BỘ THÔNG TIN VÀ TRUYỀN THÔNG
TRUNG TÂM INTERNET VIỆT NAM

TÀI LIỆU

TÀI LIỆU TESTCASE TRIỂN KHAI THỬ NGHIỆM DNSSEC TRÊN HỆ THỐNG RECURSIVE CACHING

Quản lý phiên bản tài liệu:

Phiên bản	Ngày cập nhật	Ghi chú
1.0	08/8/2020	Biên soạn

MỤC LỤC

DANH MỤC CÁC KÝ HIỆU, CHỮ VIẾT TẮT

ccTLD	Country Code Top Level Domain
DNS	Domain Name System
DNSSEC	Domain Name System Security Extensions
ISP	Doanh nghiệp Internet
VNNIC	Vietnam Internet Network Information Center

DANH MỤC HÌNH VẼ

HƯỚNG DẪN KỊCH BẢN KIỂM THỬ (TESTCASE) DNSSEC TRÊN HỆ THỐNG RECURSIVE CACHING DNS

Tài liệu hướng dẫn các kịch bản testcase trong thử nghiệm DNSSEC trên hệ thống Recursive Caching DNS (DNS Caching). Các đơn vị (ISP) có thể thực hiện kiểm thử trên một trong hai hệ thống:

(1) ISP tự triển khai hệ thống thử nghiệm:

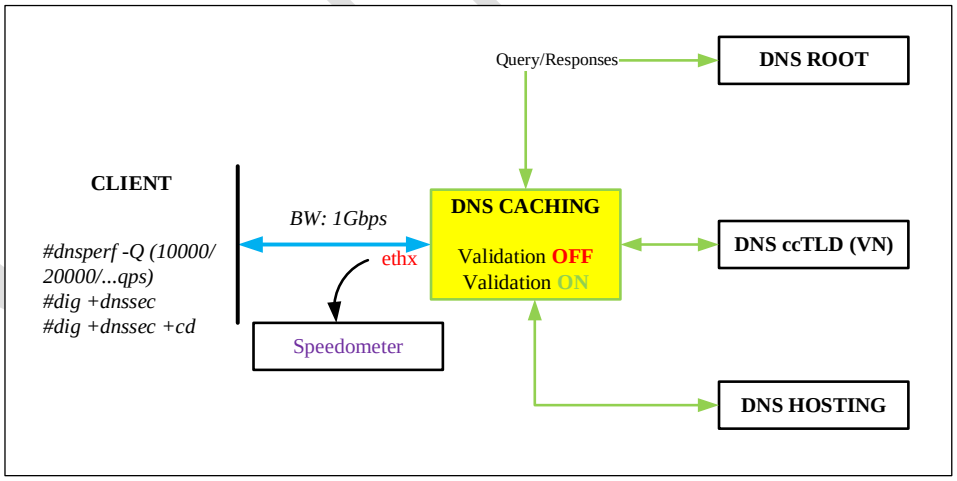
- Triển khai máy chủ DNS Caching
- Bật tính năng xác thực DNSSEC (DNSSEC Validation)
- Thử nghiệm các kịch bản theo hướng dẫn để đo kiểm và đánh giá

(2) ISP kết nối và thử nghiệm trên hệ thống thử nghiệm VNNIC

- VNNIC triển triển khai sẵn hệ thống DNS Caching đã bật tính năng DNSSEC Validation.
- ISP đăng ký kết nối để thử nghiệm.
- Thử nghiệm các kịch bản theo hướng dẫn để đo kiểm và đánh giá.

1. Hướng dẫn ISP tự triển khai hệ thống thử nghiệm

1.1. Mô hình triển khai



Hình 1: Mô hình kiểm thử DNS Caching

Mô tả:

Tại mỗi ISP triển khai xây dựng hệ thống DNS Caching thử nghiệm có kết nối đến hệ thống DNS Root và các hệ thống DNS Authoritative khác trên thực tế như mô hình ở trên (Hình 1).

Trên các Client thực hiện cài đặt và sử dụng các công cụ để tạo hàng loạt các truy vấn DNS/DNSSEC (dnsperf) nhằm kiểm tra hiệu năng, năng lực của hệ thống DNS Caching.

Thực hiện theo dõi, giám sát các thông số hệ thống như: tài nguyên, năng lực hệ thống máy chủ, băng thông bằng các công cụ giám sát như Cacti, Solarwinds,…

1.2. Các bước triển khai chính

(1) Bước 1: Chuẩn bị hạ tầng mạng và máy chủ

- Máy chủ triển khai thử nghiệm đặt tại vùng mạng đảm bảo ATTT, có băng thông đáp ứng tối thiểu 10 Mbps, tránh ảnh hưởng đến các hệ thống Production tại các đơn vị.

- Thông số cấu hình máy chủ DNS Caching: Máy chủ sử dụng để giả lập máy chủ DNS Caching có cấu hình tài nguyên tối thiểu như sau:

+ Thông số ổ cứng: 20 GB

+ Bộ nhớ RAM: 4GB

+ CPU: Tốc độ 2.0 GHz

Các phần mềm cài đặt có thông số khuyến nghị như sau:

+ Hệ điều hành: CentOS/REHL 6.x trở lên, Ubuntu 16.x trở lên,…

+ Phần mềm DNS: BIND: 9.11.x trở lên (ngoài ra có thể sử dụng các phần mềm DNS khác hỗ trợ chế độ Cache như Unbound, …).

(2) Bước 2: Triển khai cài đặt, cấu hình máy chủ

- Cài đặt máy chủ trên một số nền tảng Unix/Linux và theo các thông số khuyến nghị nêu trên.

(3) Bước 3: Cài đặt, cấu hình phần mềm DNS

- Sử dụng một số phần mềm DNS dùng cho các máy chủ Caching theo khuyến nghị như: BIND9, Unbound.

- Cấu hình máy chủ hoạt động với chức năng là một máy chủ DNS Recursive Caching, có hoạt động kết nối, truy cập được đến các hệ thống DNS trên thực tế (DNS Root, các DNS Authortitative, DNS Hosting,…) theo mô hình khuyến nghị ở trên.

- Cấu hình bật xác thực DNSSEC (Chi tiết hướng dẫn cấu hình bật xác thực DNSSEC cho phần mền BIND9 tại: https://vnnic.vn/sites/default/files/tailieu/vnnic-tailieuhuongdantrienkhaidnssec-isp-v2.0.pdf).

(4) Bước 4: Kiểm tra hoạt động.

- Kiểm tra hoạt động truy vấn DNS thông thường

- Kiểm tra hoạt động truy vấn có xác thực DNSSEC

2. Các công cụ triển khai hỗ trợ

2.1. Công cụ DIG

DIG là viết tắt của Domain Information Groper là một công cụ dòng lệnh quản trị mạng được dùng để tra cứu và chẩn đoán hoạt động truy vấn DNS. Công cụ này được cài đặt kèm trong gói phần mềm BIND.

- Cú pháp sử dụng cơ bản: dig [server] [name] [type]

Trong đó:

+ [server] – địa chỉ IP hoặc hostname của name server sẽ dùng để thực hiện truy vấn.

+ [name] – tên của bản ghi tài nguyên tên miền (resource records) sẽ được truy vấn.

+ [type] – loại truy vấn được yêu cầu bởi dig. Nó có thể là 1 trong số các bản ghi: A, MX, SOA,…Nếu không có bản ghi nào được chỉ định thì dig sẽ mặc định đó là bản ghi A.

2.2. Công cụ dnsperf

Dnsperf là các công cụ tạo ra các truy vấn nhằm giúp đơn giản hóa việc thu thập số liệu độ trễ và các thông số truyền tải chính xác cho dịch vụ hệ thống DNS.

Dnsperf tạo tải truy vấn DNS để mô phỏng trên các điều kiện mạng khác nhau với các truy vấn DNS thông thường hay cả DNSSEC và đo chính xác về các phép đo độ trễ trên mỗi gói truy vấn, kích thước gói tin DNS và tải truy vấn rất chính xác.

Chi tiết cài đặt và hướng dẫn sử dụng tại Phụ lục 01.

2.3. Công cụ Speedometer

Speedometer là một công cụ nhỏ gọn, thực hiện giám sát băng thông, lưu lượng nhận và phản hồi của các gói tin trên cổng mạng của máy chủ. Cho phép thực hiện giám sát theo thời gian thực và hỗ trợ hiển thị bằng biểu đồ trực quan.

Chi tiết cài đặt và hướng dẫn sử dụng tại Phụ lục 02.

2.4. Các công cụ giám sát khác

Để giám sát một các chi tiết và có hệ thống đối với hoạt động của các máy chủ DNS Caching được cài đặt về các thông số tài nguyên máy chủ, năng lực đáp ứng truy vấn và

băng thông chiếm dụng của hoạt động động truy vấn DNS. Các doanh nghiệp ISP nên thực hiện giám sát bằng các công cụ hệ thống như: Cacti, Solarwinds hay PRTG,…

3. Các kịch bản kiểm thử

Mục đích: Đánh giá mức độ ảnh hưởng khi triển khai xác thực DNSSEC trên hệ thống máy chủ DNS Caching so với hoạt động truy vấn DNS thông thường dựa vào các tiếu chí và thông số đo kiểm.

Hình thức thực hiện: Thực hiện đo kiểm tổng hợp các thông số theo 02 kịch bản với: hoạt động truy vấn trên máy chủ DNS Caching khi chưa bật xác thực DNSSEC và hoạt động truy vấn trên máy chủ DNS Caching khi đã bật xác thực DNSSEC.

3.1. Kịch bản 1: Khi chưa bật xác thực DNSSEC

Mô tả:

Thiết lập cấu hình hoạt động truy vấn và phản hồi truy vấn DNS thông thường cho máy chủ DNS Caching (chưa cấu hình triển khai bật xác thực DNSSEC).

- Sử dụng công cụ **dnsperf** để tạo các và gửi hàng loạt truy vấn lên máy chủ DNS Caching nhằm đo kiểm năng lực đáp ứng truy vấn của hệ thống và kích thước gói tin, thời gian phản hồi truy vấn trung bình của các truy vấn DNS thông thường. Với lần lượt các mức số lượng truy vấn tối đa trên mỗi giây như sau: 10.000 QPS, 20.000 QPS, 50.000 QPS, 70.000 QPS.

- Đo kiểm năng lực đáp ứng của các thông số tài nguyên phần cứng của máy chủ DNS Caching bằng cách sử dụng các công cụ như Cacti, Solarwinds.

- Đo kiểm băng thông đáp ứng truy vấn và phản hồi truy vấn DNS thông thường bằng các sử dụng công cụ Speedometer (Hướng dẫn cài đặt và sử dụng công cụ Speedometer tại Phụ lục 02).

- Các thông số đo kiểm được ghi lại vào Bảng 02 bên dưới để tổng hợp và phân tích.

- Ví dụ: Thực hiện tạo 10.000 truy vấn mỗi giây (10.000 QPS) truy vấn DNS thông thường và gửi đến máy chủ DNS Caching có địa chỉ IP là *server_ip_address* trong vòng 10 phút (600 giây) và có file câu hỏi truy vấn mẫu là *queryfile-test-dnssec.txt*.

#dnsperf -s server_ip_address -d queryfile-test-dnssec.txt -Q 10000 -l 600

- Trong đó:

-s: địa chi IP của máy chủ DNS Caching đang kiểm thử.

-d: đường dẫn đến file chứa dữ liệu bản ghi tên miền thực hiện truy vấn.

-l: thời gian thực hiện kiểm tra.

-Q: max_qps (số lượng truy vấn DNS mỗi giây).

3.2. Kịch bản 2: Khi đã bật xác thực DNSSEC

Mô tả:

Thiết lập lại cấu hình bật xác thực DNSSEC cho máy chủ DNS Caching (hướng dẫn chi tiết tại website của VNNIC theo đường dẫn: https://vnnic.vn/dns/thong-tin-va-tai-lieu-tham-khao đối với phần mềm BIND9).

Kiểm tra xác thực DNSSEC bằng lệnh cơ bản: Sau khi bật xác thực DNSSEC trên máy chủ DNS Caching, thực hiện truy vấn DNSSEC bằng công cụ dig để kiểm tra xác thực DNSSEC thành công hay thất bại với một số tên miền đã được triển khai ký DNSSEC, sau đây là ví dụ và các trường hợp có thể xảy ra (Bảng 1):

- Ví dụ:
  - #dig @*server_ip_address* dnssec.vn A +dnssec
  - #dig @*server_ip_address* dnssec.vn A +dnssec +cd

Bảng 1: Kết quả đối chiếu xác thực DNSSEC

Case test	+dnssec	+dnssec +cd	Note
Validation OK	NOERROR qr rd ra **ad**	NOERROR qr rd ra cd **ad**	Xác thực thành công
Validation Failed	SERVFAIL qr rd ra	NOERROR qr rd ra cd	Kiểm tra thông tin cấu hình trust anchor

Tương tự như với kịch bản khi chưa bật xác thực DNSSEC:

- Sử dụng công cụ **dnsperf** để tạo và gửi hàng loạt truy vấn DNSSEC lên máy chủ DNS Caching nhằm đo kiểm năng lực đáp ứng truy vấn của hệ thống và kích thước gói tin, thời gian phản hồi truy vấn trung bình của các truy vấn DNSSEC. Với lần lượt các mức số lượng truy vấn tối đa trên mỗi giây như sau: 10.000 QPS, 20.000 QPS, 50.000 QPS, 70.000 QPS.

- Đo kiểm năng lực đáp ứng của các thông số tài nguyên phần cứng của máy chủ DNS Caching bằng các sử dụng các công cụ đo kiểm năng lực của phần cứng như Cacti, Solarwinds.

- Đo kiểm băng thông đáp ứng truy vấn và phản hồi truy vấn DNSSEC: bằng một số công cụ như Speedometer (hướng dẫn cài đặt Speedometer trong phụ lục 02) hoặc một số công cụ, phần mềm đo kiểm băng thông như Cacti, Solarwinds.

- Các thông số đo kiểm được ghi lại vào Bảng 02 bên dưới để tổng hợp và phân tích.

- Ví dụ: Thực hiện tạo 10.000 truy vấn mỗi giây (10.000 QPS) truy vấn DNSSEC và gửi đến máy chủ DNS Caching có địa chỉ IP là *server_ip_address* trong vòng 10 phút (600 giây) và có file câu hỏi truy vấn mẫu là queryfile-test-dnssec.txt.

#dnsperf -s server_ip_address -d queryfile-test-dnssec.txt -Q 10000 -l 600 -D

Trong đó:

-s: địa chi IP của máy chủ DNS Caching đang kiểm thử.

-d: đường dẫn đến file chứa dữ liệu bản ghi tên miền thực hiện truy vấn.

-l: thời gian thực hiện kiểm tra.

-D: DNSSEC OK (truy vấn có DNSSEC)

-Q: max_qps (số lượng truy vấn DNS mỗi giây).

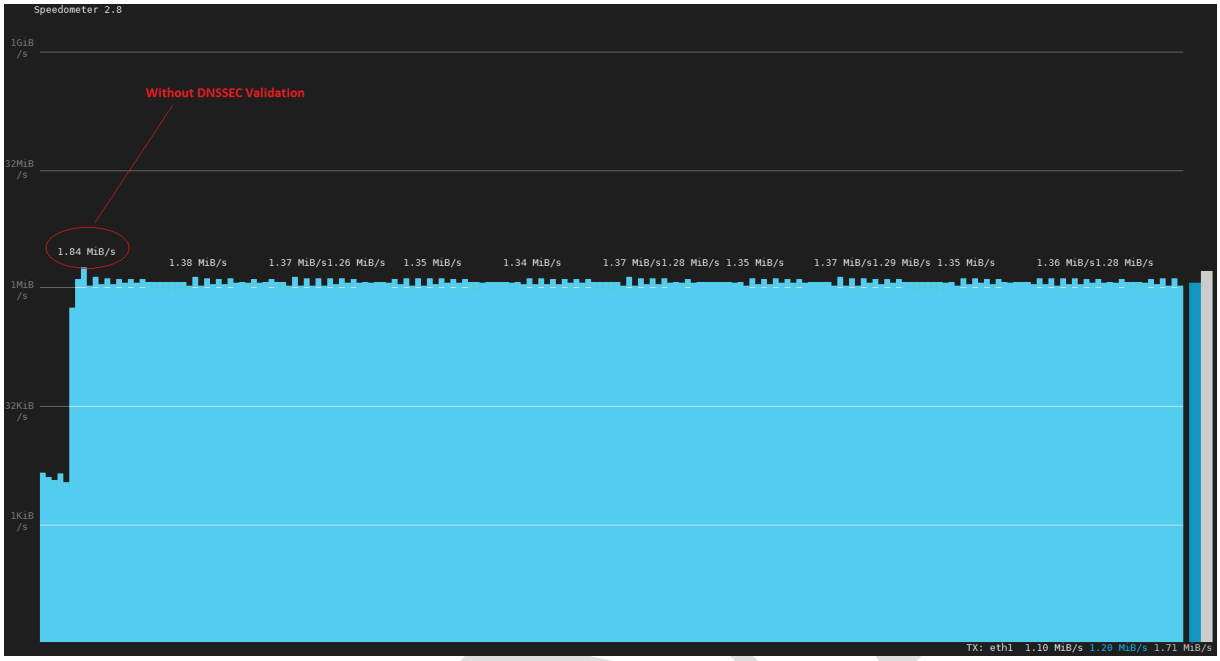
Bảng 02: Kết quả kiểm tra chất lượng truy vấn DNS/DNSSEC

QPS	Without DNSSEC validation				With DNSSEC validation			
	Packet Loss	**Response Packet size (bytes)**	**Avg Response time (ms)**	**Max Bandwidth (Mbps)**	**Packet Loss**	**Response Packet size (bytes)**	**Avg Response time (ms)**	**Max Bandwidth (Mbps)**
10.000	*0%*	*86*	*4.9*	*15.44*	*0%*	*713*	*4.9*	*73.32*
20.000								
50.000								
70.000								

- 1 MiB/s = ~8.39 Mbps

Ví dụ:

- Kết quả khi thực hiện truy vấn DNS khi không có xác thực DNSSEC và có xác thực DNSSEC với 10.000 QPS:
    - KHÔNG có xác thực DNSSEC

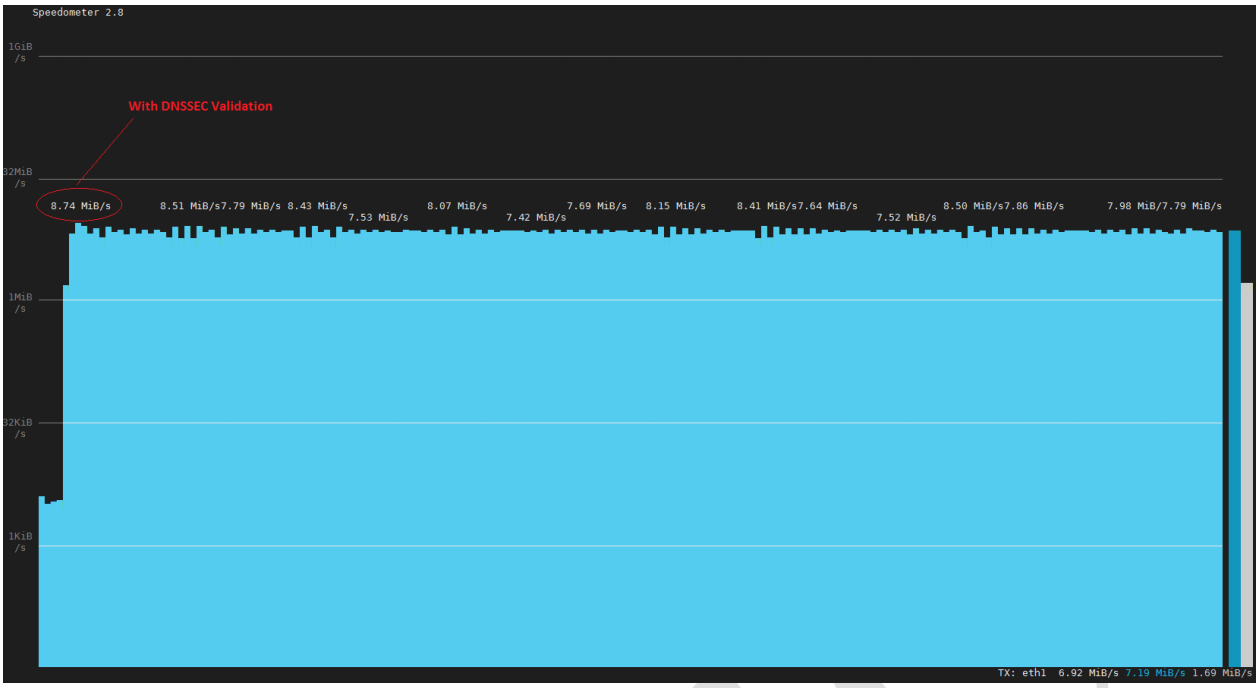


Hình 2: Băng thông đáp ứng tối đa với truy vấn DNS thông thường

```
Statistics:

  Queries sent:         3600000
  Queries completed:    3600000 (100.00%)
  Queries lost:         0 (0.00%)

  Response codes:       NOERROR 3150166 (87.50%), NXDOMAIN 449834 (12.50%)
  Average packet size:  request 36, response 86
  Run time (s):         360.009861
  Queries per second:   9999.726091

  Average Latency (s):  0.004944 (min 0.000087, max 0.095804)
  Latency StdDev (s):   0.007254
```

Hình 3: Kết quả kiểm tra năng lực đáp ứng phản hồi truy vấn DNS thông thường

- CÓ xác thực DNSSEC



Hình 4: Băng thông đáp ứng tối đa với truy vấn DNSSEC

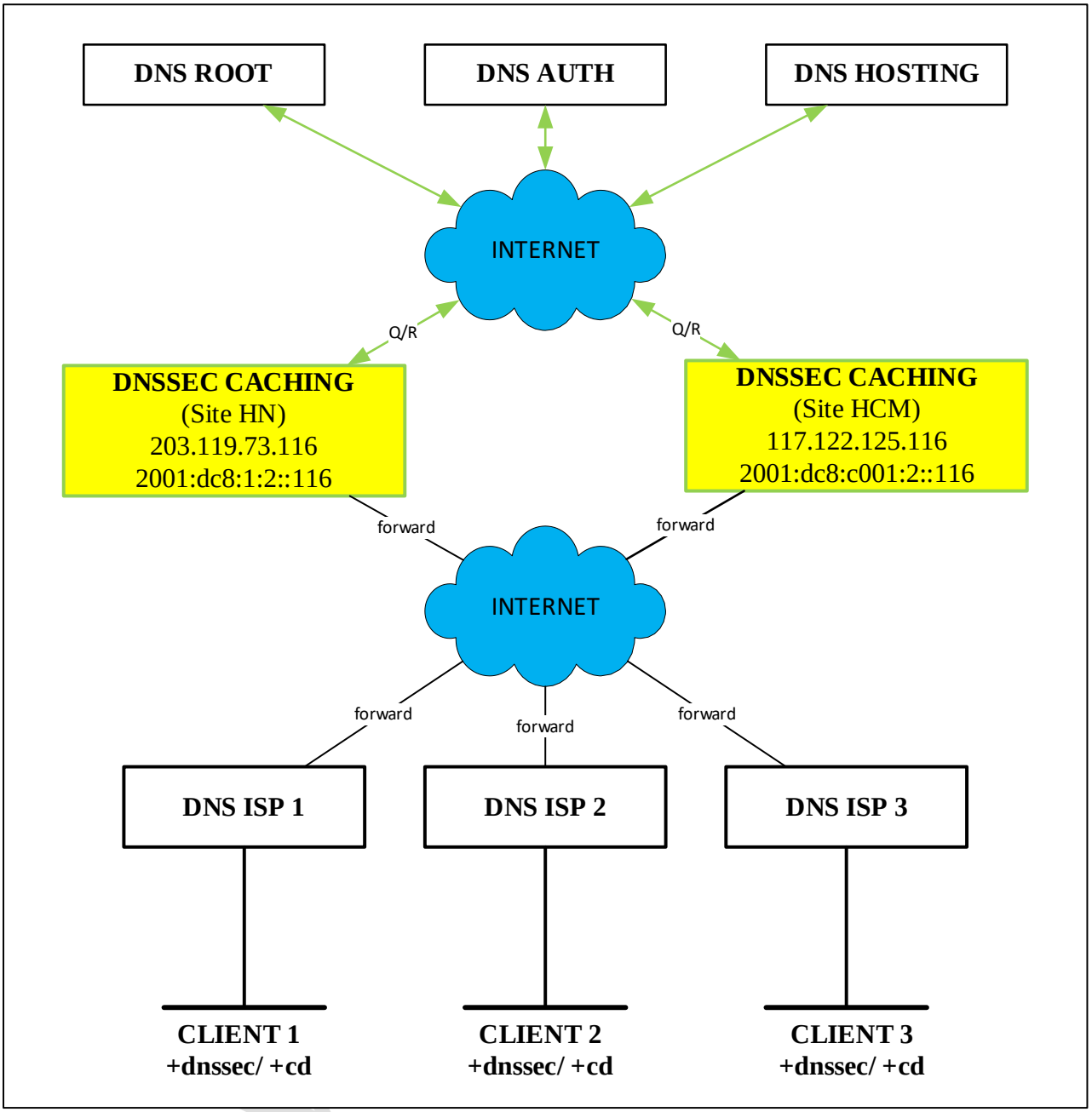
```
Statistics:

  Queries sent:         3600000
  Queries completed:    3599956 (100.00%)
  Queries lost:         44 (0.00%)

  Response codes:       NOERROR 3150135 (87.50%), NXDOMAIN 449821 (12.50%)
  Average packet size:  request 47, response 713
  Run time (s):         360.002517
  Queries per second:   9999.807862

  Average Latency (s):  0.004893 (min 0.000097, max 0.090113)
  Latency StdDev (s):   0.006869
```

Hình 5: Kết quả kiểm tra năng lực đáp ứng phản hồi truy vấn DNSSEC

4. Hướng dẫn kết nối và thử nghiệm DNSSEC trên hệ thống của VNNIC.

Mục tiêu: Thử nghiệm kiểm chứng chức năng, tính năng xác thực và nguyên lý hoạt động của DNSSEC và đánh giá hiệu năng khi có hoạt động truy vấn xác thực DNSSEC.

4.1. Mô hình kết nối thử nghiệm



Hình 6: Mô hình kết nối triển khai kiểm thử DNSSEC

Mô tả:

VNNIC triển khai hệ thống máy chủ DNS Caching, đã bật tính năng DNSSEC Validation, bao gồm 02 node máy chủ hoạt động với chức năng tương tự nhau. Hệ thống DNS Caching này tiếp nhận và phản hồi truy vấn DNSSEC từ các Resolver; kết nối liên thông DNSSEC với các hệ thống DNS khác, gồm DNS Root, các DNS Authoritative và các DNS Hosting trên Internet. Hệ thống này sử dụng để thử nghiệm, có thể tiếp nhận và phản hồi các truy vấn DNS/DNSSEC từ các ISP đăng ký kết nối thử nghiệm.

4.2. Thông số hệ thống

Hiện tại hệ thống DNSSEC Caching thử nghiệm của VNNIC đang được triển khai với các thông số như sau:

STT	Hostname/ Địa chỉ IP	Hệ điều hành	Phần mềm DNS	Năng lực đáp ứng	Xác thực DNSSEC	Ghi chú
1	DNSSEC Caching HN IPv4: 203.119.73.116 IPv6: 2001:dc8:1:2::116	REHL7.5	Unbound 1.9.4	120.000 QPS	Đã bật mặc định	
2	DNSSEC Caching HCM: IPv4: 117.122.125.116 IPv6: 2001:dc8:c001:2::116	REHL7.5	Unbound 1.9.4	120.000 QPS	Đã bật mặc định	

Hệ thống được giám sát trạng thái hoạt động và băng thông đáp ứng trên các hệ thống giám sát của VNNIC nhằm đánh giá năng lực và chất lượng hoạt động của hệ thống.

4.3. Hướng dẫn kết nối thử nghiệm

Để triển khai thử nghiệm, trước tiên các ISP cần thực hiện đăng ký kết nối thử nghiệm trên hệ thống của VNNIC theo Biểu mẫu đăng ký trực tuyến tại đường dẫn: https://vnnic.vn/dns/dang-ky-ket-noi-thu-nghiem-dnssec-tren-he-thong-dnssec-caching-vnnic.

Sau khi đăng ký kết nối thành công, các cán bộ quản trị hệ thống DNS của các ISP phối hợp với đầu mối của VNNIC để tiến hành thử nghiệm. Việc kết nối thử nghiệm sẽ thực hiện lần lượt từng ISP và thời gian thử nghiệm sẽ kéo dài trong vòng 03 ngày (72 tiếng), nhằm đảm bảo độ chính xác, năng lực đáp ứng của hệ thống và các ISP có thể thực hiện kết nối thử nghiệm.

Thực hiện thiết lập cấu hình chuyển tiếp (forward) truy vấn DNS/DNSSEC từ hệ thống DNS của các ISP đến 02 máy chủ DNSSEC Caching của VNNIC với các mức số lượng truy vấn tối đa trong một giây (QPS) được quy định tại trong Biểu mẫu đăng ký trực tuyến trên.

Hệ thống máy chủ DNSSEC Caching của VNNIC hiện đang được giám sát trên các hệ thống giá sát của VNNIC, do đó các thông tin về tài nguyên phần cứng của máy chủ

DNSSEC Caching sử dụng, băng thông tối đa sẽ được VNNIC thực hiện đo kiểm và tổng hợp, chia sẻ số liệu với các ISP để đánh giá kết quả thử nghiệm. Chi tiết các thông số sẽ được VNNIC tổng hợp và ghi vào các bảng sau cho từng ISP (Bảng 03).

Bảng 03: ISP 01

QPS	Without DNSSEC validation				With DNSSEC validation			
	Packet Loss	**Response Packet size (bytes)**	**Avg Response time (ms)**	**Max Bandwidth (Mbps)**	**Packet Loss**	**Response Packet size (bytes)**	**Avg Response time (ms)**	**Max Bandwidth (Mbps)**
10.000	*0%*	*86*	*4.9*	*15.44*	*0%*	*713*	*4.9*	*73.32*
20.000								
50.000								
70.000								

PHỤ LỤC 01: HƯỚNG DẪN CÀI ĐẶT CÔNG CỤ ĐO KIỂM CHẤT LƯỢNG TRUY VẤN DNS (DNSPERF)

1. Tải và cài đặt phần mềm

Thực hiện tải phần mềm dnsperf theo đường dẫn: https://www.dns-oarc.net/tools/dnsperf

Giải nén và cài đặt công cụ theo các bước:

```
#tar -xvf dnsperf-src-2.1.0.0-1.tar.gz
#cd dnsperf-src-2.1.0.0-1
#./configure
#make
#make install
```

2. Tạo file dữ liệu truy vấn bản ghi tên miền

Soạn thảo nội dung 1 file dữ liệu các bản ghi tên miền để truy vấn có nội dung như sau:

```
ipv6event2015.vn.   A
ipv6event2015.vn.   AAAA
vnnic.vn.           CNAME
isc.org.            TXT
<FQDN>              <RRs>
```

3. Hướng dẫn truyền các tham số và chạy công cụ kiểm tra

Một số tham số cần lưu ý:

```
DNS Performance Testing Tool
Nominum Version 2.1.0.0

Usage: dnsperf [-f family] [-s server_addr] [-p port] [-a local_addr]
               [-x  local_port]  [-d  datafile]  [-c  clients]  [-T
threads]
               [-n  maxruns]  [-l  timelimit]  [-b  buffer_size]  [-t
timeout]
               [-e] [-D] [-y [alg:]name:secret] [-q num_queries]
               [-Q max_qps] [-S stats_interval] [-u] [-v] [-h]
  -f address family of DNS transport, inet or inet6 (default: any)
  -s the server to query (default: 127.0.0.1)
  -p the port on which to query the server (default: 53)
  -a the local address from which to send queries
  -x the local port from which to send queries (default: 0)
  -d the input data file (default: stdin)
```

```
  -c the number of clients to act as
  -T the number of threads to run
  -n run through input at most N times
  -l run for at most this many seconds
  -b socket send/receive buffer size in kilobytes
  -t the timeout for query completion in seconds (default: 5)
  -e enable EDNS 0
  -D set the DNSSEC OK bit (implies EDNS)
  -y the TSIG algorithm, name and secret
  -q the maximum number of queries outstanding (default: 100)
  -Q limit the number of queries per second
  -S print qps statistics every N seconds
  -u send dynamic updates instead of queries
  -v verbose: report each query to stdout
  -h print this help
```

Ví dụ:

Thực hiện truy vấn đến máy chủ có địa chỉ 192.168.100.100 trong thời gian 60 giây với tốc độ truy vấn là 10 qps.

#dnsperf -s 192.168.100.100 -d queryfile-example-current -l 60 -c 1 -Q 10

Kết quả như sau:

```
Statistics:

  Queries sent:         18393
  Queries completed:    18157 (98.72%)
  Queries lost:         236 (1.28%)

  Response codes:       NOERROR 16904 (93.10%), NXDOMAIN 1253 (6.90%)
  Average packet size:  request 38, response 107
  Run time (s):         32.915659
  Queries per second:   551.621950

  Average Latency (s):  0.104805 (min 0.001224, max 2.991246)
  Latency StdDev (s):   0.202635
```

PHỤ LỤC 02: HƯỚNG DẪN CÀI ĐẶT CÔNG CỤ ĐO KIỂM BĂNG THÔNG SPEEDOMETER

1. Tải và cài đặt phần mềm

Tải về các gói yêu cầu cài đặt URWID trước khi cài đặt công cụ Speedometer theo đường dẫn: http://urwid.org/

Tải công cụ Speedometer theo đường dẫn sau: https://github.com/wardi/speedometer/releases

Giải nén và cài đặt trên máy chủ cần giám sát, theo dõi theo các bước:

```
#tar -xvf urwid-2.1.1.tar.gz
#cd urwid-2.1.1
#python setup.py build
#python setup.py install
```

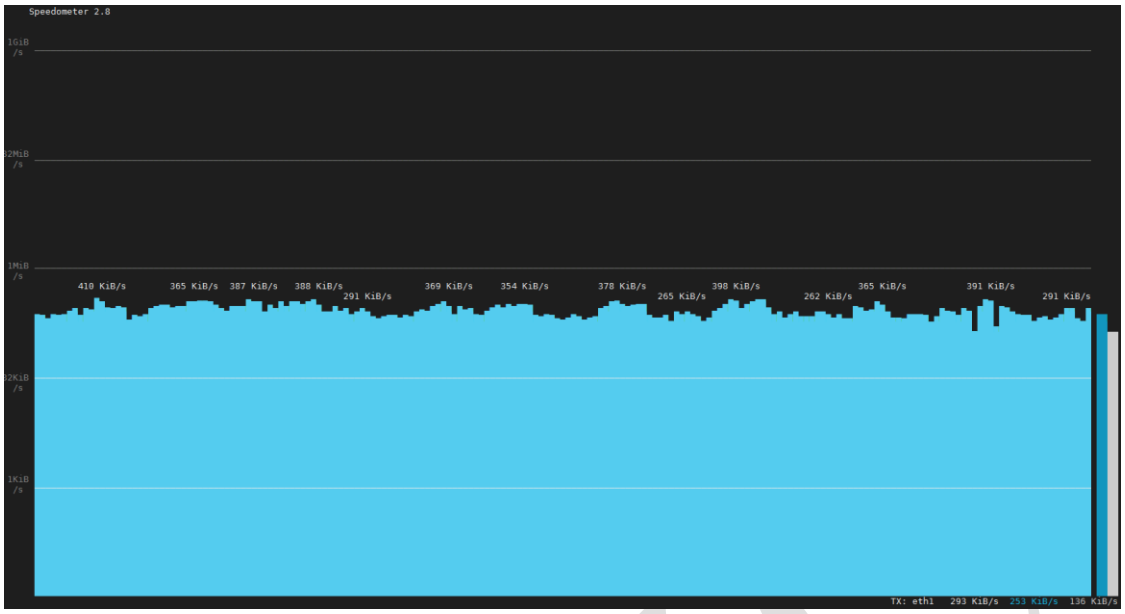
```
#tar -xvf speedometer-release-2.8.tar.gz
#cd speedometer-release-2.8
#install -m 755 speedometer.py /usr/local/bin
#python setup.py install
```

2. Hướng dẫn sử dụng Speedometer

Để đo kiểm băng thông tại các cổng mạng của máy chủ với các thông số gói tin nhận được và gói tin phản hồi theo thời gian thực thì thực hiện các lệnh tương ứng sau:

```
#speedometer -rx eth1
#speedometer -tx eth1
```

Biểu đồ thể hiện băng thông sử dụng:



Hình 7: Biểu đồ băng thông sử dụng (Speedometer)

Chỉ đạo biên soạn:

Ông Nguyễn Trường Thành – Trưởng phòng Kỹ thuật

Nhóm biên soạn:

Ông Nguyễn Văn Trí – Chuyên viên phòng Kỹ thuật

Bà Vũ Thị Hoàn – Chuyên viên Đài DNS-VNIX

Ông Lê Khắc Chính – Chuyên viên Đài DNS-VNIX