Zonemaster
A new DNS testing tool

Patrik Wallström, .SE
DNSCheck

DNSCheck is a program that was designed to help people check, measure and hopefully also understand the workings of the Domain Name System, DNS.
Background

• DNSCheck does not give truly deterministic results

• ZoneCheck written in Ruby, old legacy code

• AFNIC and .SE needed better tools for DNS measurements

• Decision to create a joint “reference” tool
The Collaboration

- Based on DNSCheck and ZoneCheck
  - Joint requirements and specifications
- Collaboration between AFNIC and .SE
- A new tool with a great name
Requirements

- For version 1.0:
  - All test cases from DNSCheck and ZoneCheck
  - All functionality from DNSCheck and ZoneCheck
  - Modular code
  - Faster, and lower impact on network!
<table>
<thead>
<tr>
<th>Req</th>
<th>Requirement description</th>
<th>Level and Test Case</th>
</tr>
</thead>
<tbody>
<tr>
<td>R01</td>
<td>UDP connectivity</td>
<td>CONNECTIVITY</td>
</tr>
<tr>
<td>R02</td>
<td>TCP connectivity</td>
<td>CONNECTIVITY</td>
</tr>
<tr>
<td>R03</td>
<td>Address in a private network</td>
<td>ADDRESS</td>
</tr>
<tr>
<td>R04</td>
<td>Address should not be part of a bogon prefix</td>
<td>ADDRESS</td>
</tr>
<tr>
<td>R05</td>
<td>Illegal symbols in domain name</td>
<td>SYNTAX</td>
</tr>
<tr>
<td>R06</td>
<td>Dash ('-') at start or beginning of domain name</td>
<td>SYNTAX</td>
</tr>
<tr>
<td>R07</td>
<td>Double dash in domain name</td>
<td>SYNTAX</td>
</tr>
<tr>
<td>R09</td>
<td>At least two nameservers for the domain</td>
<td>DELEGATION</td>
</tr>
<tr>
<td>R10</td>
<td>Identical addresses</td>
<td>DELEGATION</td>
</tr>
<tr>
<td>R11</td>
<td>Nameserver addresses on same subnet</td>
<td>CONNECTIVITY</td>
</tr>
<tr>
<td>R12</td>
<td>Nameserver addresses are all on the same subnet</td>
<td>CONNECTIVITY</td>
</tr>
<tr>
<td>R13</td>
<td>Delegation response fit in a 512 byte UDP packet</td>
<td>DELEGATION</td>
</tr>
<tr>
<td>R14</td>
<td>Delegation response with additional fit in a 512 byte UDP packet</td>
<td>DELEGATION</td>
</tr>
<tr>
<td>R15</td>
<td>NS record present</td>
<td>BASIC</td>
</tr>
<tr>
<td>R16</td>
<td>NS authoritative answer</td>
<td>DELEGATION</td>
</tr>
<tr>
<td>R17</td>
<td>NS name has a valid domain/hostname syntax</td>
<td>SYNTAX</td>
</tr>
<tr>
<td>Req</td>
<td>Requirement description</td>
<td>Level</td>
</tr>
<tr>
<td>------</td>
<td>-----------------------------------------</td>
<td>---------------</td>
</tr>
<tr>
<td>R01</td>
<td>UDP connectivity</td>
<td>Connectivity-TP</td>
</tr>
<tr>
<td>R02</td>
<td>TCP connectivity</td>
<td>Connectivity-TP</td>
</tr>
<tr>
<td>R03</td>
<td>address in a private network</td>
<td>Address-TP</td>
</tr>
<tr>
<td>R04</td>
<td>address should not be part of a bogon prefix</td>
<td>Address-TP</td>
</tr>
<tr>
<td>R05</td>
<td>illegal symbols in domain name</td>
<td>Syntax-TP</td>
</tr>
<tr>
<td>R06</td>
<td>dash ('-') at start or beginning of domain name</td>
<td>Syntax-TP</td>
</tr>
<tr>
<td>R07</td>
<td>double dash in domain name</td>
<td>Syntax-TP</td>
</tr>
</tbody>
</table>
CONNECTIVITY01: UDP connectivity

Test case identifier

CONNECTIVITY01: UDP connectivity

Objective

DNS queries are sent using UDP on port 53, as described in section 4.2.1 of RFC 1035.

The objective for this test is that all the authoritative name servers for the domain are accessible over UDP on port 53

Inputs

The domain to be tested.

Ordered description of steps to be taken to execute the test case

1. Obtains the IP address of the name servers from Method4 and Method5
2. A SOA query is sent over UDP to distint IP addresses of each name server found in step 1.
3. If all queries in step 2 receive a DNS answer (bogus responses are not checked here) then the test case succeed.

Outcome(s)

If there is any name server that fails to answer queries over port 53 using UDP, this test case fails

Special procedural requirements

If either IPv4 or IPv6 transport is disabled, ignore the evaluation of the result of any test using this transport protocol.
Log a message reporting on the ignored result.

Intercaase dependencies

None
Implementation

- Written in Perl...
  - Engine
  - CLI
  - Backend
  - GUI (Javascript + Perl)
Zonemaster Engine

- A Perl library (`Zonemaster::*`)
  - That implements
    - All functionality for testing
    - All the test cases
    - Functionality for logging results
    - Its own resolver
      - That uses `Net::LDNS` (built on ldns) instead of `Net::DNS`
Zonemaster CLI

• Takes its input from a user
• Executes a test
• Publishes a log
  • Log as text, raw text - or JSON
Zonemaster Backend

- JSON-RPC-interface to the Engine
- Used by the GUI to execute tests
- Can also be used by other applications for batch testing
Zonemaster GUI

- The UI to run tests
- … and present the result
- Is available at zonemaster.net
Domain name

Test # 8828

Executed at 2015-04-27T10:25+0200

Link

http://zonemaster.net/test/8828

Basic Advanced Export History

- ✓ SYSTEM
- ✓ BASIC
- ✓ ADDRESS
- ✓ CONNECTIVITY
- ✓ CONSISTENCY
- ✓ DNSSEC
- ✓ DELEGATION
- ✓ NAMESERVER
- ✓ SYNTAX
- ✓ ZONE
Releases

• The four components can be released independently

• “Zonemaster Distribution” releases
Installation


**sudo cpan -i Zonemaster**

sudo apt-get install libmoosex-getopt-perl libtext-reflow-perl libmodule-install-perl

**sudo cpan -i Zonemaster::CLI**
How to run a test?

```
$> zonemaster-cli blipp.com
Seconds  Level       Message
-------- --------       ------------
  8.25   NOTICE  Nameserver boa.blipp.com has an IP address (2001:1b40:5600:900:4321:1234:9b92:4bc0) with mismatched PTR result (snake.blipp.com.).
  8.25   NOTICE  Nameserver boa.blipp.com has an IP address (95.154.217.14) with mismatched PTR result (snake.blipp.com.).
  8.25   NOTICE  Nameserver vic20.blipp.com has an IP address (2001:16d8:ff00:2a9::2) with mismatched PTR result (cl-682.sto-01.se.sixxs.net.).
 33.47   NOTICE  Nameserver boa.blipp.com/2001:1b40:5600:900:4321:1234:9b92:4bc0 allow zone transfer using AXFR.
 33.57   NOTICE  Nameserver boa.blipp.com/95.154.217.14 allow zone transfer using AXFR.
 34.40   NOTICE  Nameserver vic20.blipp.com/192.195.142.21 allow zone transfer using AXFR.
 34.42   NOTICE  Nameserver vic20.blipp.com/2001:16d8:ff00:2a9::2 allow zone transfer using AXFR.
```
usage: zonemaster-cli [-?h] [long options...]

-h -? --usage --help  Prints this usage information.
--version  Print version information and exit.
--level    The minimum severity level to display. Must be one of CRITICAL, ERROR, WARNING, NOTICE, INFO or DEBUG.
--locale   The locale to use for messages translation.
--json     Flag indicating if output should be in JSON or not.
--raw      Flag indicating if output should be translated to human language or dumped raw.
--time     Print timestamp on entries.
--show_level Print level on entries.
--show_module Print the name of the module on entries.
--ns       A name/ip string giving a nameserver for undelegated tests. Can be given multiple times.
--save     Name of a file to save DNS data to after running tests.
--restore  Name of a file to restore DNS data from before running test.
--ipv4     Flag to permit or deny queries being sent via IPv4. --ipv4 permits IPv4 traffic, --no-ipv4 forbids it.
--ipv6     Flag to permit or deny queries being sent via IPv6. --ipv6 permits IPv6 traffic, --no-ipv6 forbids it.
--list_tests Instead of running a test, list all available tests.
--test     Specify test to run. Should be either the name of a module, or the name of a module and the name of a method in that module separated by a "/" character (Example: "Basic/basic1"). The method specified must be one that takes a zone object as its single argument. This switch can be repeated.
--stop_level As soon as a message at this level or higher is logged, execution will stop. Must be one of CRITICAL, ERROR, WARNING, NOTICE, INFO or DEBUG.
--config   Name of configuration file to load.
--policy   Name of policy file to load.
--ds       Strings with DS data on the form "keytag,algorithm,type,digest"
--count    Print a count of the number of messages at each level
--progress Boolean flag for activity indicator. Defaults to on if STDOUT is a tty, off if it is not.
--encoding Name of the character encoding used for command line arguments
--nstimess At the end of a run, print a summary of the times the zone's name servers took to answer.
--dump_config Print the effective configuration used in JSON format, then exit.
--dump_policy Print the effective policy used in JSON format, then exit.
CLI Features

• Pre-delegation tests
• Record a dump of queries+answers
• Use answers from a recorded dump
• Stop execution at specific log level
• Use different policy evaluating the results
• Record name server response times
• Human readable output in Swedish and French ;)

[AFNIC Logo]
Log levels

- DEBUG 1, 2, 3
- INFO
- NOTICE
- WARNING
- ERROR
- CRITICAL

Configured by policy
$> zonemaster-cli --dump_policy
{
    "ADDRESS" : {
        "NAMESERVERS_IP_WITH_REVERSE" : "INFO",
        "NAMESERVER_IP_PRIVATE_NETWORK" : "ERROR",
        "NAMESERVER_IP_PTR_MATCH" : "INFO",
        "NAMESERVER_IP_PTR_MISMATCH" : "NOTICE",
        "NAMESERVER_IP_WITHOUT_REVERSE" : "WARNING",
        "NO_IP_PRIVATE_NETWORK" : "INFO",
        "NO_RESPONSE_PTR_QUERY" : "WARNING"
    },
    ...
}
<table>
<thead>
<tr>
<th>Seconds</th>
<th>Level</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.25</td>
<td>NOTICE</td>
<td>Nameserver boa.blipp.com has an IP address (2001:1b40:5600:900:4321:1234:9b92:4bc0) with mismatched PTR result (snake.blipp.com.).</td>
</tr>
<tr>
<td>8.25</td>
<td>NOTICE</td>
<td>Nameserver boa.blipp.com has an IP address (95.154.217.14) with mismatched PTR result (snake.blipp.com.).</td>
</tr>
<tr>
<td>8.25</td>
<td>NOTICE</td>
<td>Nameserver vic20.blipp.com has an IP address (2001:16d8:ff00:2a9::2) with mismatched PTR result (cl-682.sto-01.se.sixxs.net.).</td>
</tr>
<tr>
<td>33.47</td>
<td>NOTICE</td>
<td>Nameserver boa.blipp.com/2001:1b40:5600:900:4321:1234:9b92:4bc0 allow zone transfer using AXFR.</td>
</tr>
<tr>
<td>33.57</td>
<td>NOTICE</td>
<td>Nameserver boa.blipp.com/95.154.217.14 allow zone transfer using AXFR.</td>
</tr>
<tr>
<td>34.40</td>
<td>NOTICE</td>
<td>Nameserver vic20.blipp.com/192.195.142.21 allow zone transfer using AXFR.</td>
</tr>
<tr>
<td>34.42</td>
<td>NOTICE</td>
<td>Nameserver vic20.blipp.com/2001:16d8:ff00:2a9::2 allow zone transfer using AXFR.</td>
</tr>
</tbody>
</table>
Log - Raw

$> zonemaster-cli --raw blipp.com

  8.13 NOTICE  ADDRESS:NAMESERVER_IP_PTR_MISMATCH
  address=2001:1b40:5600:900:4321:1234:9b92:4bc0, names=snake.blipp.com., ns=boa.blipp.com

  8.13 NOTICE  ADDRESS:NAMESERVER_IP_PTR_MISMATCH address=95.154.217.14,
  names=snake.blipp.com., ns=boa.blipp.com

  8.13 NOTICE  ADDRESS:NAMESERVER_IP_PTR_MISMATCH address=2001:16d8:ff00:2a9::2,
  names=cl-682.sto-01.se.sixxs.net., ns=vic20.blipp.com

  33.60 NOTICE  NAMESERVER:AXFR_AVAILABLE
  address=2001:1b40:5600:900:4321:1234:9b92:4bc0, ns=boa.blipp.com

  33.74 NOTICE  NAMESERVER:AXFR_AVAILABLE address=95.154.217.14, ns=boa.blipp.com

  34.57 NOTICE  NAMESERVER:AXFR_AVAILABLE address=192.195.142.21, ns=vic20.blipp.com

  34.59 NOTICE  NAMESERVER:AXFR_AVAILABLE address=2001:16d8:ff00:2a9::2,
  ns=vic20.blipp.com
Log - JSON

$> zonemaster-cli --json blipp.com

[{
"args":
{"address": "2001:1b40:5600:900:4321:1234:9b92:4bc0", "names": "snake.blipp.com.", "ns": "boa.blipp.com"},
"level": "NOTICE",
"module": "ADDRESS",
"tag": "NAMESERVER_IP_PTR_MISMATCH",
"timestamp": 8.25753903388977}, {
"args":
{"address": "95.154.217.14", "names": "snake.blipp.com.", "ns": "boa.blipp.com"},
"level": "NOTICE",
"module": "ADDRESS",
"tag": "NAMESERVER_IP_PTR_MISMATCH",
"timestamp": 8.25794792175293}, {
"args":
{"address": "2001:16d8:ff00:2a9::2", "names": "cl-682.sto-01.se.sixxs.net.", "ns": "vic20.blipp.com"},
"level": "NOTICE",
"module": "ADDRESS",
"tag": "NAMESERVER_IP_PTR_MISMATCH",
"timestamp": 8.26008701324463}, {
"args":
{"address": "2001:1b40:5600:900:4321:1234:9b92:4bc0", "ns": "boa.blipp.com"},
"level": "NOTICE",
"module": "NAMESERVER",
"tag": "AXFRAVAILABLE",
"timestamp": 33.5192708969116}, {
"args":
{"address": "95.154.217.14", "ns": "boa.blipp.com"},
"level": "NOTICE",
"module": "NAMESERVER",
"tag": "AXFRAVAILABLE",
"timestamp": 33.6047399044037}, {
"args":
{"address": "192.195.142.21", "ns": "vic20.blipp.com"},
"level": "NOTICE",
"module": "NAMESERVER",
"tag": "AXFRAVAILABLE",
"timestamp": 34.4463429450989}, {
"args":
{"address": "2001:16d8:ff00:2a9::2", "ns": "vic20.blipp.com"},
"level": "NOTICE",
"module": "NAMESERVER",
"tag": "AXFR_AVAILABLE",
"timestamp": 34.4668040275574}]

afnic
.se
Anatomy of a log entry

[
{
"tag" : "TEST_CASE_TAG",
"timestamp" : 6.35820984840393,
"module" : "TEST-MODULE",
"level" : "MESSAGELEVEL",
"args" : {
    "ns" : "nameserver.tld",
    "address" : "127.0.0.1"
}
},
{...
}
The .SE Healthcheck
Healthcheck Categories

- 57 State owned companies
- 81 Banks, financial institutes and insurance companies
- 21 Internet Service Providers (ISPs)
- 290 Municipalities
- 20 Counties
- 36 Media companies
- 229 Government agencies
- 37 Universities and higher education
- 151 Registrars
Number of ASNs
Open recursors
use Zonemaster;

# execute a test
my @log = Zonemaster->test_zone( 'blipp.com');
my $json = Zonemaster->logger->json( 'NOTICE');

# get name servers for a zone
my $zone = Zonemaster->zone( 'another-zone.com');
my $nameservers = join ( ' ', @{ $zone->ns_names } );
expo$~>zonemaster-info ripe.net

Zone: ripe.net
Parent zone: net

Glue nameserver list:
- ns3.nic.fr/192.134.0.49
- ns3.nic.fr/2001:660:3006:1::1
- pri.authdns.ripe.net/193.0.9.5
- pri.authdns.ripe.net/2001:67c:e0::5
- sec1.apnic.net/202.12.29.59
- sec3.apnic.net/2001:dc0:1:0:4777::140
- sec3.apnic.net/202.12.28.140
- sns-pb.isc.org/192.5.4.1
- sns-pb.isc.org/2001:500:2e::1
- tinnie.arin.net/199.212.0.53
- tinnie.arin.net/2001:500:13::c7d4:35

Authoritative nameserver list:
- ns3.nic.fr/192.134.0.49
- ns3.nic.fr/2001:660:3006:1::1
- pri.authdns.ripe.net/193.0.9.5
- pri.authdns.ripe.net/2001:67c:e0::5
- sec1.apnic.net/202.12.29.59
- sec3.apnic.net/2001:dc0:1:0:4777::140
- sec3.apnic.net/202.12.28.140
- sns-pb.isc.org/192.5.4.1
- sns-pb.isc.org/2001:500:2e::1
- tinnie.arin.net/199.212.0.53
- tinnie.arin.net/2001:500:13::c7d4:35

Parent has DS record(s) for ripe.net.
- Key tag: 65306 Digest algorithm: SHA-256
- Key tag: 65306 Digest algorithm: SHA-1

DNSKEY records:
- Tag: 65306 Algorithm: RSA/SHA1
- Tag: 964 Algorithm: RSA/SHA1
- Tag: 14716 Algorithm: RSA/SHA1
- Tag: 8937 Algorithm: RSA/SHA1

SOA record:
- MNAME: pri.authdns.ripe.net.
- RNAME: dns.ripe.net.
- Serial: 1431002041
- Refresh: 3600
- Retry: 600
- Expire: 864000
- Minimum: 300

SOA record signature(s):
- Keytag: 14716
- Algorithm: RSA/SHA1
- Labels: 2
- Signer: ripe.net.
- Expiration: 2015-06-06 14:38:32
“zonemaster-collector”

- My own tool for mass collection
- Multi-threaded use of Zonemaster
- Storage in MongoDB
- Easy to query a lot of test data

- [https://github.com/pawal/zonemaster-collector](https://github.com/pawal/zonemaster-collector)
  - Examples in the “howtomongo” document
Mass collection

$ collect.pl -f 10000.txt --mongo --db results --collection foo --threads 35
Query example 1

# results in a list of open resolvers

db.domains.aggregate(
   { $match: { "result.tag": "IS_A_RECURSOR" } },
   { $unwind: "$result" },
   { $match: { "result.tag": "IS_A_RECURSOR" } },
   { $project: { "name":1, "result.args": 1, "_id": 0 } }
);

{
   "result" : {
      "args" : {
         "ns" : "ns2.example.com",
         "address" : "12.34.56.78",
         "dname" : "xx--domain-cannot-exist.xx--illegal-syntax-tld"
      }
   },
   "name" : "example.com"
}, ...
db.domains.aggregate(
    { $match: { "result.level": "ERROR" } },
    { $unwind: "$result" },
    { $match: { "result.level": "ERROR" } },
    { $match: { "result.args.ns": { $exists: true } } },
    { $project: { "name":1, "result": 1, "_id": 0 } },
    { $group: { _id: "$result.args.ns", nscount: { $sum: 1 } } },
    { $sort: { nscount: -1 } },
    { $limit: 25 }
);

{
    "result": [
        {
            "_id": "ns1.example.com",
            "nscount": 233
        },
        {
            "_id": "ns2.example.com",
            "nscount": 232
        },
        ...
    ]
}
Top list of errors

- 1614 NS_FAILED
- 1002 NAMESERVER_NO_TCP_53
- 456 IS_A_RECURSOR
- 410 EXTRA_NAME_PARENT
- 366 NAMESERVER_NO_UDP_53
- 327 TOTAL_NAME_MISMATCH
- 142 HAS_A_RECORDS (broken NS delegation)
Future improvements

• Fix all the log imperfection
• Implement new test requirements
• “IANA test profile” - different test profiles/policies
• HTML export of results
What do you need?

• Batch testing from CLI?

• Anycast testing?

• Mobile apps?

• Any specific test case? (They are easy to write and just “plugin” to the existing framework.)
TRTF

- The test specifications will be further refined by a new CENTR task force, the TRTF
- The goal is to have a best practices document
- Published as an informational RFC
TRTF status

- Mailinglist created in November 2014
  - A little activity right after that without followups
- Mats Dufberg starts working in December 2014
  - First overview of requirements posted in February
- I take over the work late April
The way forward

• Follow up on my suggestions made in April

• Decide on document format (Markdown, but also content)

• The scope of the work (Requirements and later Specifications?)

• Write detailed example requirements

• Arrange a F2F meeting…
Participate!

https://github.com/CENTRccTLDs/TRTF
Test Zooonemaster yourself!

- https://github.com/dotse/zonemaster
- http://lists.iis.se/cgi-bin/mailman/admin/zonemaster-users
- http://lists.iis.se/cgi-bin/mailman/admin/zonemaster-devel