

# Thiết kế & triển khai mạng IP

Bài thực hành số 4: Các dịch vụ Internet (Internet Services)

## Bài 1: Vai trò của cổng TCP & UDP trong dịch vụ Client/Server

Bài này sử dụng công cụ *iperf* để thử nghiệm **quá trình vận hành một cặp ứng dụng** trên mạng TCP/IP theo mô hình client/server. *Wireshark* được sử dụng để theo dõi các gói tin truyền giữa client và server, qua đó đối chiếu với sơ đồ chuyển trạng thái TCP. Các bước thực hiện như sau:

- Bước 1: Cài đặt ứng dụng *iperf3* trên máy client và server
- Bước 2: Chạy ứng dụng *iperf3* trên server và client
- Bước 3: Quan sát quá trình vận hành liên kết TCP với *Wireshark*.

### Bước 1: Cài đặt ứng dụng *iperf3* trên máy client và server

Công cụ *iperf*<sup>1</sup> và *ipref3* (phiên bản 3) cho phép gửi các gói tin TCP, UDP theo các địa chỉ unicast, broadcast hay multicast. Nó còn cho phép đo đặc bằng thông giữa trạm truyền. Để cài đặt *iperf*, cần kiểm tra Extra Packages for Enterprise Linux (epel)<sup>2</sup> đã được đăng ký trong repository của *yum* chưa, nếu chưa thì đăng ký thêm. Sau đó dùng *yum* để cài đặt *iperf* hoặc *iperf3*:

```
[root@localhost ~]# yum repolist
repo id      repo name      status
base/7/x86_64  CentOS-7 - Base  9,007
extras/7/x86_64  CentOS-7 - Extras  356
updates/7/x86_64  CentOS-7 - Updates  2,005
repolist: 11,368

[root@localhost ~]# yum search epel
===== N/S matched: epel =====
epel-release.noarch : Extra Packages for Enterprise Linux repository      : configuration

Name and summary matches only, use "search all" for everything.
[root@localhost ~]# yum install epel-release.noarch
...
Complete!

[root@localhost ~]# yum repolist
repo id      repo name      status
base/7/x86_64  CentOS-7 - Base  9,007
epel/x86_64    Extra Packages for Enterprise Linux 7 - x86_64  10,350
extras/7/x86_64  CentOS-7 - Extras  356
updates/7/x86_64  CentOS-7 - Updates  2,005
repolist: 21,718
[root@localhost ~]# yum install iperf iperf3
...
```

### Bước 2: Chạy ứng dụng *iperf3* trên server và client

Trên máy server, giả sử có địa chỉ 192.168.2.1, chạy *iperf3* chế độ server và đăng ký cổng 5001 để chờ kết nối từ client.

```
[root@R1 ~]# iperf3 -s -p 5001
.....
Server listening on 5001
.....
```

<sup>1</sup> <https://iperf.fr/>

<sup>2</sup> <https://fedoraproject.org/wiki/EPEL>

Trên client, chạy *iperf3* chế độ client và kết nối đến server theo địa chỉ IP và cổng tương ứng. Mặc định, client sẽ kết nối đến server bằng giao thức TCP. Nếu client và server kết nối được với nhau, các thông tin được hiển thị phía client như sau:

```
[root@C2 ~]# iperf3 -c 192.168.2.1 -p 5001
Connecting to host 192.168.2.1, port 5001
[ 4] local 192.168.2.15 port 44692 connected to 192.168.2.1 port 5001
[ ID] Interval      Transfer    Bandwidth   Retr  Cwnd
[ 4] 0.00-1.00 sec  2.54 MBytes 21.3 Mbits/sec  4  41.0 KBytes
[ 4] 1.00-2.00 sec 13.3 MBytes 112 Mbits/sec  3  218 KBytes
[ 4] 2.00-3.00 sec  7.15 MBytes 60.0 Mbits/sec  3  69.3 KBytes
[ 4] 3.00-4.00 sec  1.20 MBytes 10.1 Mbits/sec  2  91.9 KBytes
[ 4] 4.00-5.00 sec   267 KBytes 2.19 Mbits/sec  2  53.7 KBytes
[ 4] 5.00-6.00 sec  1.42 MBytes 11.9 Mbits/sec  0  69.3 KBytes
[ 4] 6.00-7.00 sec  1.49 MBytes 12.5 Mbits/sec  2  97.6 KBytes
[ 4] 7.00-8.00 sec 23.7 MBytes 200 Mbits/sec 48 252 KBytes
[ 4] 8.00-9.00 sec 63.8 MBytes 535 Mbits/sec 91 188 KBytes
[ 4] 9.00-10.00 sec 84.6 MBytes 709 Mbits/sec  0 202 KBytes
-----
[ ID] Interval      Transfer    Bandwidth   Retr
[ 4] 0.00-10.00 sec 199 MBytes 167 Mbits/sec 155      sender
[ 4] 0.00-10.00 sec 199 MBytes 167 Mbits/sec      receiver

iperf Done.
```

Trên server, thông tin cũng được hiển thị tương ứng:

```
[root@R1 ~]# iperf3 -s -p 5001
-----
Server listening on 5001
-----
Accepted connection from 192.168.2.15, port 44690
[ 5] local 192.168.2.1 port 5001 connected to 192.168.2.15 port 44692
[ ID] Interval      Transfer    Bandwidth
[ 5] 0.00-1.00 sec  2.21 MBytes 18.6 Mbits/sec
[ 5] 1.00-2.00 sec  9.40 MBytes 78.7 Mbits/sec
[ 5] 2.00-3.00 sec 10.7 MBytes 89.8 Mbits/sec
[ 5] 3.00-4.00 sec  759 KBytes 6.21 Mbits/sec
[ 5] 4.00-5.00 sec  631 KBytes 5.17 Mbits/sec
[ 5] 5.00-6.00 sec  1.40 MBytes 11.7 Mbits/sec
[ 5] 6.00-7.00 sec  781 KBytes 6.39 Mbits/sec
[ 5] 7.00-8.00 sec 21.6 MBytes 181 Mbits/sec
[ 5] 8.00-9.00 sec 64.7 MBytes 542 Mbits/sec
[ 5] 9.00-10.00 sec 84.2 MBytes 706 Mbits/sec
[ 5] 10.00-10.03 sec 2.49 MBytes 739 Mbits/sec
-----
[ ID] Interval      Transfer    Bandwidth
[ 5] 0.00-10.03 sec 0.00 Bytes 0.00 bits/sec      sender
[ 5] 0.00-10.03 sec 199 MBytes 166 Mbits/sec      receiver
-----
Server listening on 5001
-----
```

Có thể sử dụng tham số *-u* để yêu cầu client kết nối đến server bằng giao thức UDP:

```
[root@C2 ~]# iperf3 -u -c 192.168.2.1 -p 5001
Connecting to host 192.168.2.1, port 5001
[ 4] local 192.168.2.15 port 35392 connected to 192.168.2.1 port 5001
[ ID] Interval      Transfer    Bandwidth   Total Datagrams
[ 4] 0.00-1.00 sec 120 KBytes 982 Kbits/sec 15
[ 4] 1.00-2.00 sec 128 KBytes 1.05 Mbits/sec 16
[ 4] 2.00-3.00 sec 128 KBytes 1.05 Mbits/sec 16
[ 4] 3.00-4.00 sec 128 KBytes 1.05 Mbits/sec 16
[ 4] 4.00-5.00 sec 128 KBytes 1.05 Mbits/sec 16
[ 4] 5.00-6.00 sec 128 KBytes 1.05 Mbits/sec 16
[ 4] 6.00-7.00 sec 128 KBytes 1.05 Mbits/sec 16
[ 4] 7.00-8.00 sec 128 KBytes 1.05 Mbits/sec 16
[ 4] 8.00-9.00 sec 128 KBytes 1.05 Mbits/sec 16
```

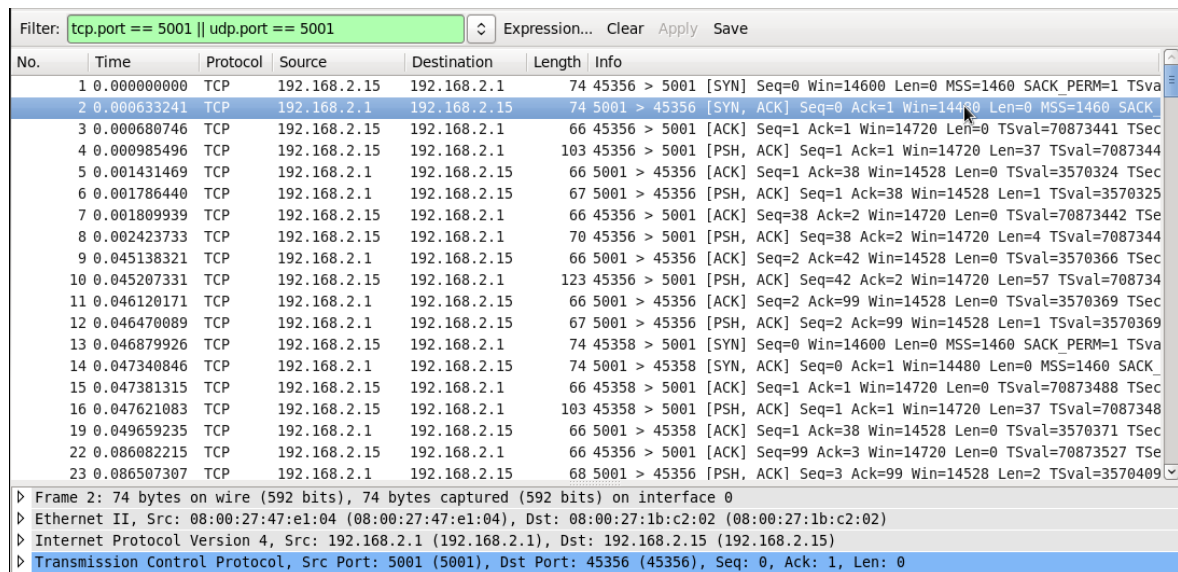
[ 4] 9.00-10.00 sec 128 KBytes 1.05 Mbits/sec 16

[ ID] Interval Transfer Bandwidth Jitter Lost/Total Datagrams  
[ 4] 0.00-10.00 sec 1.24 MBytes 1.04 Mbits/sec 0.468 ms 0/159 (0%)  
[ 4] Sent 159 datagrams

iperf Done.

### Bước 3: Quan sát quá trình vận hành liên kết TCP với Wireshark

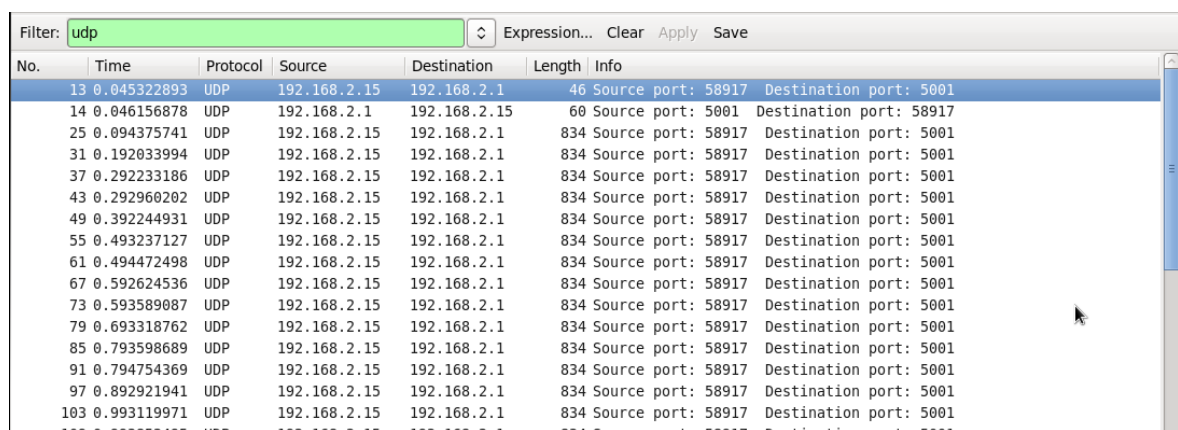
Trong khi vận hành *iperf3* để kết nối client-server, sử dụng Wireshark bắt các gói tin truyền giữa 2 trạm. Có thể lọc hiển thị các gói tin TCP hoặc UDP có cổng đích là 5001. Kết quả như sau:



No.	Time	Protocol	Source	Destination	Length	Info
1	0.000000000	TCP	192.168.2.15	192.168.2.1	74	45356 > 5001 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSva
2	0.000633241	TCP	192.168.2.1	192.168.2.15	74	5001 > 45356 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK
3	0.000680746	TCP	192.168.2.15	192.168.2.1	66	45356 > 5001 [ACK] Seq=1 Ack=1 Win=14720 Len=0 TSval=70873441 TSec
4	0.000985496	TCP	192.168.2.15	192.168.2.1	103	45356 > 5001 [PSH, ACK] Seq=1 Ack=1 Win=14720 Len=37 TSval=7087344
5	0.001431469	TCP	192.168.2.1	192.168.2.15	66	5001 > 45356 [ACK] Seq=1 Ack=38 Win=14528 Len=0 TSval=3570324 TSec
6	0.001786440	TCP	192.168.2.1	192.168.2.15	67	5001 > 45356 [PSH, ACK] Seq=1 Ack=38 Win=14528 Len=1 TSval=3570325
7	0.001809939	TCP	192.168.2.15	192.168.2.1	66	45356 > 5001 [ACK] Seq=38 Ack=2 Win=14720 Len=0 TSval=70873442 TSe
8	0.002423733	TCP	192.168.2.15	192.168.2.1	70	45356 > 5001 [PSH, ACK] Seq=38 Ack=2 Win=14720 Len=4 TSval=7087344
9	0.045138321	TCP	192.168.2.1	192.168.2.15	66	5001 > 45356 [ACK] Seq=2 Ack=42 Win=14528 Len=0 TSval=3570366 TSec
10	0.045207331	TCP	192.168.2.15	192.168.2.1	123	45356 > 5001 [PSH, ACK] Seq=42 Ack=2 Win=14720 Len=57 TSval=708734
11	0.046120171	TCP	192.168.2.1	192.168.2.15	66	5001 > 45356 [ACK] Seq=2 Ack=99 Win=14528 Len=0 TSval=3570369 TSec
12	0.046470089	TCP	192.168.2.1	192.168.2.15	67	5001 > 45356 [PSH, ACK] Seq=2 Ack=99 Win=14528 Len=1 TSval=3570369
13	0.046879926	TCP	192.168.2.15	192.168.2.1	74	45358 > 5001 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSva
14	0.047340846	TCP	192.168.2.1	192.168.2.15	74	5001 > 45358 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK
15	0.047381315	TCP	192.168.2.15	192.168.2.1	66	45358 > 5001 [ACK] Seq=1 Ack=1 Win=14720 Len=0 TSval=70873488 TSec
16	0.047621083	TCP	192.168.2.15	192.168.2.1	103	45358 > 5001 [PSH, ACK] Seq=1 Ack=1 Win=14720 Len=37 TSval=7087348
19	0.049659235	TCP	192.168.2.1	192.168.2.15	66	5001 > 45358 [ACK] Seq=1 Ack=38 Win=14528 Len=0 TSval=3570371 TSec
22	0.086082215	TCP	192.168.2.15	192.168.2.1	66	45356 > 5001 [ACK] Seq=99 Ack=3 Win=14720 Len=0 TSval=70873527 TSe
23	0.086507307	TCP	192.168.2.1	192.168.2.15	68	5001 > 45356 [PSH, ACK] Seq=3 Ack=99 Win=14528 Len=2 TSval=3570409

Frame 2: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0  
Ethernet II, Src: 08:00:27:47:e1:04 (08:00:27:47:e1:04), Dst: 08:00:27:1b:c2:02 (08:00:27:1b:c2:02)  
Internet Protocol Version 4, Src: 192.168.2.1 (192.168.2.1), Dst: 192.168.2.15 (192.168.2.15)  
Transmission Control Protocol, Src Port: 5001 (5001), Dst Port: 45356 (45356), Seq: 0, Ack: 1, Len: 0

Có thể nhìn thấy 3 gói tin TCP đầu tiên được trao đổi giữa client và server là SYN, SYN ACK và ACK. Đây chính là quá trình bắt tay 3 bước để thiết lập kết nối TCP. Tiếp theo là các gói dữ liệu truyền giữa client và server cùng với trường *Seq* và *Ack* để xác nhận các gói tin đã được nhận tốt ở mỗi phía. Tiếp tục sử dụng Wireshark và bắt các gói tin khi *iperf3* kết nối với UDP. Kết quả như sau:



No.	Time	Protocol	Source	Destination	Length	Info
13	0.045322893	UDP	192.168.2.15	192.168.2.1	46	Source port: 58917 Destination port: 5001
14	0.046156878	UDP	192.168.2.1	192.168.2.15	60	Source port: 5001 Destination port: 58917
25	0.094375741	UDP	192.168.2.15	192.168.2.1	834	Source port: 58917 Destination port: 5001
31	0.192033994	UDP	192.168.2.15	192.168.2.1	834	Source port: 58917 Destination port: 5001
37	0.292233186	UDP	192.168.2.15	192.168.2.1	834	Source port: 58917 Destination port: 5001
43	0.292960202	UDP	192.168.2.15	192.168.2.1	834	Source port: 58917 Destination port: 5001
49	0.392244931	UDP	192.168.2.15	192.168.2.1	834	Source port: 58917 Destination port: 5001
55	0.493237127	UDP	192.168.2.15	192.168.2.1	834	Source port: 58917 Destination port: 5001
61	0.494472498	UDP	192.168.2.15	192.168.2.1	834	Source port: 58917 Destination port: 5001
67	0.592624536	UDP	192.168.2.15	192.168.2.1	834	Source port: 58917 Destination port: 5001
73	0.593589087	UDP	192.168.2.15	192.168.2.1	834	Source port: 58917 Destination port: 5001
79	0.693318762	UDP	192.168.2.15	192.168.2.1	834	Source port: 58917 Destination port: 5001
85	0.793598689	UDP	192.168.2.15	192.168.2.1	834	Source port: 58917 Destination port: 5001
91	0.794754369	UDP	192.168.2.15	192.168.2.1	834	Source port: 58917 Destination port: 5001
97	0.892921941	UDP	192.168.2.15	192.168.2.1	834	Source port: 58917 Destination port: 5001
103	0.993119971	UDP	192.168.2.15	192.168.2.1	834	Source port: 58917 Destination port: 5001

Có thể thấy với phương pháp truyền dữ liệu bằng UDP, không có quá trình bắt tay giữa client và server để thiết lập liên kết. Gói tin đầu tiên client gửi đến server cũng là gói dữ liệu được gửi thẳng đến cổng 5001 và không có cơ chế xác nhận từ server về client khi hoàn thành nhận các gói dữ liệu này.

Quay trở lại với trường hợp truyền dữ liệu *iperf3* sử dụng TCP, theo dõi các gói tin cuối cùng của phiên truyền thông, có thể thấy máy client gửi đi thông điệp FIN, ACK và máy server trả lời bằng một thông điệp ACK. Đây là các bước kết thúc kênh truyền TCP và hủy kết nối.

Filter: tcp.dstport == 5001		Expression... Clear Apply Save				
No.	Time	Protocol	Source	Destination	Length	Info
13004	10.088213003	TCP	192.168.2.15	192.168.2.1	13098	45676 > 5001 [ACK] Seq=462301190 Ack=1 Win=14720 Len=13032 TSval=7
13005	10.088250487	TCP	192.168.2.15	192.168.2.1	13098	45678 > 5001 [ACK] Seq=462314222 Ack=1 Win=14720 Len=13032 TSval=7
13006	10.088285037	TCP	192.168.2.15	192.168.2.1	13098	45678 > 5001 [ACK] Seq=462327254 Ack=1 Win=14720 Len=13032 TSval=7
13007	10.088436668	TCP	192.168.2.15	192.168.2.1	67	45676 > 5001 [PSH, ACK] Seq=99 Ack=5 Win=14720 Len=1 TSval=7150182
13010	10.091459373	TCP	192.168.2.15	192.168.2.1	66	45676 > 5001 [ACK] Seq=100 Ack=6 Win=14720 Len=0 TSval=71501831 TS
13011	10.091783270	TCP	192.168.2.15	192.168.2.1	70	45676 > 5001 [PSH, ACK] Seq=100 Ack=6 Win=14720 Len=4 TSval=715018
13015	10.132799500	TCP	192.168.2.15	192.168.2.1	263	45676 > 5001 [PSH, ACK] Seq=104 Ack=6 Win=14720 Len=197 TSval=7150
13018	10.175321412	TCP	192.168.2.15	192.168.2.1	66	45676 > 5001 [ACK] Seq=301 Ack=10 Win=14720 Len=0 TSval=71501915 T
13020	10.176191129	TCP	192.168.2.15	192.168.2.1	66	45676 > 5001 [ACK] Seq=301 Ack=208 Win=15744 Len=0 TSval=71501915
13021	10.176785042	TCP	192.168.2.15	192.168.2.1	67	45676 > 5001 [PSH, ACK] Seq=301 Ack=208 Win=15744 Len=1 TSval=7150
13022	10.177261645	TCP	192.168.2.15	192.168.2.1	66	45676 > 5001 [FIN, ACK] Seq=302 Ack=208 Win=15744 Len=0 TSval=7150
13024	10.177513776	TCP	192.168.2.15	192.168.2.1	66	45676 > 5001 [ACK] Seq=303 Ack=209 Win=15744 Len=0 TSval=71501917

Tham khảo thêm:

- Xây dựng ứng dụng client/server với TCP:  
<https://users.soict.hust.edu.vn/hoangph/textbook/ch02-2.html>
- Xây dựng ứng dụng client/server với UDP:  
<https://users.soict.hust.edu.vn/hoangph/textbook/ch02-3.html>

## Bài 2: Dịch vụ DNS - BIND & DNS tools (dig, nslookup)

BIND là ứng dụng cung cấp DNS server phổ biến nhất hiện nay. Bài này yêu cầu cài đặt và thực hiện các cấu hình cơ bản của một máy chủ BIND. Ngoài ra, một số công cụ hỗ trợ làm việc với DNS cũng cần được cài đặt. Các bước thực hiện như sau:

- Bước 1: Tải phần mềm BIND và cài đặt.
- Bước 2: Cài đặt và sử dụng lệnh dig.
- Bước 3: Cài đặt và sử dụng lệnh nslookup.

### Bước 1: Tải phần mềm BIND và cài đặt

Thiết lập ít nhất một card mạng cho máy chủ CentOS sử dụng cơ chế NAT để có thể truy nhập Internet thông qua máy host Windows. Kiểm tra kết nối Internet và sử dụng công cụ *yum* để cài đặt *bind* và các ứng dụng hỗ trợ *bind* (*bind-utils*) như *nslookup* hay *dig*. Có thể kiểm tra các gói ứng dụng này đã có trên máy chủ CentOS hay chưa rồi tiến hành cài đặt:

```
> yum list bind bind-utils
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
* base: centos-hn.viettelidc.com.vn
* extras: centos-hn.viettelidc.com.vn
* updates: centos-hn.viettelidc.com.vn
Installed Packages
bind.x86_64                32:9.8.2-0.37.rc1.el6_7.4      @updates
bind-utils.x86_64          32:9.8.2-0.37.rc1.el6_7.4      @updates

> yum install bind bind-utils
Loaded plugins: fastestmirror
Setting up Install Process
Loading mirror speeds from cached hostfile
* base: centos-hn.viettelidc.com.vn
* extras: centos-hn.viettelidc.com.vn
* updates: centos-hn.viettelidc.com.vn
Package 32:bind-9.8.2-0.37.rc1.el6_7.4.x86_64 already installed and latest version
Package 32:bind-utils-9.8.2-0.37.rc1.el6_7.4.x86_64 already installed and latest version
```

Chú ý kiểm tra quyền truy nhập của **file zone**. Khi chạy lệnh *dig* mà DNS server không trả về kết quả (thiếu thông tin *ANSWER SECTION* cùng với thông tin trạng thái *status: SERVFAIL*) thì có thể là do không đọc được file zone. Khi đó cần kiểm tra và bổ sung quyền đọc (read) cho file này với lệnh *chmod +r*.

### Bước 2: Cài đặt và sử dụng lệnh *dig*

Lệnh sau đây kiểm tra kết nối đến máy chủ DNS tại địa chỉ 127.0.0.1 và hiển thị resource record thuộc tất cả các kiểu (có thể thay *any* bằng SOA, NS, MX, v.v..) thuộc domain *mydomain.vn*:

```
> dig @127.0.0.1 mydomain.vn any

; <<>> DiG 9.8.2rc1-RedHat-9.8.2-0.37.rc1.el6_7.4 <<>> @127.0.0.1 mydomain.vn any
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 16658
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 2

;; QUESTION SECTION:
;mydomain.vn.          IN      ANY

;; ANSWER SECTION:
mydomain.vn.          86400   IN      SOA     ns1.mydomain.vn. hostmaster.hp.vn. 20151108 86400 3600 604800 10800
mydomain.vn.          86400   IN      NS      ns1.mydomain.vn.
mydomain.vn.          86400   IN      MX      10 mail.mydomain.vn.

;; ADDITIONAL SECTION:
ns1.mydomain.vn.      86400   IN      A        1.2.3.4
mail.mydomain.vn.     86400   IN      A        2.3.4.5

;; Query time: 1 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Wed Nov 11 07:24:33 2015
;; MSG SIZE rcvd: 150
```

Cần kiểm tra kết nối DNS giữa các máy chủ bằng cách thay 127.0.0.1 thành địa chỉ IP của máy chủ khác. Nếu kết nối thành công, kết quả cũng giống như khi chạy trên nội bộ máy DNS. Trường hợp có lỗi xảy ra, *dig* sẽ hiển thị thông tin như sau:

```
> dig @192.168.56.2 mydomain.vn any

; <<>> DiG 9.8.2rc1-RedHat-9.8.2-0.37.rc1.el6_7.4 <<>> @192.168.56.2 mydomain.vn any
; (1 server found)
;; global options: +cmd
;; connection timed out; no servers could be reached
```

Cần kiểm tra một số tình huống gây lỗi sau đây:

- DNS server được cấu hình **mặc định** chỉ **chấp nhận kết nối từ máy nội bộ**, không nhận các kết nối từ bên ngoài. Dùng lệnh *netstat -a|grep domain* để kiểm tra service DNS đã chạy và chấp nhận các truy nhập từ tất cả các máy trên mạng hay chưa (cổng 53 được khai báo mặc định là *domain* trong file cấu hình */etc/services*). Nếu chưa, mở file cấu hình *named.conf* và sửa lại cho phép kết nối từ tất cả các máy trên mạng thông qua các tham số *listen-on* và *allow-query* như sau:

```
options {
    listen-on port 53 { any; };
    allow-query { any; };
};
```

- DNS server mặc định chạy firewall iptables và có thể đang block các kết nối tcp hoặc udp. Chạy lệnh `service iptables status` để kiểm tra và nếu cần có thể tạm thời dừng firewall iptables bằng lệnh `service iptables stop`.

### Bước 3: Cài đặt và sử dụng lệnh nslookup

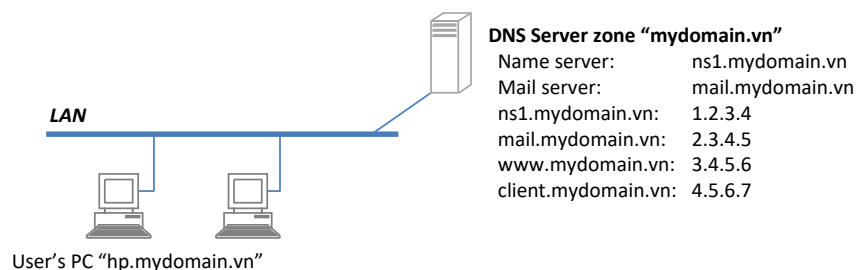
`nslookup` cho phép thực hiện các câu truy vấn DNS đến các máy chủ DNS bất kỳ. Câu lệnh bên dưới truy vấn đến máy chủ DNS `mydomain.com` yêu cầu hiển thị tất cả các resource record tương ứng tên miền `www.redhat.com`:

```
> nslookup -type=any www.redhat.com mydomain.vn
Server:      mydomain.vn
Address:     192.168.56.3#53

Non-authoritative answer:
www.redhat.com canonical name = ev-www.redhat.com.edgekey.net.

Authoritative answers can be found from:
redhat.com      nameserver = ns4.redhat.com.
redhat.com      nameserver = ns3.redhat.com.
redhat.com      nameserver = ns2.redhat.com.
redhat.com      nameserver = ns1.redhat.com.
ns3.redhat.com  internet address = 209.132.176.100
ns1.redhat.com  internet address = 209.132.186.218
ns4.redhat.com  internet address = 209.132.188.218
ns2.redhat.com  internet address = 209.132.183.2
```

## Bài 3: Xây dựng một DNS server nội bộ với BIND



Bài thực hành này yêu cầu thiết lập **một DNS server nội bộ** cho mạng Intranet của một công ty với **tên miền mydomain.vn**. DNS nội bộ cung cấp dịch vụ tên miền cho một số máy chủ riêng của công ty như Mail, Web, v.v.. và các máy trạm (client). Các bước thực hiện như sau:

- Bước 1: Cấu hình máy chủ BIND.
- Bước 2: Vận hành và kiểm tra dịch vụ DNS.

### Bước 1: Cấu hình máy chủ BIND

Bỏ qua các thông tin không quan trọng, các file cấu hình cần thiết như sau:

```
> cat /etc/named.conf

options {
    listen-on port 53 { any; };
    directory "/var/named";
    allow-query { any; };
    recursion no;
};

logging {
    channel default_debug {
        file "data/named.run";
```

```

        severity dynamic;
    };
};

zone "." IN {
    type hint;
    file "named.empty";
};

zone "mydomain.vn" IN {
    type master;
    file "named.mydomain.vn";
    allow-update { none; };
};

```

Trong mục *options*, tham số *listen-on* cho phép thiết lập DNS server nghe ở cổng nào (53) vào có thể truy nhập từ đâu (*any* = bất cứ máy nào). Tham số *directory* thiết lập thư mục chứa các file dữ liệu. Tham số *recursion* xác định cách làm việc của DNS server (trong trường hợp này là “no recursive”).

Mục zone “.” cung cấp cho server danh sách các máy chủ root. BIND thường được cung cấp kèm với file */var/named/named.ca* chứa danh sách máy chủ gốc. Trong trường hợp này ta muốn máy chủ DNS chỉ phục vụ các tên miền nội bộ của công ty nên thay vì sử dụng file *named.ca*, ta sử dụng file “rỗng” *named.empty* như sau:

```

> cat /var/named/named.empty
$TTL 3H
@   IN SOA @ rname.invalid. (
        0      ; serial
        1D     ; refresh
        1H     ; retry
        1W     ; expire
        3H )   ; minimum
NS  @
A   127.0.0.1
AAAA ::1

```

```

> cat /var/named/named.mydomain.vn
$TTL 1D ; resource record can be cached by other server for maximum 1 day
@   IN  SOA  ns1.mydomain.vn. hostmaster.hp.vn. (
        20151108      ; serial
        1D     ; refresh
        1H     ; retry
        1W     ; expire
        3H )   ; minimum
NS   ns1.mydomain.vn.
MX 10 mail.mydomain.vn.
ns1  A   1.2.3.4
mail A   2.3.4.5
www  A   3.4.5.6
client A 4.5.6.7

```

## Bước 2: Vận hành và kiểm tra dịch vụ DNS

Sau khi hoàn thành thiết lập các file cấu hình, khởi động lại dịch vụ DNS:

```

> service named restart
Stopping named:          [ OK ]
Starting named:          [ OK ]

```

Để kiểm tra hoạt động của DNS server, sử dụng *dig* để liệt kê tất cả các resource record của máy chủ DNS (giả sử server có địa chỉ là 192.168.56.5):

```

> dig @192.168.56.5 mydomain.vn any

```

```

; <<>> DiG 9.8.2rc1-RedHat-9.8.2-0.37.rc1.el6_7.4 <<>> @192.168.56.5 mydomain.vn any
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 47070
;; flags: qr aa rd; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 2
;; WARNING: recursion requested but not available

;; QUESTION SECTION:
;mydomain.vn.      IN      ANY

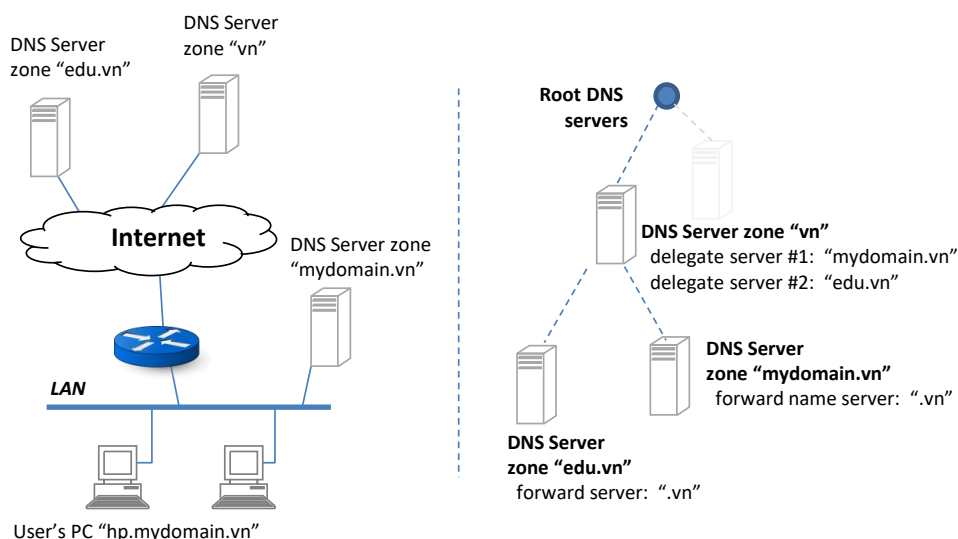
;; ANSWER SECTION:
mydomain.vn.      86400  IN      SOA     ns1.mydomain.vn. hostmaster.hp.vn. 20151108 86400 3600 604800 10800
mydomain.vn.      86400  IN      NS      ns1.mydomain.vn.
mydomain.vn.      86400  IN      MX      10 mail.mydomain.vn.

;; ADDITIONAL SECTION:
ns1.mydomain.vn.  86400  IN      A       1.2.3.4
mail.mydomain.vn. 86400  IN      A       2.3.4.5

;; Query time: 0 msec
;; SERVER: 192.168.56.3#53(192.168.56.3)
;; WHEN: Wed Nov 11 04:35:54 2015
;; MSG SIZE rcvd: 150

```

## Bài 4: Kết nối DNS trên Internet



Sau khi đã thiết lập được máy chủ DNS nội bộ, bước tiếp theo cần làm là **kết nối máy chủ DNS nội bộ** này vào **hệ thống DNS trên Internet**. Hình vẽ bên trên mô tả mô hình kết nối vật lý giữa các máy chủ và mô hình kết nối logic giữa các máy chủ để quản lý dữ liệu DNS. Theo mô hình logic này, máy chủ DNS của tên miền **"mydomain.vn"** **trở thành con** của máy chủ DNS phụ trách tên miền **"vn"**. Ngoài ra, cần **tích hợp** thống tên **miền "vn"** với hệ thống tên miền **trên toàn bộ mạng Internet**. Các bước thực hiện như sau:

- Bước 1: Cấu hình DNS **"mydomain.vn"**.
- Bước 2: Cấu hình DNS **"vn"**.
- Bước 3: Cấu hình DNS hỗ trợ các zone bên ngoài.

### Bước 1: Cấu hình DNS **"mydomain.vn"**

Để máy chủ DNS **"mydonain.vn"** có thể **trả lời các câu truy vấn** dữ liệu thuộc **tên miền cấp trên "vn"**, sử dụng chức năng **forwarding của dịch vụ DNS**. Bổ sung khai báo zone **"vn"** sau đây vào file



*/etc/named.conf* của máy chủ tên miền “*mydomain.vn*” và đặt lại tham số *recursion* thành *yes* (thiết lập máy chủ DNS “*mydomain.vn*” có khả năng hỗ trợ câu truy vấn đệ qui):

```
options {
    listen-on port 53 { any; };
    directory "/var/named";
    allow-query { any; };
    recursion yes;
};

zone "vn" IN {
    type forward;
    forwarders {192.168.56.2;};
    forward only;
};
```

Khởi động lại service *named* và sử dụng *dig* để kiểm tra máy chủ *mydomain.vn* đã có thể trả lời các câu truy vấn dữ liệu thuộc zone *vn*. Nếu hệ thống chạy tốt, kết quả trả về (trong phần ANSWER SECTION sẽ liệt kê các resource record thuộc zone “*vn*”:

```
> dig @mydomain.vn vn any

;<<>> DiG 9.8.2rc1-RedHat-9.8.2-0.37.rc1.el6_7.4 <<>> @mydomain.vn vn any
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 30827
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 2, ADDITIONAL: 2

;; QUESTION SECTION:
;vn.                IN      ANY

;; ANSWER SECTION:
vn.                 83318  IN      NS     ns2.vn.
vn.                 83318  IN      NS     ns1.vn.

;; AUTHORITY SECTION:
vn.                 83318  IN      NS     ns1.vn.
vn.                 83318  IN      NS     ns2.vn.

;; ADDITIONAL SECTION:
ns1.vn.             83318  IN      A       1.2.3.4
ns2.vn.             83321  IN      A       2.3.4.5

;; Query time: 2 msec
;; SERVER: 192.168.56.3#53(192.168.56.3)
;; WHEN: Wed Nov 11 06:11:31 2015
;; MSG SIZE rcvd: 116
```

Có thể kiểm tra thêm bằng *nslookup* để truy vấn các dữ liệu zone “*vn*” thông qua máy chủ *mydomain.vn*. Các dữ liệu zone “*vn*” được máy chủ *mydomain.vn* trả về trong phần *Non-authoritative answer*:

```
> nslookup -type=any vn mydomain.vn
Server:      mydomain.vn
Address:     192.168.56.3#53

Non-authoritative answer:
vn  nameserver = ns2.vn.
vn  nameserver = ns1.vn.

Authoritative answers can be found from:
vn  nameserver = ns2.vn.
vn  nameserver = ns1.vn.
ns1.vn internet address = 1.2.3.4
ns2.vn internet address = 2.3.4.5
```

So sánh với dữ liệu *nslookup* trả về khi truy vấn zone “*mydomain.vn*”. Các dữ liệu này được gọi là *Authoritative* (phân biệt với *Non-authoritative* bên trên).

```
> nslookup -type=any mydomain.vn mydomain.vn
Server:      mydomain.vn
Address:     192.168.56.3#53

mydomain.vn
  origin = ns1.mydomain.vn
  mail addr = hostmaster.hp.vn
  serial = 20151108
  refresh = 86400
  retry = 3600
  expire = 604800
  minimum = 10800
mydomain.vn  nameserver = ns1.mydomain.vn.
mydomain.vn  mail exchanger = 10 mail.mydomain.vn.
```

### Bước 2: Cấu hình DNS “vn”

Vấn đề tiếp theo là cấu hình để máy chủ zone “vn” có thể trả lời các truy vấn dữ liệu của zone “*mydomain.vn*”. Phương pháp ủy quyền (delegation) của dịch vụ DNS được sử dụng. Muốn vậy, trùng zone file của tên miền “vn” (/var/named/named.vn) bổ sung thêm các thông tin về máy chủ DNS của tên miền con (subdomain) “*mydomain.vn*”:

```
$TTL 1D ; resource record can be cached by other server for maximum 1 day
@   IN   SOA  ns1.vn. hostmaster.vn. (
        20151108      ; serial
        1D           ; refresh
        1H           ; retry
        1W           ; expire
        3H )         ; minimum
    IN   NS   ns1.vn.
    IN   NS   ns2.vn.
w3     IN   MX 10  mail.vn.
m3     IN   MX 20  mail2.vn.
ns1     A   1.2.3.4
ns2     A   2.3.4.5
mail    A   3.4.5.6
mail2   A   4.5.6.7
ftp     CNAME mail.vn.

$ORIGIN mydomain.vn.
@   IN   NS   ns1.mydomain.vn.
ns1  A   192.168.56.3
```

Trong phần *\$ORIGIN* của tên miền con *mydomain.vn*, khai báo resource record kiểu *NS* (name server) với tên miền *ns1.mydomain.vn* và khai báo địa chỉ IP của tên miền này là địa chỉ máy chủ tên miền *mydomain.vn* (trong ví dụ là *192.168.56.3*). Khởi động lại dịch vụ DNS trên máy chủ tên miền “vn” và sử dụng *dig* để kiểm tra máy chủ “vn” đã có thể trả lời các câu truy vấn tên miền con “*mydomain.vn*”:

```
> dig @vn mydomain.vn any

;<<>> DiG 9.8.2rc1-RedHat-9.8.2-0.37.rc1.el6_7.4 <<>> @vn mydomain.vn any
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 27784
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 1, ADDITIONAL: 2

;; QUESTION SECTION:
;mydomain.vn.                IN      ANY

;; ANSWER SECTION:
mydomain.vn.                86393 IN     MX     10 mail.mydomain.vn.
```

```

mydomain.vn.      83856 IN   NS    ns1.mydomain.vn.

;; AUTHORITY SECTION:
mydomain.vn.      83856 IN   NS    ns1.mydomain.vn.

;; ADDITIONAL SECTION:
mail.mydomain.vn. 86393 IN   A     2.3.4.5
ns1.mydomain.vn.  83856 IN   A     1.2.3.4

;; Query time: 0 msec
;; SERVER: 192.168.56.2#53(192.168.56.2)
;; WHEN: Wed Nov 11 06:32:38 2015
;; MSG SIZE rcvd: 114

```

Kiểm tra truy vấn dữ liệu tên miền “mydomain.vn” thông qua máy chủ “vn” bằng *nslookup*:

```

> nslookup -type=any mydomain.vn vn
Server:      vn
Address:     192.168.56.2#53

Non-authoritative answer:
mydomain.vn  mail exchanger = 10 mail.mydomain.vn.
mydomain.vn  nameserver = ns1.mydomain.vn.

Authoritative answers can be found from:
mydomain.vn  nameserver = ns1.mydomain.vn.
mail.mydomain.vn  internet address = 2.3.4.5
ns1.mydomain.vn internet address = 1.2.3.4

```

### Bước 3: Cấu hình DNS hỗ trợ các zone bên ngoài

Sau hai bước vừa xong, các máy chủ tên miền “vn” và “mydomain.vn” đã có thể truy vấn dữ liệu thông qua nhau và trả kết quả về cho client (phân biệt qua *Authorative* và *Non-authorative*). Vấn đề cuối cùng là làm cho các máy chủ này có khả năng truy vấn dữ liệu thuộc các zone ngoài “vn”. Giải pháp là sử dụng tính năng “*hint*” thông qua các máy chủ gốc (root). Thông tin các máy chủ gốc được lưu trữ trong file */var/named/named.ca*:

```

a.root-servers.net. 518400 IN   A     198.41.0.4
b.root-servers.net. 518400 IN   A     192.228.79.201
c.root-servers.net. 518400 IN   A     192.33.4.12
d.root-servers.net. 518400 IN   A     199.7.91.13
e.root-servers.net. 518400 IN   A     192.203.230.10
f.root-servers.net. 518400 IN   A     192.5.5.241
g.root-servers.net. 518400 IN   A     192.112.36.4
h.root-servers.net. 518400 IN   A     128.63.2.53
i.root-servers.net. 518400 IN   A     192.36.148.17
j.root-servers.net. 518400 IN   A     192.58.128.30
k.root-servers.net. 518400 IN   A     193.0.14.129
l.root-servers.net. 518400 IN   A     199.7.83.42
m.root-servers.net. 518400 IN   A     202.12.27.33
a.root-servers.net. 518400 IN   AAAA  2001:503:ba3e::2:30
c.root-servers.net. 518400 IN   AAAA  2001:500:2::c
d.root-servers.net. 518400 IN   AAAA  2001:500:2d::d
f.root-servers.net. 518400 IN   AAAA  2001:500:2f::f
h.root-servers.net. 518400 IN   AAAA  2001:500:1::803f:235
i.root-servers.net. 518400 IN   AAAA  2001:7fe::53
j.root-servers.net. 518400 IN   AAAA  2001:503:c27::2:30
k.root-servers.net. 518400 IN   AAAA  2001:7fd::1
l.root-servers.net. 518400 IN   AAAA  2001:500:3::42
m.root-servers.net. 518400 IN   AAAA  2001:dc3::35

```

Bổ sung khai báo zone “.” vào file cấu hình *named.conf* và nhớ kiểm tra tính năng recursion được bật (yes). Lưu ý là tính năng này có thể được khai báo ở bất cứ máy chủ nào (như là *mydomain.vn* hay *edu.vn*) chứ không nhất thiết là phải ở máy chủ cấp cao nhất (như là *vn*).

```
zone "." IN {
    type hint;
    file "named.ca";
};
```

Khởi động lại dịch vụ DNS để nhận khả năng “*hint*” từ các máy chủ root và kiểm tra bằng *nslookup* để thấy máy chủ DNS đã có thể trả về dữ liệu nằm ngoài zone “*vn*”:

```
> nslookup -type=any www.redhat.com vn
Server:      vn
Address:     192.168.56.2#53

Non-authoritative answer:
www.redhat.com canonical name = ev-www.redhat.com.edgekey.net.

Authoritative answers can be found from:
redhat.com nameserver = ns1.redhat.com.
redhat.com nameserver = ns2.redhat.com.
redhat.com nameserver = ns3.redhat.com.
redhat.com nameserver = ns4.redhat.com.
ns2.redhat.com internet address = 209.132.183.2
ns1.redhat.com internet address = 209.132.186.218
ns4.redhat.com internet address = 209.132.188.218
ns3.redhat.com internet address = 209.132.176.100
```

Nguyên tắc hoạt động của tính năng này như sau. Khi nhận được câu truy vấn dữ liệu ở ngoài vùng phụ trách (Non-authoritative), ví dụ là *www.redhat.com*, và cũng không thuộc forward zone nào, máy chủ DNS “*vn*” sẽ chọn một máy chủ gốc từ danh sách “*hint*” và truy vấn các máy chủ phụ trách zone “*com*”. Khi nhận được danh sách các máy chủ phụ trách zone “*com*”, máy chủ DNS “*vn*” lại chọn ra một máy chủ từ danh sách này và truy vấn danh sách máy chủ phụ trách zone “*redhat.com*”. Cuối cùng, khi nhận được danh sách các máy chủ phụ trách zone “*redhat.com*”, máy chủ DNS “*vn*” chọn 1 máy chủ từ danh sách này và truy vấn thông tin của tên miền “*www.redhat.com*”. Quá trình này có thể được hiển thị khi dùng lệnh *dig* với tham số “*+trace*”:

```
> dig @mydomain.vn redhat.com +trace

;<<>> DiG 9.8.2rc1-RedHat-9.8.2-0.37.rc1.el6_7.4 <<>> @mydomain.vn redhat.com +trace
; (1 server found)
;; global options: +cmd
.      513007 IN    NS     j.root-servers.net.
.      513007 IN    NS     l.root-servers.net.
.      513007 IN    NS     d.root-servers.net.
.      513007 IN    NS     g.root-servers.net.
.      513007 IN    NS     h.root-servers.net.
.      513007 IN    NS     a.root-servers.net.
.      513007 IN    NS     k.root-servers.net.
.      513007 IN    NS     c.root-servers.net.
.      513007 IN    NS     e.root-servers.net.
.      513007 IN    NS     m.root-servers.net.
.      513007 IN    NS     i.root-servers.net.
.      513007 IN    NS     f.root-servers.net.
.      513007 IN    NS     b.root-servers.net.
;; Received 496 bytes from 192.168.56.3#53(192.168.56.3) in 66208 ms

com.    172800 IN    NS     a.gtld-servers.net.
com.    172800 IN    NS     b.gtld-servers.net.
com.    172800 IN    NS     c.gtld-servers.net.
com.    172800 IN    NS     d.gtld-servers.net.
com.    172800 IN    NS     e.gtld-servers.net.
com.    172800 IN    NS     f.gtld-servers.net.
com.    172800 IN    NS     g.gtld-servers.net.
com.    172800 IN    NS     h.gtld-servers.net.
com.    172800 IN    NS     i.gtld-servers.net.
com.    172800 IN    NS     j.gtld-servers.net.
com.    172800 IN    NS     k.gtld-servers.net.
com.    172800 IN    NS     l.gtld-servers.net.
```

```

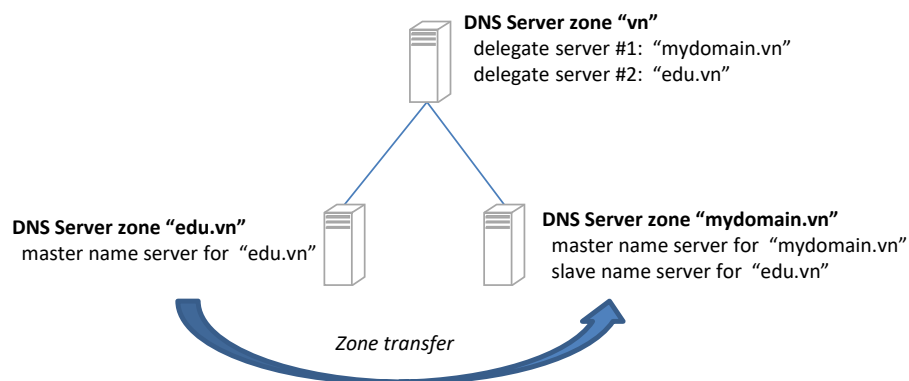
com.          172800 IN   NS    m.gtld-servers.net.
;; Received 488 bytes from 128.63.2.53#53(128.63.2.53) in 66563 ms

redhat.com.   172800 IN   NS    ns2.redhat.com.
redhat.com.   172800 IN   NS    ns3.redhat.com.
redhat.com.   172800 IN   NS    ns1.redhat.com.
redhat.com.   172800 IN   NS    ns4.redhat.com.
;; Received 164 bytes from 192.12.94.30#53(192.12.94.30) in 21357 ms

www.redhat.com. 60 IN    CNAME  ev-www.redhat.com.edgekey.net.
;; Received 75 bytes from 209.132.188.218#53(209.132.188.218) in 195 ms

```

## Bài 5: Master & Slave DNS



Ta đã có 2 máy chủ DNS làm việc ở trạng thái master cho 2 zone “*edu.vn*” và “*mydomain.vn*”. Để đảm bảo tính sẵn sàng của dịch vụ, cần thiết lập thêm một máy chủ slave cho zone “*edu.vn*”, giả sử chính là máy chủ *mydomain.vn*. Như vậy, máy chủ DNS *mydomain.vn* vừa đóng vai trò master cho zone “*mydomain.vn*” đồng thời đóng vai trò slave cho zone “*edu.vn*”. Các bước thực hiện như sau:

- Bước 1: Cấu hình máy chủ DNS master và slave.
- Bước 2: Kiểm tra vận hành hệ thống.

### Bước 1: Cấu hình máy chủ DNS master & slave

Cập nhật file cấu hình */etc/named.conf* của máy chủ *edu.vn* để khai báo thêm slave cho zone “*edu.vn*”:

```

zone "edu.vn" IN {
    type master;
    file "named.edu.vn";
    allow-transfer { 192.168.56.3; };
    allow-update { none; };
};

```

Tham số *allow-transfer* cho phép khai báo các địa chỉ (của các máy chủ slave) mà có thể nhận được dữ liệu zone transfer từ máy chủ hiện tại. Trong trường hợp này, 192.168.56.3 chính là máy chủ *mydomain.vn*.

Trên máy chủ *mydomain.vn*, cập nhật file cấu hình */etc/named.conf* để khai báo thêm zone “*edu.vn*” với vai trò slave:

```

zone "edu.vn" IN {
    type slave;
    file "slaves/named.edu.vn";
    masters {192.168.56.4;};
};

```

```
};
```

## Bước 2: Kiểm tra vận hành hệ thống

Khởi động lại các service DNS lần lượt trên các máy chủ *edu.vn* và *mydomain.vn*. Các máy chủ sẽ tự động chuyển dữ liệu zone từ máy master sang máy server. Kiểm tra log thấy xuất hiện thông báo chuyển dữ liệu thành công:

```
> tail /var/log/messages
Nov 11 11:13:43 mydomain named[3490]: running
Nov 11 11:13:43 mydomain named[3490]: zone edu.vn/IN: Transfer started.
Nov 11 11:13:43 mydomain named[3490]: transfer of 'edu.vn/IN' from 192.168.56.4#53: connected using 192.168.56.3#44614
Nov 11 11:13:43 mydomain named[3490]: zone edu.vn/IN: transferred serial 20151108
Nov 11 11:13:43 mydomain named[3490]: transfer of 'edu.vn/IN' from 192.168.56.4#53: Transfer completed: 1 messages, 10 records, 258 bytes, 0.001 secs (258000 bytes/sec)
```

Sau khi thực hiện chuyển dữ liệu zone từ máy chủ master sang máy chủ slave, dữ liệu này sẽ được ghi lại trong file */var/named/slaves/named.edu.vn*. Tắt dịch vụ DNS trên máy *edu.vn* và truy vấn dữ liệu zone “edu.vn” đến máy chủ slave *mydomain.vn*. Các câu truy vấn sẽ vẫn được thực hiện thành công:

```
> nslookup -type=any edu.vn mydomain.vn
Server:      mydomain.vn
Address:     192.168.56.3#53

edu.vn
  origin = ns1.edu.vn
  mail addr = hostmaster.edu.vn
  serial = 20151108
  refresh = 86400
  retry = 3600
  expire = 604800
  minimum = 10800
edu.vn nameserver = ns1.edu.vn.
edu.vn mail exchanger = 10 mail.edu.vn.

> dig @mydomain.vn edu.vn any

;<<<> DiG 9.8.2rc1-RedHat-9.8.2-0.37.rc1.el6_7.4 <<<> @mydomain.vn edu.vn any
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 65350
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 2

;; QUESTION SECTION:
;edu.vn.                IN      ANY

;; ANSWER SECTION:
edu.vn.                  86400   IN      SOA     ns1.edu.vn. hostmaster.edu.vn. 20151108 86400 3600 604800 10800
edu.vn.                  86400   IN      NS      ns1.edu.vn.
edu.vn.                  86400   IN      MX      10 mail.edu.vn.

;; ADDITIONAL SECTION:
ns1.edu.vn.              86400   IN      A       192.168.56.4
mail.edu.vn.             86400   IN      A       10.0.2.16

;; Query time: 1 msec
;; SERVER: 192.168.56.3#53(192.168.56.3)
;; WHEN: Wed Nov 11 11:22:27 2015
;; MSG SIZE rcvd: 142
```

## Bài 6: Thiết lập hệ thống email cho một domain

Trong bài thực hành này, ta sẽ cấu hình máy chủ email có tên miền *mail.mydomain.vn* chạy *Postfix* để cung cấp dịch vụ email cho domain “*mydomain.vn*”. Đây là phần mềm Email server phổ biến hiện nay và có sẵn trên CentOS. Trên các máy trạm, sử dụng các phần mềm *mail* hoặc *mutt*. Các bước thực hiện như sau:

- Cấu hình Email server *Postfix*.
- Cài đặt Email client *mail* hoặc *mutt*.
- Vận hành và kiểm tra hệ thống.
- Sử dụng các bí danh (aliases).

### Bước 1: Cấu hình Email server *Postfix*

#### a) Thiết lập tên hostname

Tên miền của máy chủ email là *mail.mydomain.vn*, tức là khi máy chủ liên lạc với các máy chủ khác sẽ sử dụng tên miền này để tìm kiếm. Trong khi đó, các email được giao dịch trong domain và ra ngoài domain có dạng *<user name>@mydomain.vn*. *Postfix* sử dụng tham số *myhostname* để đưa vào phần domain trong các địa chỉ email. Sửa lại (hoặc thêm mới) tham số *myhostname* trong file cấu hình */etc/postfix/main.cf*:

```
myhostname = mydomain.vn
```

#### b) Thiết lập domain được *Postfix* cung cấp dịch vụ

*Postfix* dựa vào tên domain trong địa chỉ email để xác định email đó có thuộc phạm vi cung cấp dịch vụ của mình không (máy chủ email có thể đồng thời cung cấp dịch vụ email cho nhiều domain – xem bài thực hành sau). Tham số *mydestination* trong file config liệt kê các domain này:

```
mydestination = $myhostname
```

#### c) Thiết lập tên miền tự động gắn vào địa chỉ email

Khi các user gửi mail trong nội bộ domain, có thể dùng tên login thay cho địa chỉ email. Khi gửi email ra ngoài domain, *Postfix* sẽ kiểm tra và tự động gắn thêm tên miền vào email. Tham số *myorigin* trong file config thiết lập phần tên domain này:

```
myorigin = $myhostname
```

### Bước 2: Cài đặt Email client *mail* hoặc *mutt*

Có nhiều lựa chọn cho user để làm việc với mail trên Linux. *Mail* mà *mutt* là 2 phần mềm phổ dụng. *Mail* nhỏ gọn nhưng sử dụng khá bất tiện. *Mutt* cung cấp giao diện khá tiện dụng. Sử dụng yum để cài đặt các ứng dụng này trên các máy client:

```
[root@Client ~]# yum install mail mutt
...
Resolving Dependencies
--> Running transaction check
--> Package mailx.x86_64 0:12.4-8.el6_6 will be installed
--> Package mutt.x86_64 5:1.5.20-7.20091214hg736b6a.el6 will be installed
--> Processing Dependency: urlview for package: 5:mutt-1.5.20-7.20091214hg736b6a.el6.x86_64
--> Processing Dependency: libtokyocabinet.so.8()(64bit) for package: 5:mutt-1.5.20-7.20091214hg736b6a.el6.x86_64
--> Running transaction check
--> Package tokyocabinet.x86_64 0:1.4.33-6.el6 will be installed
```

```

---> Package urlview.x86_64 0:0.9-7.el6 will be installed
--> Finished Dependency Resolution

Dependencies Resolved

...

Installed:
  mailx.x86_64 0:12.4-8.el6_6                mutt.x86_64 5:1.5.20-7.20091214hg736b6a.el6

Dependency Installed:
  tokyocabinet.x86_64 0:1.4.33-6.el6          urlview.x86_64 0:0.9-7.el6

Complete!

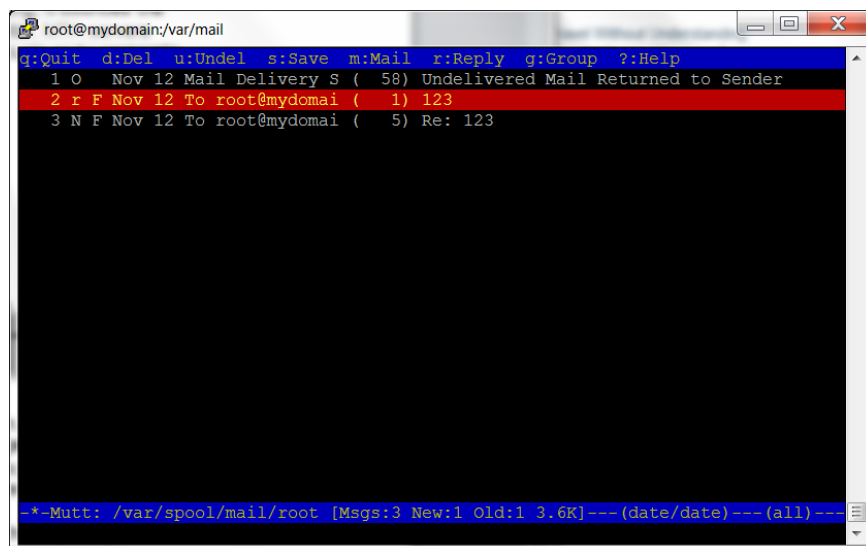
```

Giao diện tương tác người dùng của các phần mềm mail và mutt như sau:

```

> mail
Heirloom Mail version 12.4 7/29/08. Type ? for help.
"/var/spool/mail/root": 3 messages 2 unread
>U 1 Mail Delivery System Thu Nov 12 10:25 78/2403 "Undelivered Mail Retu"
A 2 root Thu Nov 12 10:42 22/582 "123"
U 3 root Thu Nov 12 10:43 27/736 "Re: 123"
&_

```



### Bước 3: Vận hành và kiểm tra hệ thống

Khởi động lại dịch vụ mail để cập nhật các thay đổi cấu hình vừa tiến hành:

```
> service postfix restart
```

Tạo một số user trong hệ thống bằng lệnh *adduser* và *passwd* để vận hành dịch vụ Email:

```

> adduser hp01
> passwd hp01
Changing password for user hp01.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
> adduser hp02
> passwd hp02
Changing password for user hp02.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.

```



Sử dụng *mutt* hoặc *mail* để gửi nhận mail giữa *root*, *hp01* và *hp02*. Có thể kiểm tra hệ thống bằng cách sử dụng *telnet* để nói chuyện với *Postfix* theo giao thức *SMTP*:

```
> telnet 127.0.0.1 25
Trying 127.0.0.1...
Connected to 127.0.0.1.
Escape character is '^]'.
220 mydomain.vn ESMTP Postfix
HELO client.mydomain.vn
250 mydomain.vn
MAIL FROM: <hp02@mydomain.vn>
250 2.1.0 Ok
RCPT TO: <hp01@mydomain.vn>
250 2.1.5 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
test abbbbb
.
250 2.0.0 Ok: queued as 137DF401A4
QUIT
221 2.0.0 Bye
Connection closed by foreign host.
```

#### Bước 4: Sử dụng các bí danh (*aliases*)

Đa phần các trường hợp tên hiển thị trong email khác với tên login vào hệ thống. Ngoài ra, với trường hợp các user đặc biệt như *root*, việc gửi/nhận mail trực tiếp đến user này có thể gây nhiều bài toán an ninh. Để xử lý vấn đề này, mỗi tài khoản user trong hệ thống nên được gắn với một hoặc nhiều bí danh. Các bí danh này sẽ được sử dụng trong địa chỉ email khi gửi/nhận mail thay vì tên login.

File */etc/aliases* cho phép liệt kê các bí danh của user trong hệ thống. Một số bí danh mặc định đã có như *postmaster* (cho *root*), *fptadmin* (cho *fpt*), v.v.. Ta có thể tạo thêm các bí danh cho từng người sử dụng hoặc nhóm:

```
> cat /etc/aliases
#users
hoang.pham: hp01
phamhuyhoang: hp02

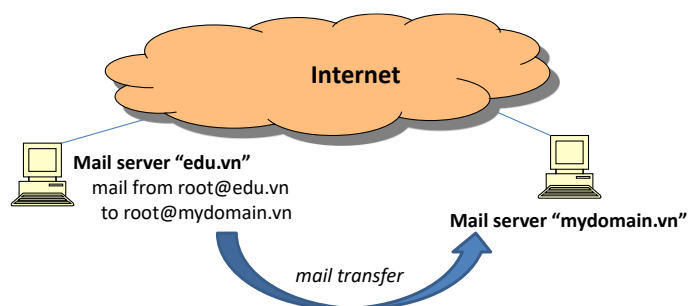
#groups
prof: hp01, hp02
```

Chú ý: sau khi cập nhật file *aliases* phải chạy index lại bằng lệnh *newaliases* và khởi động lại *Postfix*:

```
> newaliases
> service postfix restart
Shutting down postfix: [ OK ]
Starting postfix: [ OK ]
```

Hệ thống khởi động thành công sẽ cho phép gửi nhận mail với các bí danh thay vì tên login. Sử dụng *mail* hoặc *mutt* để kiểm tra chức năng này.

## Bài 7: Thiết lập hệ thống email giữa 2 domain



Thực hiện các bước tương tự như bài thực hành trên, máy chủ *mail.edu.vn* được cấu hình để cung cấp thêm dịch vụ email cho domain “*edu.vn*”. Trong bài thực hành này, các máy chủ Email cần kết nối được với nhau để chuyển tiếp mail giữa 2 domain có các thông số cấu hình như sau:

Zone "edu.vn":            name: mail.edu.vn  
   IP: 192.168.56.4

Zone "mydomain.vn": name: mail.mydomain.vn  
IP: 192.168.56.3

Các bước thực hiện như sau:

- Bước 1: Kiểm tra hệ thống hàng đợi email
- Bước 2: Kết nối với hệ thống DNS
- Bước 3: Kiểm tra vận hành hệ thống

### Bước 1: Kiểm tra hệ thống hàng đợi mail

Khi một user trong domain “*mydomain.vn*” gửi mail cho một user khác trong cùng domain, mail này sẽ được chuyển ngay vào mailbox của user trên máy chủ email. Trường hợp gửi cho một user nằm ngoài domain, mail sẽ được đưa vào hàng đợi để *Postfix* trên các máy chủ email liên lạc với nhau và chuyển tiếp mail. Lệnh *postqueue -p* hiển thị danh sách các mail đang thuộc hàng đợi. Mỗi mail được gán với một mã số *Queue ID*:

```
> postqueue -p
-Queue ID-- --Size-- -----Arrival Time----- -Sender/Recipient-----
7411B4019A    397 Thu Nov 12 12:02:32  root@mydomain.vn
              (connect to mail.edu.vn[1.2.3.4]:25: Connection refused)
              hp@edu.vn

EFFF840180    402 Thu Nov 12 11:49:59  root@mydomain.vn
              (connect to mail.edu.vn[2.3.4.5]:25: Connection refused)
              root@edu.vn
```

Để xem nội dung một mail đang trong hàng đợi, sử dụng lệnh *postcat -q* với mã số mail trong hàng đợi:

```
> postcat -q EFFD840180
*** ENVELOPE RECORDS deferred/E/EFFD840180 ***
message_size:      402      199      1      0      402
message_arrival_time: Thu Nov 12 11:49:59 2015
create_time: Thu Nov 12 11:49:59 2015
named_attribute: rewrite_context=local
sender_fullname: root
sender: root@mydomain.vn
original_recipient: root@edu.vn
recipient: root@edu.vn
*** MESSAGE CONTENTS deferred/E/EFFD840180 ***
```

```
Received: by mydomain.vn (Postfix, from userid 0)
        id EFFD840180; Thu, 12 Nov 2015 11:49:59 -0500 (EST)
Date: Thu, 12 Nov 2015 11:49:59 -0500
From: root <root@mydomain.vn>
To: root@edu.vn
Subject: test
Message-ID: <20151112164959.GA1466@mydomain.vn>
MIME-Version: 1.0
Content-Type: text/plain; charset=us-ascii
Content-Disposition: inline
User-Agent: Mutt/1.5.20 (2009-12-10)
```

```
abc
:wq!
```

```
*** HEADER EXTRACTED deferred/E/EFFD840180 ***
*** MESSAGE FILE END deferred/E/EFFD840180 ***
```

Tùy theo cấu hình, *Postfix* liên lạc với nhau và gửi mail đang nằm trong các hàng đợi. Sử dụng lệnh *postqueue -f* để yêu cầu *Postfix* gửi ngay email đang nằm trong hàng đợi.

### Bước 2: Kết nối với hệ thống DNS

Nhìn vào nội dung hàng đợi có thể thấy trạng thái các mail. Hiện tại đều có trạng thái là “*connect to mail.edu.vn[1.2.3.4]:25: Connection refused*”. Có thể thấy ngay địa chỉ IP của các máy chủ mail đang sai. Các thông báo lỗi chi tiết có thể được xem trong file log với lệnh “*tail /var/log/maillog*”. Sử dụng dịch vụ DNS để sửa lại các địa chỉ IP của mail server cho đúng. Ví dụ, đối với zone “*edu.vn*”, cần cập nhật lại resource record kiểu MX:

```
$TTL 1D ; resource record can be cached by other server for maximum 1 day
$ORIGIN edu.vn.
@ IN SOA ns1.edu.vn. hostmaster.edu.vn. (
        20151108 ; serial
        1D ; refresh
        1H ; retry
        1W ; expire
        3H ) ; minimum
    NS ns1.edu.vn.
    MX 10 mail.edu.vn.
ns1 A 192.168.56.4
mail A 192.168.56.4
```

Xử lý tương tự trên máy chủ DNS zone “*mydomain.vn*”:

```
$TTL 1D ; resource record can be cached by other server for maximum 1 day
@ IN SOA ns1.mydomain.vn. hostmaster.hp.vn. (
        20151108 ; serial
        1D ; refresh
        1H ; retry
        1W ; expire
        3H ) ; minimum
    NS ns1.mydomain.vn.
    MX 10 mail.mydomain.vn.
ns1 A 192.168.56.3
mail A 192.168.56.3
```

Khởi động lại các dịch vụ DNS trên các máy chủ DNS và dùng *nslookup* kiểm tra các máy chủ *mail.mydomain.vn* và *mail.edu.vn* đã được cập nhật địa chỉ IP đúng.

### Bước 3: Kiểm tra và vận hành hệ thống

Sử dụng *postqueue -f* để yêu cầu postfix chuyển tiếp tất cả các mail trong hàng đợi và lại kiểm tra hàng đợi bằng *postqueue -p*:

```

> postqueue -f
> postqueue -p
-Queue ID-- --Size-- ----Arrival Time---- -Sender/Recipient-----
7411B4019A   397 Thu Nov 12 12:02:32 root@mydomain.vn
              (connect to mail.edu.vn[192.168.56.4]:25: Connection refused)
              hp@edu.vn

EFFF840180   402 Thu Nov 12 11:49:59 root@mydomain.vn
              (connect to mail.edu.vn[192.168.56.4]:25: Connection refused)
              root@edu.vn

-- 1 Kbytes in 2 Requests.

```

Có thể thấy các mail vẫn chưa được chuyển đi nhưng trạng thái đã thay đổi (chuyển thành “*Connection refused*”) cùng với các địa chỉ IP của mail server đã được cập nhật chính xác. Có thể phán đoán được rằng postfix trên máy *mydomain.vn* đã tìm được đúng địa chỉ IP của mail server cho tên miền “*edu.vn*” nhưng khi kết nối thì chưa thành công.

Lý do ở đây là vấn đề đảm bảo an ninh. Postfix được cấu hình mặc định không nhận chuyển tiếp mail từ bên ngoài. Nó chỉ nhận mail qua card mạng *localhost*. Trong tình huống hiện tại, các Postfix trên máy *mail.edu.vn* và *mail.mydomain.vn* cần phải liên lạc với nhau qua cổng 25. Có thể kiểm tra bằng lệnh *telnet* vào cổng 25 hoặc *netstat* xem các dịch vụ của hệ thống đang nghe kết nối trên card mạng nào:

```

> netstat -a | grep smtp
tcp        0      0 localhost:smtp      *.*          LISTEN
tcp        0      0 localhost:smtp      *.*          LISTEN
unix 2      [ ACC ] STREAM LISTENING 10785 private/smtp

```

Sửa lại tham số *inet\_interfaces* trong file cấu hình */etc/postfix/main.cf* để cho phép Postfix nhận kết nối từ tất cả các card mạng của máy chủ:

```
net_interfaces = all
```

Khởi động lại dịch vụ Postfix và kiểm tra với *netstat*:

```

> service postfix restart
Shutting down postfix: [ OK ]
Starting postfix: [ OK ]
> netstat -a | grep smtp
tcp        0      0 *:smtp              *.*          LISTEN
tcp        0      0 *:smtp              *.*          LISTEN
unix 2      [ ACC ] STREAM LISTENING 26792 private/smtp

```

Sử dụng *postqueue -f* để yêu cầu chuyển tiếp mail trong hàng đợi và check lại bằng *postqueue -p*. Khi mail đã được chuyển đi thành công, sử dụng *mail* hoặc *mutt* trên các máy chủ *mail.edu.vn* và *mail.mydomain.vn* để kiểm tra gửi nhận mail đã chạy tốt giữa 2 domain.