Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: January 17, 2013

S. Perreault
Viagenie
J. Latour
J. Zack
Canadian Internet Registration Authority (CIRA)
July 16, 2012

DNS Server Statistics Management Information Base (MIB)
draft-perreault-dnsop-stats-mib-01

Abstract

This memo defines a portion of the Management Information Base (MIB) for monitoring statistics of DNS servers.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

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."

This Internet-Draft will expire on January 17, 2013.

Table of Contents

1. Introduction

Monitoring statistics of DNS servers is a common task. In the case of top-level domain (TLD) operators, it can be crucial to the well-being of the Internet.

This document defines managed objects for monitoring statistics of a DNS server. It is intentionally read-only: there is no way to alter the state of a DNS server using this module. The vast majority of the objects are simple, self-explanatory counters.

Managing the configuration of a server, changing zones, and triggering any action is out of scope.

Related work: A MIB prototype has been proposed for Bind 10: <http://bind10.isc.org/attachment/wiki/StatsModule/ISC-BIND10-MIB.txt>.

1.1. Use Case: TLD Operator

A popular model for a TLD operator is to make use of third-party DNS service providers. To increase resilience and availability, more than one service provider can be used. This can be in addition to a self-operated DNS service. These services are typically deployed using anycast.

It is necessary for the TLD operator to obtain management data from each anycast node in order to accomplish tasks such as capacity planning, DDoS mitigation, resilience planning, etc. When multiple parties are involved, a standard management protocol is necessary.

1.2. On RFC 3197

A previous attempt at defining a MIB for DNS servers failed. [RFC3197] analyses the causes of that failure and identifies a few lessons to be learned. This section compares those lessons against the proposal contained in this draft.

- Define a clear set of goals before writing any MIB extensions. Know who the constituency is and make sure that what you write solves their problem.
  - There is a single goal: expose usage statistics (i.e., counters) over SNMP.
  - Constituency: The problem has been identified by TLD operators trying to obtain usage statistics from anycast nodes. One TLD operator having this problem is co-authoring this draft.

- Keep the MIB extensions short, and don't add variables just because somebody in the WG thinks they'd be a cool thing to measure.
  - The proposed MIB is short (subjectively).
  - The stats exposed by the MIB are those already available in a popular DNS server used by many TLDs.
- If some portion of the task seems to be very hard to do within the SMI, that's a strong hint that SNMP is not the right tool for whatever it is that you're trying to do.
  - Writing this MIB was easy and straightforward.
- If the entire project is taking too long, perhaps that's a hint too.
  - From a technical point of view, this could be wrapped up quickly.

2. Overview

2.1. Counters

This MIB defines several counters. As a best practice, a management entity, when reading these counters, should use the discontinuity object, dnsStatsDiscontinuityTime, to determine if an event that would invalidate the management entity understanding of the counters has occurred. A restart of the DNS server process is a possible example of a discontinuity event.

2.2. Multiple DNS Server Instances

SNMPv3 supports "Contexts" that can be used to implement MIB views on multiple DNS server instances on the same system. See [RFC3411] or its successors for details.

3. Definitions

This MIB module IMPORTs objects from [RFC2578] and [RFC2579].

```
DNS-STATS-MIB DEFINITIONS ::= BEGIN

IMPORTS
    MODULE-IDENTITY, OBJECT-TYPE, Integer32, Counter64, mib-2
```

```
        FROM SNMPv2-SMI

    TEXTUAL-CONVENTION, TimeStamp
        FROM SNMPv2-TC;

dnsStatsMIB MODULE-IDENTITY
    LAST-UPDATED "200001010000Z"
    ORGANIZATION "TBD"
    CONTACT-INFO "TBD"
    DESCRIPTION
        "This MIB module defines statistics counters for DNS servers."

    REVISION "200001010000Z"
    DESCRIPTION
        "TBD"

    ::= { mib-2 9999 }


-- table of contents

dnsStatsGeneral          OBJECT IDENTIFIER ::= { dnsStatsMIB 1 }
dnsStatsCounters         OBJECT IDENTIFIER ::= { dnsStatsMIB 2 }
    dnsStatsCntInRequest OBJECT IDENTIFIER ::= { dnsStatsCounters 1 }
    dnsStatsCntInQuery   OBJECT IDENTIFIER ::= { dnsStatsCounters 2 }
    dnsStatsCntOutQuery  OBJECT IDENTIFIER ::= { dnsStatsCounters 3 }
    dnsStatsCntServer    OBJECT IDENTIFIER ::= { dnsStatsCounters 4 }
dnsStatsConformance      OBJECT IDENTIFIER ::= { dnsStatsMIB 3 }
    dnsStatsGroups       OBJECT IDENTIFIER ::= { dnsStatsConformance 1 }
    dnsStatsCompliance   OBJECT IDENTIFIER ::= { dnsStatsConformance 2 }


-- textual conventions

DnsOpCode ::= TEXTUAL-CONVENTION
    DISPLAY-HINT "d"
    STATUS current
    DESCRIPTION
        "This textual convention is used to represent the DNS OPCODE
         values used in the header section of DNS messages.  Existing
         standard OPCODE values are listed at
         <http://www.iana.org/assignments/dns-parameters>."
    SYNTAX Integer32 (0..15)

DnsType ::= TEXTUAL-CONVENTION
    DISPLAY-HINT "d"
    STATUS current
    DESCRIPTION
```

```
        "This data type is used to represent the type values which
         appear in Resource Records in the DNS.  A 16-bit unsigned
         integer is used to allow room for new record types to be
         defined.  Existing standard types are listed at
         <http://www.iana.org/assignments/dns-parameters>."
    SYNTAX Integer32 (0..65535)


-- general stuff

dnsStatsDiscontinuityTime OBJECT-TYPE
    SYNTAX TimeStamp
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "The value of sysUpTime on the most recent occasion at which any
         one of this MIB's counters suffered a discontinuity.

         If no such discontinuities have occurred since the last
         re-initialization of the local management subsystem, then this
         object contains a zero value."
    ::= { dnsStatsGeneral 1 }


-- counters

--- incoming requests

dnsStatsCntInRequestTotal OBJECT-TYPE
    SYNTAX Counter64
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "Total number of incoming DNS requests."
    ::= { dnsStatsCntInRequest 1 }

dnsStatsCntInRequestTable OBJECT-TYPE
    SYNTAX SEQUENCE OF DnsStatsCntInRequestEntry
    MAX-ACCESS not-accessible
    STATUS current
    DESCRIPTION
        "The number of incoming DNS requests for each OPCODE."
    ::= { dnsStatsCntInRequest 2 }

dnsStatsCntInRequestEntry OBJECT-TYPE
    SYNTAX DnsStatsCntInRequestEntry
    MAX-ACCESS not-accessible
    STATUS current
```

```
    DESCRIPTION
        "The number of incoming DNS requests for a single OPCODE."
    INDEX { dnsStatsCntInRequestOpcode }
    ::= { dnsStatsCntInRequestTable 1 }

DnsStatsCntInRequestEntry ::=
    SEQUENCE {
        dnsStatsCntInRequestOpcode   DnsOpCode,
        dnsStatsCntInRequestCount    Counter64
    }

dnsStatsCntInRequestOpcode OBJECT-TYPE
    SYNTAX DnsOpCode
    MAX-ACCESS not-accessible
    STATUS current
    DESCRIPTION
        "DNS OPCODE of incoming requests."
    ::= { dnsStatsCntInRequestEntry 1 }

dnsStatsCntInRequestCount OBJECT-TYPE
    SYNTAX Counter64
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "The number of incoming DNS requests for a single OPCODE."
    ::= { dnsStatsCntInRequestEntry 2 }


--- incoming queries

dnsStatsCntInQueryTotal OBJECT-TYPE
    SYNTAX Counter64
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "Total number of incoming DNS queries."
    ::= { dnsStatsCntInQuery 1 }

dnsStatsCntInQueryTable OBJECT-TYPE
    SYNTAX SEQUENCE OF DnsStatsCntInQueryEntry
    MAX-ACCESS not-accessible
    STATUS current
    DESCRIPTION
        "The number of incoming queries for each RR type."
    ::= { dnsStatsCntInQuery 2 }

dnsStatsCntInQueryEntry OBJECT-TYPE
    SYNTAX DnsStatsCntInQueryEntry
```

```
    MAX-ACCESS not-accessible
    STATUS current
    DESCRIPTION
        "The number of incoming queries for a single RR type."
    INDEX { dnsStatsCntInQueryType }
    ::= { dnsStatsCntInQueryTable 1 }

DnsStatsCntInQueryEntry ::=
    SEQUENCE {
        dnsStatsCntInQueryType   DnsType,
        dnsStatsCntInQueryCount  Counter64
    }

dnsStatsCntInQueryType OBJECT-TYPE
    SYNTAX DnsType
    MAX-ACCESS not-accessible
    STATUS current
    DESCRIPTION
        "RR type of incoming queries."
    ::= { dnsStatsCntInQueryEntry 1 }

dnsStatsCntInQueryCount OBJECT-TYPE
    SYNTAX Counter64
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "The number of incoming DNS queries for a single RR type."
    ::= { dnsStatsCntInQueryEntry 2 }


--- outgoing queries

dnsStatsCntOutQueryTotal OBJECT-TYPE
    SYNTAX Counter64
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "Total number of outgoing DNS queries."
    ::= { dnsStatsCntOutQuery 1 }

dnsStatsCntOutQueryTable OBJECT-TYPE
    SYNTAX SEQUENCE OF DnsStatsCntOutQueryEntry
    MAX-ACCESS not-accessible
    STATUS current
    DESCRIPTION
        "The number of outgoing queries for each RR type."
    ::= { dnsStatsCntOutQuery 2 }
```

```
dnsStatsCntOutQueryEntry OBJECT-TYPE
    SYNTAX DnsStatsCntOutQueryEntry
    MAX-ACCESS not-accessible
    STATUS current
    DESCRIPTION
        "The number of outgoing queries for a single RR type."
    INDEX { dnsStatsCntOutQueryType }
    ::= { dnsStatsCntOutQueryTable 1 }

DnsStatsCntOutQueryEntry ::=
    SEQUENCE {
        dnsStatsCntOutQueryType   DnsType,
        dnsStatsCntOutQueryCount  Counter64
    }

dnsStatsCntOutQueryType OBJECT-TYPE
    SYNTAX DnsType
    MAX-ACCESS not-accessible
    STATUS current
    DESCRIPTION
        "RR type of outgoing queries."
    ::= { dnsStatsCntOutQueryEntry 1 }

dnsStatsCntOutQueryCount OBJECT-TYPE
    SYNTAX Counter64
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "The number of outgoing DNS queries for a single RR type."
    ::= { dnsStatsCntOutQueryEntry 2 }


--- name server statistics

dnsStatsCntServerRequestv4 OBJECT-TYPE
    SYNTAX Counter64
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "IPv4 requests received. Note: this also counts non query
         requests."
    ::= { dnsStatsCntServer 1 }

dnsStatsCntServerRequestv6 OBJECT-TYPE
    SYNTAX Counter64
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
```

```
        "IPv6 requests received. Note: this also counts non query
         requests."
    ::= { dnsStatsCntServer 2 }

dnsStatsCntServerReqEdns0 OBJECT-TYPE
    SYNTAX Counter64
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "Requests with EDNS(0) received."
    ::= { dnsStatsCntServer 3 }

dnsStatsCntServerReqBadEDNSVer OBJECT-TYPE
    SYNTAX Counter64
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "Requests with unsupported EDNS version received."
    ::= { dnsStatsCntServer 4 }

dnsStatsCntServerReqTSIG OBJECT-TYPE
    SYNTAX Counter64
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "Requests with TSIG received."
    ::= { dnsStatsCntServer 5 }

dnsStatsCntServerReqSIG0 OBJECT-TYPE
    SYNTAX Counter64
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "Requests with SIG(0) received."
    ::= { dnsStatsCntServer 6 }

dnsStatsCntServerReqBadSIG OBJECT-TYPE
    SYNTAX Counter64
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "Requests with invalid (TSIG or SIG(0)) signature."
    ::= { dnsStatsCntServer 7 }

dnsStatsCntServerReqTCP OBJECT-TYPE
    SYNTAX Counter64
    MAX-ACCESS read-only
    STATUS current
```

```
    DESCRIPTION
        "TCP requests received."
    ::= { dnsStatsCntServer 8 }

dnsStatsCntServerAuthQryRej OBJECT-TYPE
    SYNTAX Counter64
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "Authoritative (non recursive) queries rejected."
    ::= { dnsStatsCntServer 9 }

dnsStatsCntServerRecQryRej OBJECT-TYPE
    SYNTAX Counter64
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "Recursive queries rejected."
    ::= { dnsStatsCntServer 10 }

dnsStatsCntServerXfrRej OBJECT-TYPE
    SYNTAX Counter64
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "Zone transfer requests rejected."
    ::= { dnsStatsCntServer 11 }

dnsStatsCntServerUpdateRej OBJECT-TYPE
    SYNTAX Counter64
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "Dynamic update requests rejected."
    ::= { dnsStatsCntServer 12 }

dnsStatsCntServerResponse OBJECT-TYPE
    SYNTAX Counter64
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "Responses sent."
    ::= { dnsStatsCntServer 13 }

dnsStatsCntServerRespTruncated OBJECT-TYPE
    SYNTAX Counter64
    MAX-ACCESS read-only
    STATUS current
```

```
    DESCRIPTION
        "Truncated responses sent."
    ::= { dnsStatsCntServer 14 }

dnsStatsCntServerRespEDNS0 OBJECT-TYPE
    SYNTAX Counter64
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "Responses with EDNS(0) sent."
    ::= { dnsStatsCntServer 15 }

dnsStatsCntServerRespTSIG OBJECT-TYPE
    SYNTAX Counter64
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "Responses with TSIG sent."
    ::= { dnsStatsCntServer 16 }

dnsStatsCntServerRespSIG0 OBJECT-TYPE
    SYNTAX Counter64
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "Responses with SIG(0) sent."
    ::= { dnsStatsCntServer 17 }

dnsStatsCntServerQrySuccess OBJECT-TYPE
    SYNTAX Counter64
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "Queries resulted in a successful answer. This means the query
         which returns a NOERROR response with at least one answer RR."
    ::= { dnsStatsCntServer 18 }

dnsStatsCntServerQryAuthAns OBJECT-TYPE
    SYNTAX Counter64
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "Queries resulted in authoritative answer."
    ::= { dnsStatsCntServer 19 }

dnsStatsCntServerQryNoauthAns OBJECT-TYPE
    SYNTAX Counter64
    MAX-ACCESS read-only
```

```
    STATUS current
    DESCRIPTION
        "Queries resulted in non authoritative answer."
    ::= { dnsStatsCntServer 20 }

dnsStatsCntServerQryReferral OBJECT-TYPE
    SYNTAX Counter64
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "Queries resulted in referral answer."
    ::= { dnsStatsCntServer 21 }

dnsStatsCntServerQryNxrrset OBJECT-TYPE
    SYNTAX Counter64
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "Queries resulted in NOERROR responses with no data."
    ::= { dnsStatsCntServer 22 }

dnsStatsCntServerQrySERVFAIL OBJECT-TYPE
    SYNTAX Counter64
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "Queries resulted in SERVFAIL."
    ::= { dnsStatsCntServer 23 }

dnsStatsCntServerQryFORMERR OBJECT-TYPE
    SYNTAX Counter64
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "Queries resulted in FORMERR."
    ::= { dnsStatsCntServer 24 }

dnsStatsCntServerQryNXDOMAIN OBJECT-TYPE
    SYNTAX Counter64
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "Queries resulted in NXDOMAIN."
    ::= { dnsStatsCntServer 25 }

dnsStatsCntServerQryRecursion OBJECT-TYPE
    SYNTAX Counter64
    MAX-ACCESS read-only
```

```
    STATUS current
    DESCRIPTION
        "Queries which caused the server to perform recursion in order
         to find the final answer."
    ::= { dnsStatsCntServer 26 }

dnsStatsCntServerQryDuplicate OBJECT-TYPE
    SYNTAX Counter64
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "Queries which the server attempted to recurse but discovered an
         existing query with the same IP address, port, query ID, name,
         type and class already being processed."
    ::= { dnsStatsCntServer 27 }

dnsStatsCntServerQryDropped OBJECT-TYPE
    SYNTAX Counter64
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "Recursive queries for which the server discovered an excessive
         number of existing recursive queries for the same name, type
         and class and were subsequently dropped."
    ::= { dnsStatsCntServer 28 }

dnsStatsCntServerQryFailure OBJECT-TYPE
    SYNTAX Counter64
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "Other query failures."
    ::= { dnsStatsCntServer 29 }

dnsStatsCntServerXfrReqDone OBJECT-TYPE
    SYNTAX Counter64
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "Requested zone transfers completed."
    ::= { dnsStatsCntServer 30 }

dnsStatsCntServerUpdateReqFwd OBJECT-TYPE
    SYNTAX Counter64
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "Update requests forwarded."
```

```
    ::= { dnsStatsCntServer 31 }

dnsStatsCntServerUpdateRespFwd OBJECT-TYPE
    SYNTAX Counter64
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "Update responses forwarded."
    ::= { dnsStatsCntServer 32 }

dnsStatsCntServerUpdateFwdFail OBJECT-TYPE
    SYNTAX Counter64
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "Dynamic update forward failed."
    ::= { dnsStatsCntServer 33 }

dnsStatsCntServerUpdateDone OBJECT-TYPE
    SYNTAX Counter64
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "Dynamic updates completed."
    ::= { dnsStatsCntServer 34 }

dnsStatsCntServerUpdateFail OBJECT-TYPE
    SYNTAX Counter64
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "Dynamic updates failed."
    ::= { dnsStatsCntServer 35 }

dnsStatsCntServerUpdateBadPrereq OBJECT-TYPE
    SYNTAX Counter64
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "Dynamic updates rejected due to prerequisite failure."
    ::= { dnsStatsCntServer 36 }


-- conformance groups

-- TBD

END
```

4. Security Considerations

TBD

5. IANA Considerations

TBD

6. Acknowledgements

This module is heavily based on the documentation of the statistics provided by Bind 9.8 [Bind].

7. References

7.1. Normative References

[RFC2578] McCloghrie, K., Ed., Perkins, D., Ed., and J. Schoenwaelder, Ed., "Structure of Management Information Version 2 (SMIv2)", STD 58, RFC 2578, April 1999.

[RFC2579] McCloghrie, K., Ed., Perkins, D., Ed., and J. Schoenwaelder, Ed., "Textual Conventions for SMIv2", STD 58, RFC 2579, April 1999.

[RFC3411] Harrington, D., Presuhn, R., and B. Wijnen, "An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks", STD 62, RFC 3411, December 2002.

7.2. Informative References

[Bind] "Bind9 Statistics", <http://ftp.isc.org/isc/bind9/cur/9.8/doc/arm/Bv9ARM.ch06.html#statistics>.

[RFC3197] Austein, R., "Applicability Statement for DNS MIB Extensions", RFC 3197, November 2001.

Appendix A. Open Issues

This is a list of open issues on which we would like to get feedback.

1. There are many more statistics produced by Bind. There are also other stats from Unbound and NSD that could be added. Should we

add more?

2. The current version does not include any notification. Should this be added? Would it even be desirable to add to already-busy DNS servers the burden of sending notifications?

3. Should we add per-zone stats? Should they be indexed by zone name, by something else, or not indexed at all?

4. Should we add per-view stats? (A "view" is a Bind-specific concept.) Is the "context" concept from SNMPv3 already sufficient? That is, a view can be seen as a different DNS server running on the same system...

5. How should we define conformance groups? Go with the traditional "recursive", "authoritative", "mixed" classification?

Authors' Addresses

Simon Perreault
Viagenie
246 Aberdeen
Quebec, QC G1R 2E1
Canada

Phone: +1 418 656 9254
Email: simon.perreault@viagenie.ca
URI: http://viagenie.ca

Jacques Latour
Canadian Internet Registration Authority (CIRA)
350 Sparks Street, Suite 306
Ottawa, ON K1R 7S8
Canada

Email: jacques.latour@cira.ca
URI: http://cira.ca

Jake Zack
Canadian Internet Registration Authority (CIRA)
350 Sparks Street, Suite 306
Ottawa, ON K1R 7S8
Canada

Email: jake.zack@cira.ca
URI: http://cira.ca