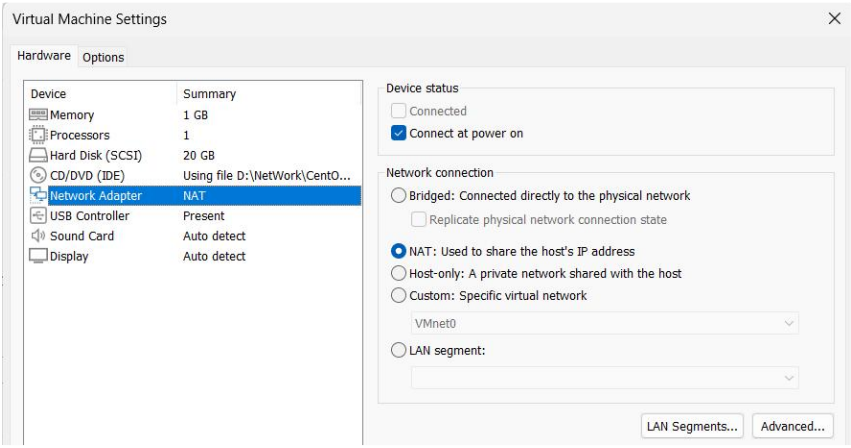
DNS SERVER TRÊN CENTOS7

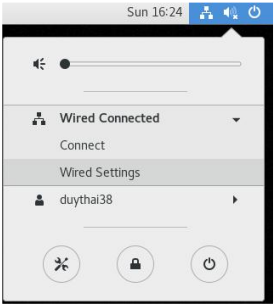
■ PHẦN 1 CÀI ĐẶT & CẤU HÌNH DNS SERVER

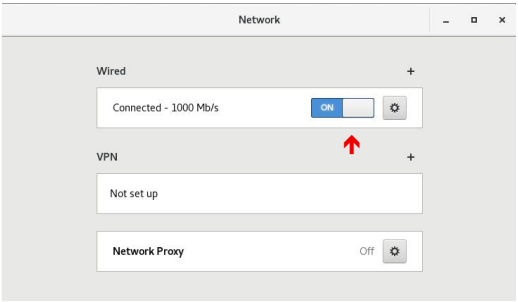
BƯỚC 1: Cài đặt gói BIND (Berkeley Internet Name Domain)

Trước khi cài đặt gói bind ta cần kiểm tra kết nối đến Internet: Virtual Machine → Virtual Machine Settings → Hardware thiết lập Network Adapter ở chế độ NAT



Sau đó Power On Virtual Machine, vào giao diện cấu hình IP: chọn Wired Settings bật ON





Ta có thể kiểm tra kết nối qua lệnh ping tới địa chỉ 8.8.8.8 hoặc 1.1.1.1

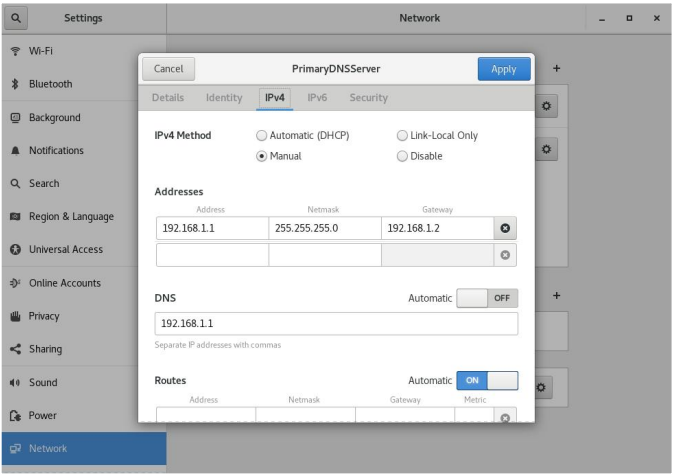
```
[root@localhost ~]# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=128 time=41.5 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=128 time=39.6 ms
^C
--- 8.8.8.8 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 39.686/40.599/41.513/0.935 ms
```

Cuối cùng tiến hành cài đặt gói bind, công cụ kiểm tra và làm việc với DNS ở quyền root

```
yum install bind bind-utils -y
```

BƯỚC 2: Thực hiện cấu hình IP tĩnh bằng giao diện đồ họa

Tại IPv4 Method chọn Manual để cấu hình IP tĩnh và nhấn Apply



BƯỚC 3: Cấu hình DNS

Đầu tiên cấu hình tập tin named.conf ở quyền root bằng lệnh:

```
nano /etc/named.conf
```

Chỉnh các thông số như sau:

```
 GNU nano 2.3.1            File: /etc/named.conf


options {
        listen-on port 53 { 127.0.0.1;192.168.1.1; };
        #listen-on-v6 port 53 { ::1; };
        directory       "/var/named";
        dump-file       "/var/named/data/cache_dump.db";
        statistics-file "/var/named/data/named_stats.txt";
        memstatistics-file "/var/named/data/named_mem_stats.txt";
        recursing-file  "/var/named/data/named.recursing";
        secroots-file   "/var/named/data/named.secroots";
        allow-query     { localhost;192.168.1.0/24;any; };
```

Tiếp theo định nghĩa vùng (zone) phân giải xuôi và phân giải ngược cho tên miền nội bộ trong tập tin named.rfc1912.zones hoặc named.conf

```
nano /etc/named.rfc1912.zones
```

```
 GNU nano 2.3.1          File: /etc/named.rfc1912.zones

//
zone "sgu.edu.vn" IN {
        type master;
        file "forward.sgu.edu.vn";
        allow-update { none; };
};

zone "1.168.192.in-addr.arpa" IN {
        type master;
        file "reverse.192.168.1.0";
        allow-update {none; } ;
};
```

Tạo các bản ghi (Record) cho vùng phân giải xuôi (forward zone):

```
nano /var/named/forward.sgu.edu.vn
```

```
  GNU nano 2.3.1       File: /var/named/forward.sgu.edu.vn

$TTL    86400
@       IN      SOA     server.dgu.edu.vn. root.sgu.egu.vn. (
        2025070901      ;Serial
        3600            ;Refresh
        1800            ;Retry
        604800          ;Expire
        86400           ;Minimun TTL
)
@       IN      NS      server.sgu.edu.vn.
@       IN      A       192.168.1.1
server  IN      A       192.168.1.1
```

Tạo các bản ghi (Record) cho vùng phân giải ngược (reverse zone):

```
nano /var/named/reverse.192.168.1.0
```

```
  GNU nano 2.3.1       File: /var/named/reverse.192.168.1.0          Modified

$TTL    86400
@       IN      SOA     server.sgu.edu.vn. root.sgu.edu.vn. (
        2025090701      ;Serial
        3600            ;Refresh
        1800            ;Retry
        604800          ;Expire
        86400           ;Minimun TTL
)
@       IN      NS      server.sgu.edu.vn.
1       IN      PTR     server.sgu.edu.vn.
1       IN      PTR     sgu.edu.vn.
```

BƯỚC 4: Khởi động DNS

Ta khởi động DNS bằng 2 câu lệnh sau

```
systemctl enable named
systemctl start named
```

Ngoài ra, đôi khi ta phải tắt firewall để DNS hoạt động.

```
firewall-cmd --permanent --zone=public --add-service=dns
firewall-cmd --reload
```

Sau đó ta có thể kiểm tra lại DNS bằng câu lệnh nslookup hoặc dig/host

```
[root@localhost ~]# nslookup
> sgu.edu.vn
Server:         192.168.1.1
Address:        192.168.1.1#53

Name:   sgu.edu.vn
Address: 192.168.1.1
> 192.168.1.1
1.1.168.192.in-addr.arpa        name = sgu.edu.vn.
1.1.168.192.in-addr.arpa        name = server.sgu.edu.vn.
>
```

■ PHẦN 2 CÀI ĐẶT VÀ CẤU HÌNH BACKUP DNS SERVER

XÉT MÔ HÌNH MẠNG NHƯ SAU

BƯỚC 1: Chỉnh sửa một số cấu hình và khởi động lại dịch vụ trên Primary DNS Server

Trên máy Primary DNS Server, vào cấu hình tập tin named.conf ta nhập lệnh

```
nano /etc/named.conf
```

Thêm vào dòng allow-transfer {localhost; 192.168.1.2;}; để khai báo việc truyền dữ liệu của DNS Server. Ở đây, ta cho phép máy Primary có thể truyền dữ liệu sang máy 192.168.1.2 là máy Secondary DNS Server.

```
 GNU nano 2.3.1            File: /etc/named.conf


options {
        listen-on port 53 { 127.0.0.1;192.168.1.1; };
        #listen-on-v6 port 53 { ::1; };
        directory       "/var/named";
        dump-file       "/var/named/data/cache_dump.db";
        statistics-file "/var/named/data/named_stats.txt";
        memstatistics-file "/var/named/data/named_mem_stats.txt";
        recursing-file  "/var/named/data/named.recursing";
        secroots-file   "/var/named/data/named.secroots";
        allow-query     { localhost;192.168.1.0/24;any; };
        allow-transfer  { localhost;192.168.1.2; };
```

Thiết lập thêm các cấu hình trên file: forward.sgu.edu.vn đã cấu hình ở phần 1 trước đó

```
nano /var/named/forward.sgu.edu.vn
```

```
 GNU nano 2.3.1       File: /var/named/forward.sgu.edu.vn

$TTL 86400
@       IN      SOA     server.sgu.edu.vn. root.sgu.edu.vn. (
        2025080901      ;Serial
        3600            ;Refresh
        1800            ;Retry
        60400           ;Expire
        86400           ;Minimum TTL
)

@       IN      NS      server.sgu.edu.vn.
@       IN      NS      secondary.sgu.edu.vn.
@       IN      A       192.168.1.1
server  IN      A       192.168.1.1
secondary       IN      A       192.168.1.2
```

Thiết lập thêm các cấu hình trên file: reverse.192.168.1.0 đã cấu hình ở phần 1 trước đó

```
nano /var/named/reverse.sgu.edu.vn
```

```
 GNU nano 2.3.1        File: /var/named/reverse.192.168.1.0

$TTL 86400
@       IN      SOA     server.sgu.edu.vn. root.shu.edu.vn. (
        2025080901      ;Serial
        3600            ;Refresh
        1800            ;Retry
        60400           ;Expire
        86400           ;Minimum TTL
)
@       IN      NS      server.sgu.edu.vn.
@       IN      NS      secondary.sgu.edu.vn.
1       IN      PTR     server.sgu.edu.vn.
1       IN      PTR     sgu.edu.vn.
2       IN      PTR     secondary.sgu.edu.vn.
```

Sau khi đã thêm các thiết lập ở trên, ta save lại và cho restart lại dịch vụ DNS để đồng bộ dữ liệu:

```
systemctl restart named
```

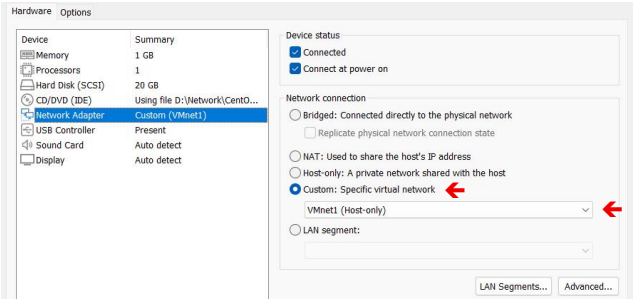
Dùng lệnh nslookup để kiểm tra các thông số như sau:

```
[root@server ~]# nslookup
> sgu.edu.vn
Server:         192.168.1.1
Address:        192.168.1.1#53

Name:   sgu.edu.vn
Address: 192.168.1.1
> server.sgu.edu.vn
Server:         192.168.1.1
Address:        192.168.1.1#53

Name:   server.sgu.edu.vn
Address: 192.168.1.1
> secondary.sgu.edu.vn
Server:         192.168.1.1
Address:        192.168.1.1#53

Name:   secondary.sgu.edu.vn
Address: 192.168.1.2
> 192.168.1.1
1.1.168.192.in-addr.arpa        name = sgu.edu.vn.
1.1.168.192.in-addr.arpa        name = server.sgu.edu.vn.
> 192.168.1.2
2.1.168.192.in-addr.arpa        name = secondary.sgu.edu.vn.
```

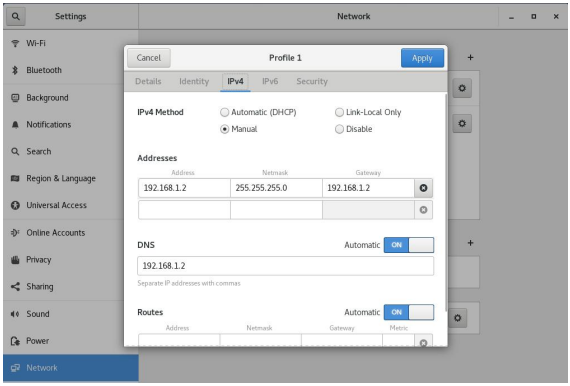
BƯỚC 2: Cấu hình Secondary DNS Server

Trước tiên cài đặt gói bind và bind-utils như phần 1

Ta cũng cần chỉnh lại card mạng sang dạng VMNET1 (host only) trên cả 2 máy Primary DNS Server và Secondary DNS Server để đảm bảo rằng các DNS server này chỉ vận hành trong mạng Local trước



Cấu hình IP động như sau:



Cấu hình file named.conf trên máy Secondary DNS Server

```
nano /etc/named.conf
```

```
 GNU nano 2.3.1              File: /etc/named.conf


options {
        listen-on port 53 { 127.0.0.1; 192.168.1.2; };
        #listen-on-v6 port 53 { ::1; };
        directory       "/var/named";
        dump-file       "/var/named/data/cache_dump.db";
        statistics-file "/var/named/data/named_stats.txt";
        memstatistics-file "/var/named/data/named_mem_stats.txt";
        recursing-file  "/var/named/data/named.recursing";
        secroots-file   "/var/named/data/named.secroots";
        allow-query     { localhost;192.168.1.0/24;any; };
        allow-transfer  { localhost;192.168.1.1; };
```

Sau đó ta sẽ vào cấu hình các zones:

```
nano /etc/named.rfc1912.zones
```

```
 GNU nano 2.3.1          File: /etc/named.rfc1912.zones

//
zone "sgu.edu.vn" IN {
        type slave;
        file "slaves/forward.sgu.edu.vn";
        masters {192.168.1.1;};
};

zone "1.168.192.in-addr.arpa" IN {
        type slave;
        file "slaves/reverse.192.168.1.0";
        masters {192.168.1.1;};
};
```

Tiếp theo thực hiện start dịch vụ DNS để đồng bộ dữ liệu

```
systemctl start named
```

Và tắt tường lửa trên Secondary DNS Server

```
systemctl stop firewalld
systemctl disable firewalld
```

Sau khi start dịch vụ, ta cần restart dịch vụ 1 lần nửa để đảm bảo rằng các file đã được đồng bộ

```
systemctl restart named
```

Kiểm tra trong thư mục slaves

```
ls -l /var/named/slaves
```

Dùng lệnh nslookup để kiểm tra

```
[root@localhost ~]# nslookup
> sgu.edu.vn
Server:         192.168.1.2
Address:        192.168.1.2#53

Name:   sgu.edu.vn
Address: 192.168.1.1
> server.sgu.edu.vn
Server:         192.168.1.2
Address:        192.168.1.2#53

Name:   server.sgu.edu.vn
Address: 192.168.1.1
> secondary.sgu.edu.vn
Server:         192.168.1.2
Address:        192.168.1.2#53

Name:   secondary.sgu.edu.vn
Address: 192.168.1.2
> 192.168.1.1
1.1.168.192.in-addr.arpa        name = server.sgu.edu.vn.
1.1.168.192.in-addr.arpa        name = sgu.edu.vn.
> 192.168.1.2
2.1.168.192.in-addr.arpa        name = secondary.sgu.edu.vn.
```

Ngoài ra, khi ta cập nhật DNS trên máy Primary, ta nên thay đổi chỉ số serial, sau đó ta có thể dùng lệnh sau để tự động cập nhật ở máy Secondary:

```
rndc reload [zone-name]
```

PHẦN 3 THIẾT LẬP FORWARDER GIỮA CÁC DNS SERVER

XÉT MÔ HÌNH MẠNG NHƯ SAU

Trên DNS Server 1	Trên DNS Server 2
Ta cấu hình DNS Server như đã thực hiện ở phần 1, ở đây ta sẽ tạo 1 zone là sgu.edu.vn cho DNS Server 1 quản lý với IP như sau: IPv4 Address 192.168.1.1 IPv6 Address fe80::6b29:761e:1797:ff20 Hardware Address 00:0C:29:3D:86:F1 Default Route 192.168.1.1 DNS 192.168.1.1	Ta cấu hình DNS Server như đã thực hiện ở phần 1, ở đây ta sẽ tạo 1 zone là linux.org cho DNS Server 2 quản lý với IP như sau: IPv4 Address 192.168.1.2 IPv6 Address fe80::e9f4:416c:dac:a705 Hardware Address 00:0C:29:62:4D:74 Default Route 192.168.1.2 DNS 192.168.1.2

Kiểm tra trên DNS Server 1

```
[root@localhost ~]# nslookup
> sgu.edu.vn
Server:                 192.168.1.1
Address:        192.168.1.1#53

Name:sgu.edu.vn
Address: 192.168.1.1
> linux.org
;; connection time out; no servers could be reach
```

Kiểm tra trên DNS Server 2

```
[root@localhost ~]# nslookup
> sgu.edu.vn
;; connection time out; no servers could be reach
> linux.org
Server:                 192.168.1.2
Address:        192.168.1.2#53

Name:linux.org
Address: 192.168.1.2
```

Ta thấy khi truy vấn tên miền thì cả 2 DNS Server đều không truy vấn được tên miền do DNS Server còn lại quản lí, do đó ta phải cấu hình forwarder cho các DNS Server

Trên DSN Server 1 ta thực hiện chỉnh sửa cấu hình

nano /etc/named.conf

```
 GNU nano 2.3.1            File: /etc/named.conf


options {
        listen-on port 53 { 127.0.0.1;192.168.1.1; };
        #listen-on-v6 port 53 { ::1; };
        directory       "/var/named";
        dump-file       "/var/named/data/cache_dump.db";
        statistics-file "/var/named/data/named_stats.txt";
        memstatistics-file "/var/named/data/named_mem_stats.txt";
        recursing-file  "/var/named/data/named.recursing";
        secroots-file   "/var/named/data/named.secroots";
        allow-query     { localhost;192.168.1.0/24;any; };
        forwarders      { 192.168.1.2; };
```

Ta cấu hình thêm 2 dòng sau

```
 GNU nano 2.3.1            File: /etc/named.conf

           reduce such attack surface
        */
        recursion yes;

        dnssec-enable no;
        dnssec-validation no;
```

Để đảm bảo mọi thứ vận hành tốt, ta có thể chỉnh **SELINUX** để tạm tắt tính năng Security của Linux, giúp cho việc trao đổi truy vấn DNS sẽ chạy ổn định hơn. Tuy nhiên, với cách làm này, sau khi đã hoàn thiện hệ thống, ta cần phải thiết lập lại security để hệ thống bảo đảm an toàn. nhập câu lệnh sau:

nano /etc/sysconfig/selinux

```
 GNU nano 2.3.1          File: /etc/sysconfig/selinux


# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#     enforcing - SELinux security policy is enforced.
#     permissive - SELinux prints warnings instead of enforcing.
#     disabled - No SELinux policy is loaded.
SELINUX=disable
# SELINUXTYPE= can take one of three values:
#     targeted - Targeted processes are protected,
#     minimum - Modification of targeted policy. Only selected processes are pr$
#     mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

Trên DSN Server 2 ta thực hiện chỉnh sửa cấu hình

nano /etc/named.conf

```
 GNU nano 2.3.1            File: /etc/named.conf                    Modified


options {
        listen-on port 53 { 127.0.0.1;192.168.1.2; };
        #listen-on-v6 port 53 { ::1; };
        directory       "/var/named";
        dump-file       "/var/named/data/cache_dump.db";
        statistics-file "/var/named/data/named_stats.txt";
        memstatistics-file "/var/named/data/named_mem_stats.txt";
        recursing-file  "/var/named/data/named.recursing";
        secroots-file   "/var/named/data/named.secroots";
        allow-query     { localhost;192.168.1.0/24;any; };
        forwarders      { 192.168.1.1; };
```

Còn lại làm như DNS Server 1

Sau khi thực hiện chỉnh sửa cấu hình trên 2 DNS Server, ta khởi động lại dịch vụ để đồng bộ

```
systemctl restart named
```

Kiểm tra việc phân giải ở hai máy:

Trên DNS Server 1

```
[root@localhost ~]# nslookup
> sgu.edu.vn
Server:         192.168.1.1
Address:        192.168.1.1#53

Name:   sgu.edu.vn
Address: 192.168.1.1
> linux.org
Server:         192.168.1.1
Address:        192.168.1.1#53

Non-authoritative answer:
Name:   linux.org
Address: 192.168.1.2
```

Trên DNS Server 2

```
[root@localhost ~]# nslookup
> sgu.edu.vn
Server:         192.168.1.2
Address:        192.168.1.2#53

Non-authoritative answer:
Name:   sgu.edu.vn
Address: 192.168.1.1
> linux.org
Server:         192.168.1.2
Address:        192.168.1.2#53

Name:   linux.org
Address: 192.168.1.2
```