim compliance with this feature.

1.3 Use Cases

The applicability of AXFR on UDP is envisioned to be zones small enough to fit inside the limited size of a DNS message (as adjusted by EDNS0 [RFC2671]). These may be encountered in application hosting facilities in which customers might register only a handful of resource records for their delegated domain.

An alternative to AXFR on UDP would be an IXFR [RFC1995] with a serial number of 0, which would result in a full transfer in the IXFR message format.

2 AXFR Session on UDP

An AXFR session on UDP consists of one AXFR query message and one AXFR response message. Unlike AXFR sessions on TCP [RFC0793], only one AXFR response message is to be sent. Note that due to the unreliable nature of UDP, there is no guarantee that an AXFR client will see an AXFR response to an AXFR query.

The AXFR response on UDP is restricted to one message because there is no guarantee that UDP datagrams are delivered in the same sequence they are sent. Consequently, it is possible that if there were multiple AXFR messages allowed, the final message might be delivered before other parts of the zone.

An AXFR client SHOULD attempt to use AXFR on UDP if there is reason to deduce the zone is small, for example, referring to the currently held version of the zone.

Field names used in this document will correspond to the names as they appear in the IANA registry for DNS Header Flags [DNSFLGS].

2.1 AXFR query

An AXFR query on UDP is the same as an AXFR query on TCP. See section **2.1 in [DRAFT07].**

2.2 AXFR response

For the most part, the description in section 2.2 of [DRAFT07] applies here, with some important exceptions. Principally, any discussion of the underlying connection is not relevant but the comments about error returns are.

The AXFR response will consist of 1 message.

2.2.1 Header Values

Two header values have changed meanings on UDP, the rest remain unchanged from section 2.2.1 of [DRAFT07].

```
TC          Set to 0 if the entire zone is in the message,
             Set to 1 if the zone failed to fit
QDCOUNT     MUST be 1
```

2.2.2 Query Section

This section MUST be copied from the query.

2.2.3 Answer Section

This section MUST be populated with the zone's entire contents.

The first and last resource records MUST be the zone's SOA. The requirement that the last resource record forces the contents of a UDP delivered AXFR response to be the same of a 1 message TCP delivered AXFR response or the merging of all the responses in a multi-message TCP delivery.

2.2.4 Authority Section

See section 2.2.4 of [DRAFT07].

2.2.5 Additional Section

See section 2.2.5 of [DRAFT07].

3 Zone Contents

See section 3 of [DRAFT07].

4 Transport

The intent is to define AXFR on UDP to be as close to identical to AXFR on TCP. That is, the net result, the transfer of the zone's contents, is supposed to be the same regardless of the transport protocol. But there are differences relating to the mechanics of the transfer that need to be described.

4.1.1 AXFR client UDP

An AXFR client that is able to use UDP has to make the right decision on when to use UDP. This can be be from configuration settings or perhaps noting that the held zone is small enough to fit in one DNS message.

An AXFR client receiving a truncated (TC=1) message MUST discard the the AXFR response and SHOULD retry on TCP.

If an AXFR client does not receive an AXFR response (as decided by normal DNS message management), the AXFR client SHOULD retry on TCP.

4.1.2 AXFR server UDP

An AXFR server on UDP MUST accept AXFR queries over the UDP transport.

If the zone does not fit inside the one DNS Message permitted on UDP, the TC bit must be set to one.

5 Authorization

This section is entirely the same as section 5 of [DRAFT07].

6 Zone Integrity

This section is the same as section 6 of [DRAFT07] with the exception of the comment about protecting TCP sessions does not apply.

7 Backwards Compatibility

The general principles from section 7 of [DRAFT07] apply here.

8 Security Considerations

Concerns regarding authorization, traffic flooding, and message integrity are mentioned in "Authorization" (section 5), "UDP" (section 4.1) and Zone Integrity (section 6).

9 IANA Considerations

No new registries or new registrations are included in this document.

10 Internationalization Considerations

It is assumed that supporting of international domain names has been solved via "Internationalizing Domain Names in Applications (IDNA)" [RFC3490].

11 Acknowledgements

I'll figure this out later.

12 References

All references prefixed by "RFC" can be obtained from the RFC Editor, information regarding this organization can be found at the following URL:

http://rfc-editor.org/

Additionally, these documents can be obtained via the IETF web site.

12.1 Normative

[RFC0793] "Transmission Control Protocol." J. Postel. September 1981.

[RFC0768] "User Datagram Protocol. " J. Postel. August 1980.

[RFC1034] "Domain names - concepts and facilities.", P.V. Mockapetris. Nov-01-1987.

[RFC1035] "Domain names - implementation and specification." P.V. Mockapetris. Nov-01-1987.

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

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

[DNSFLGS] http://www.iana.org/assignments/dns-header-flags

[DRAFT07] "DNS Zone Transfer Protocol (AXFR)." E. Lewis. Work In Progress. draft-ietf-dnsext-axfr-clarify-<newest>.

12.2 Informative

[BCP14] "Key words for use in RFCs to Indicate Requirement Levels." S. Bradner. March 1997.

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

13 Editor's Address

Edward Lewis
46000 Center Oak Plaza
Sterling, VA, 22033, US
+1-571-434-5468
ed.lewis@neustar.biz

Full Copyright Statement

Copyright (C) The IETF Trust (2008).

This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY, THE IETF TRUST AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM 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.

Intellectual Property

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).