DNS measurements with RIPE Atlas

Stéphane Bortzmeyer

bortzmeyer@nic.fr

Domain Name System

Domain Name System

- A part of the Internet infrastructure,

Domain Name System

- A part of the Internet infrastructure,
- As necessary as IP,

Domain Name System

- A part of the Internet infrastructure,
- As necessary as IP,
- Often forgotten in studies about resilience or quality of service.
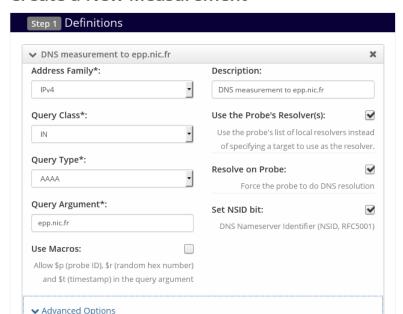
RIPE Atlas and DNS

RIPE Atlas and DNS

- RIPE Atlas probes can do DNS measurements,

RIPE Atlas and DNS

- RIPE Atlas probes can do DNS measurements,
- Many options in
  `https://atlas.ripe.net/docs/api/v2/reference/#/measurem`

Web interface

Create a New Measurement

Result

📖⁴ DNS measurement to epp.nic.fr

General Information	Probes	Map	Results

Probe ⇕	ASN (IPv4) ⇕	ASN (IPv6) ⇕	⇕ ⇕	Time (UTC) ⇕	Answer ⇕	NSID	⇕	Response Time
6012	3333	3333	🇳🇱 ☁	2017-10-02 15:34	NOERROR	nl-ams-as3333-test.anchors.atlas.ripe.net		926.075
13482	13046		🇭🇷 ☁	2017-10-02 15:34	NOERROR	null		71.779
16336	5603		🇸🇮 ☁	2017-10-02 15:34	FORMERR			29.287
16556	56402		🏳 ☁	2017-10-02 15:34	NOERROR	null		620.774
16795	42525		🇩🇰 ☁	2017-10-02 15:34	NOERROR	null		82.798
23445	17501		🇳🇵 ☁	2017-10-02 15:34	NOERROR	null		404.175
23860	50316		🇮🇹 ☁	2017-10-02 15:34	NOERROR	null		54.959
28562	35807		🇷🇺 ☁	2017-10-02 15:34	NOERROR	null		16
30266	12418		🇷🇺 ☁	2017-10-02 15:34	NOERROR	null		1
32044	60294		🇩🇪 ☁	2017-10-02 15:34	NOERROR	null		20.379

From the API

```
{'definitions': [{'protocol': 'UDP',
     'description': 'DNS resolution of ns.eu.org', 'af': 4,
     'query_argument': 'ns.eu.org', 'query_type': 'AAAA',
     'query_class': 'IN', 'set_rd_bit': True, 'type': 'dns',
     'use_probe_resolver': True}], 'is_oneoff': True, 'probes':
  [{'requested': 10, 'type': 'area', 'value': 'WW',
     'tags': {'include': ['system-resolves-a-correctly', 'system-r
```

Many options

[dns] **udp_payload_size** (integer): Set the DNS0 option for UDP payload size to this value, between 512 and 4096.Defaults to 512),

[dns] **use_probe_resolver** (boolean): Send the DNS query to the probe's local resolvers (instead of an explicitly specified target),

[dns] **set_rd_bit** (boolean): Flag indicating Recursion Desired bit was set,

[dns] **prepend_probe_id** (boolean): Each probe prepends its probe number and a timestamp to the DNS query argument to make it unique,

[dns] **protocol** (string) = ['UDP' or 'TCP']: Protocol used in measurement. Defaults to UDP,

[dns] **retry** (integer): Number of times to retry,

[dns] **include_qbuf** (boolean): include the raw DNS query data in the result. Defaults to false,

[dns] **set_nsid_bit** (boolean): Flag indicating Name Server Identifier (RFC5001) was set,

[dns] **include_abuf** (boolean): include the raw DNS answer data in the result. Defaults to true,

[dns] **query_class** (string) = ['IN' or 'CHAOS']: The `class` part of the query used in the measurement,

[dns] **query_argument** (string): The `argument` part of the query used in the measurement,

From Magellan

Output similar to dig

```
% ripe-atlas measure dns --query-argument=lqdn.net
...
Probe #29198
======================================================================

  ; <<>> RIPE Atlas Tools <<>> lqdn.net.
  ;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 47134
  ;; flags: qr ra rd; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 10

  ;; QUESTION SECTION:
  ;lqdn.net.                        IN      A

  ;; ANSWER SECTION:
  lqdn.net.               600      IN      A      204.12.240.154
...
  ;; Query time: 386.869 msec
  ;; SERVER: 172.20.7.1#53(172.20.7.1)
  ;; WHEN: Mon Oct 02 17:43:55 CEST 2017
  ;; MSG SIZE  rcvd: 253
```

From my tool

```
% atlas-resolve --nsid --type AAAA --requested 10 \
    --country FR mamot.fr
[2a00:99a0:0:1000::7] : 9 occurrences
Test #9407903 done at 2017-10-02T15:47:28Z
```

Result in JSON

```
"from": "89.142.236.92",
"msm_id": 9668778,
"msm_name": "Tdig",
"prb_id": 16336,
"resultset": [
  {
    "dst_addr": "192.168.1.1",
    "result": {
      "ANCOUNT": 3,
      "ARCOUNT": 1,
      "ID": 10350,
      "abuf": "KG6BgAABAAMA...
```

Traps

Traps

- Some probes use strange resolvers (alternative roots, lying resolvers. . .),

Traps

- Some probes use strange resolvers (alternative roots, lying resolvers. . .),
- Some networks intercept and rewrite DNS traffic, some have transparent proxies.

Examples of use

Examples of use

- Measuring censorship (selecting probes by country).
  Warning: may raise ethical issues.

afnic

Examples of use

- Measuring censorship (selecting probes by country).
  Warning: may raise ethical issues.
- Check the different instances of an anycast server.

afnic

Examples of use

- Measuring censorship (selecting probes by country). **Warning**: may raise ethical issues.
- Check the different instances of an anycast server.
- Test that your domain name resolves from everywhere. (Many zones have all eggs in the same basket.)

afnic

Merci !