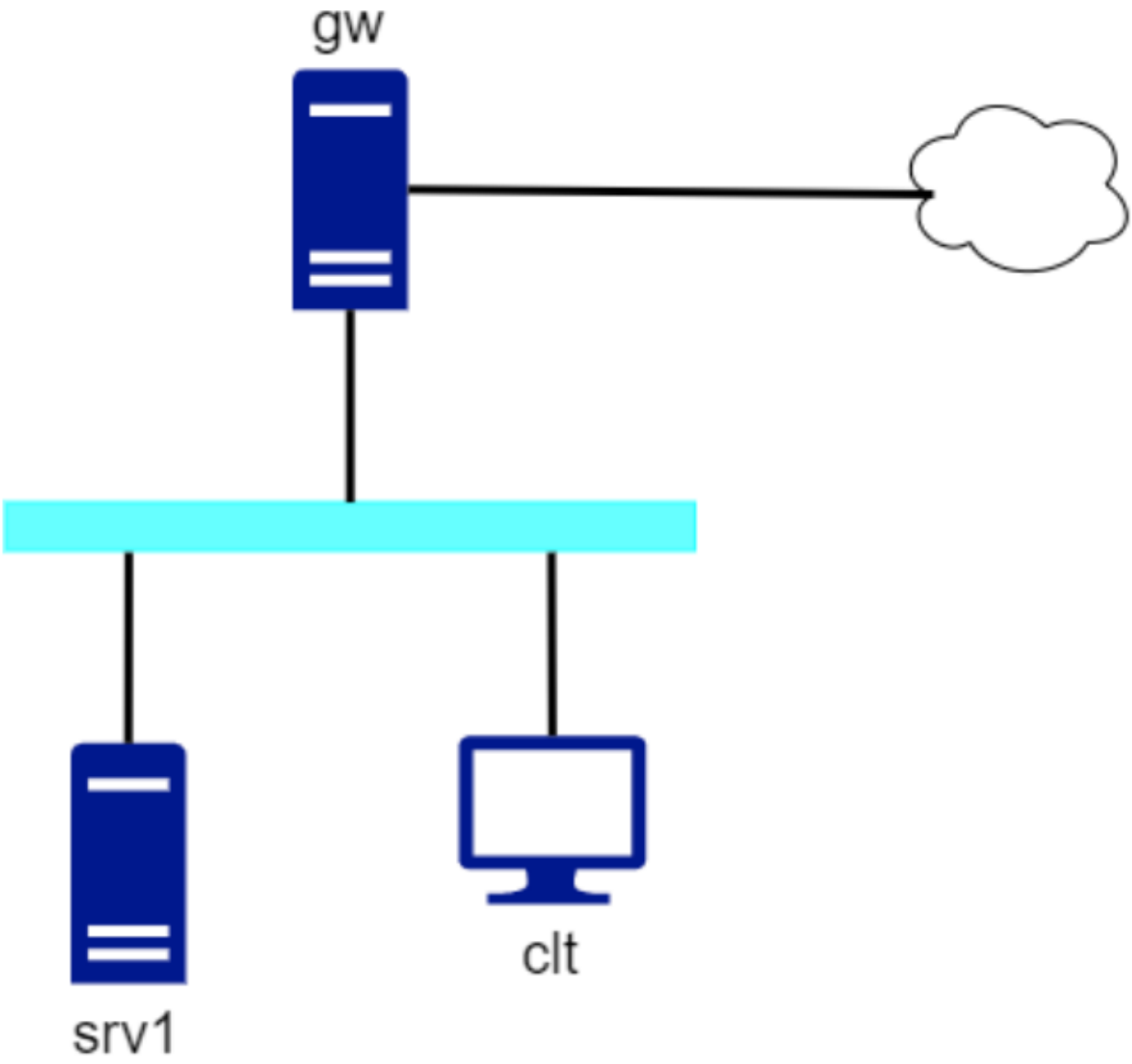
計網4

```
vi /etc/bind/named.conf.options
dnssec-validation no; // close
forward :
. . . .
```

```
nslookup //查dns
e.g.:www.id.nasa
e.g.:www.google.nasa
```

LAB9

整體架構：



Hostname	Interface	IP Address	Gateway	Nameserver
gw	<對外實體網卡>	僅用來連 wan VPN	僅用來連 wan VPN	僅用來連 wan VPN
	wan	via vpn profile	via vpn profile	via vpn profile
	lan	192.168.3.254/24		
srv1	eth0	192.168.3.1/24	192.168.3.254	<your nameserver's ip address>
clt	eth0	via DHCP	via DHCP	via DHCP

gw

用nat網路

/etc/netplan/00-installer-config.yaml

```
# This is the network config written by 'subiquity'
network:
  ethernets:
    ens33:
      dhcp4: true
      nameservers:
              addresses: [10.100.100.254]
    lan:
      dhcp4: false
      match:
              macaddress: "00:0c:29:3f:e2:ea"
      set-name: lan
      addresses: [192.168.3.254/24]
  version: 2
~
```

ISC DHCP Server

```
apt install isc-dhcp-server
```

DHCP server 為內網機器配發 IP

```
vim /etc/dhcp/dhcpd.conf

sudo systemctl restart isc-dhcp-server
sudo systemctl status isc-dhcp-server
```

```
option domain-name "q56101078.nasa";
option domain-name-servers 10.100.100.254;

default-lease-time 600;
max-lease-time 7200;

subnet 192.168.3.0 netmask 255.255.255.0 {
        range 192.168.3.100 192.168.3.200;
        option routers 192.168.3.254;
}
```

filter 設定

```
iptables -P INPUT DROP

iptables -A INPUT -i lo -j ACCEPT
#Allow SSH session to firewall 2 by using the following command:
iptables -A INPUT -p tcp --dport 22 -s 0/0 -j ACCEPT

#Allow ICMP traffic to firewall 2 by using the following command:
iptables -A INPUT -p icmp -j ACCEPT

#Allow all related and established traffic for firewall 2 by using the following
iptables -A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT

#dns domain port=53
iptables -A INPUT -p tcp --dport 53 -s 0/0 -j ACCEPT

iptables -A INPUT -p tcp --dport 80 -s 0/0 -j ACCEPT

iptables -t nat -A POSTROUTING -s 192.168.3.1/24 -o wan -j MASQUERADE

iptables -t nat -A PREROUTING -i wan -p tcp --dport 80 -j DNAT \
            --to-destination 192.168.3.1 #srv1 ip

```

```
*filter
:INPUT ACCEPT [16:3815]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [102:15251]
-P INPUT DROP
-A INPUT -i lo -j ACCEPT
-A INPUT -p tcp -m tcp --dport 22 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 53 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 80 -j ACCEPT
-A INPUT -p udp -m udp --dport 53 -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
```

```
*nat
:PREROUTING ACCEPT [22089:1460785]
:INPUT ACCEPT [132:10792]
:OUTPUT ACCEPT [76:6247]
:POSTROUTING ACCEPT [76:6247]
-A POSTROUTING -s 192.168.3.0/24 -o wan -j MASQUERADE
-A POSTROUTING -j MASQUERADE
COMMIT
```

```
q56101078@gw:~$ sudo iptables -L
Chain INPUT (policy DROP)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:ssh
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:domain
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:http
ACCEPT     udp  --  anywhere             anywhere             udp dpt:domain
ACCEPT     icmp --  anywhere             anywhere
ACCEPT     all  --  anywhere             anywhere             state RELATED,ESTABLISHED
```

參考 (https://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-sg-zh_tw-4/s1-firewall-ipt-fwd.html)

修改options

```
sudo vim /etc/bind/named.conf.options
```

新增下列

```
dnssec-validation no;
forward only;
allow-query { any;};
allow-transfer { any;};
listen-on port 53 { any;};
listen-on { any;};
forwarders {
        10.100.100.254;
};
auth-nxdomain no;
listen-on-v6 { any; };
```

增加zone

使用 views

`sudo vim /etc/bind/named.conf.local`

```
view "internal" {
        match-clients {
                192.168.3.0/24;
        };

        zone "q56101078.nasa" {
                type master;
                file "/etc/bind/db.q56101078.nasa";
                allow-query { localhost; 192.168.3.0/24; };
                allow-update { none; };
        };

        //zone "3.168.192.in-addr.arpa" {
                //type master;
                //file "/etc/bind/db.192";
                //allow-query { any; };
                //allow-update { none;};
        //};
};
view "external" {
        match-clients {
                any;
        };
        zone "q56101078.nasa" {
                type master;
                file "/etc/bind/db.q56101078.nasa.ext";
                allow-query { any; };
                allow-update { none; };
        };

        //zone "100.100.10.in-addr.arpa" {
                //type master;
                //file "/etc/bind/db.10";
                //allow-query {any;};
                //allow-update { none;};
                //};
};
```

`/etc/bind/named.conf.local`

需要將全部包起來，當作一個views

```
// prime the server with knowledge of the root servers
view "default-zones" {

        match-clients {any;};
        zone "." {
                type hint;
                file "/usr/share/dns/root.hints";
        };

        // be authoritative for the localhost forward and reverse zones, and for
        // broadcast zones as per RFC 1912

        zone "localhost" {
                type master;
                file "/etc/bind/db.local";
        };

        zone "127.in-addr.arpa" {
                type master;
                file "/etc/bind/db.127";
        };

        zone "0.in-addr.arpa" {
                type master;
                file "/etc/bind/db.0";
        };

        zone "255.in-addr.arpa" {
                type master;
"/etc/bind/named.conf.default-zones" 34L, 570C
```

1. `sudo vim /etc/bind/db.q56101078.nasa`

```
;
; BIND data file for local loopback interface
;
$TTL    604800
$ORIGIN q56101078.nasa.
@       IN      SOA     dns.q56101078.nasa. root.q56101078.nasa. (
                              1         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      dns.q56101078.nasa.

dns     IN      A       192.168.3.254

www     IN      A       192.168.3.1
```

2. 反易 `/etc/bind/db.192`

```
; BIND reverse data file for local loopback interface
;
$TTL    604800
@       IN      SOA     ns.q56101078.nasa. root.q56101078.nasa. (
                              1         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      ns.q56101078.nasa.
ns      IN      A       192.168.3.1

1       IN      PTR     www.q56101078.nasa.
1       IN      PTR     ns.q56101078.nasa.
```

3. `sudo vim /etc/bind/db.q56101078.nasa.ext`

```
;
; BIND data file for local loopback interface
;
$TTL    604800
$ORIGIN q56101078.nasa.
@       IN      SOA     dns.q56101078.nasa. root.q56101078.nasa. (
                              1         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      dns.q56101078.nasa.

dns     IN      A       10.100.100.87

www     IN      A       10.100.100.87
~
~
```

4. 反易 `/etc/bind/db.10`

```
;
; BIND reverse data file for local loopback interface
;
$TTL    604800
@       IN      SOA     ns.q56101078.nasa. root.q56101078.nasa. (
                              1         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      dns.q56101078.nasa.
ns      IN      A       10.100.100.87

87      IN      PTR     www.q56101078.nasa.
87      IN      PTR     ns.q56101078.nasa.
~
~
```

看有無設定好

named-checkzone

```
named-checkzone name.nasa /etc/bind/db.192
```

看看nameserver

```
sudo vim /etc/resolv.conf
```

```
nameserver 127.0.0.53
options edns0 trust-ad
search localdomain
```

```
sudo vim /run/systemd/resolve/resolv.conf
```

```
nameserver 10.100.100.254
nameserver 192.168.220.2
search localdomain
```

查詢 systemd-resolved 服務的設定

```
resolvectl status #看看dns
```

重載

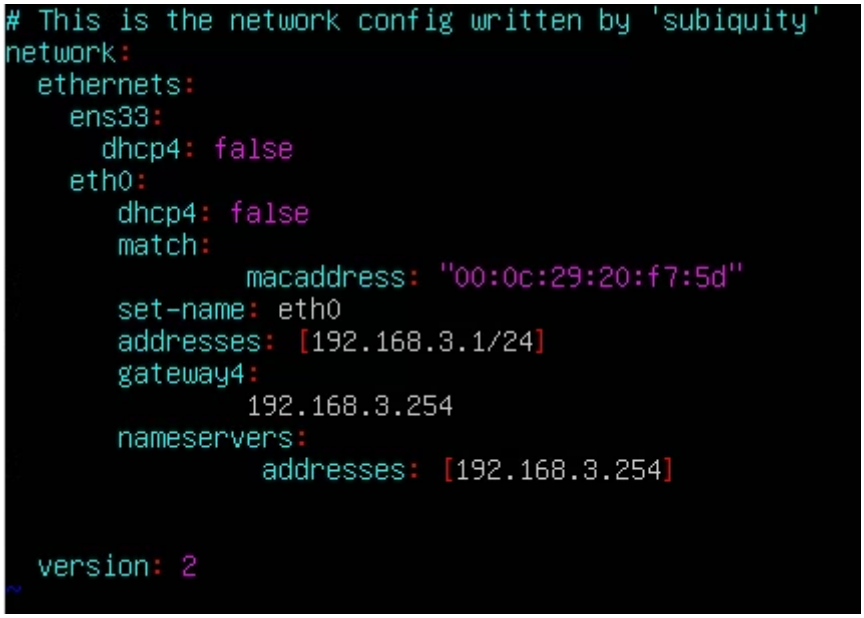
```
sudo service bind9 restart
sudo service bind9 status # 看狀態

```

測試

```
nslookup#查
host www.<id>.nasa
dig www.<id>.nasa
```

srv1

/etc/netplan/00-installer-config.yaml



nginx

```
#in srv vm
sudo apt-get update #Step 1 : 更新 apt-get 套件內容
apt-get install nginx  #Step 2 : 安裝 Nginx
sudo netstat -tlnp | grep nginx #CP連接埠為HTTP預設的80，可以使用以下指令來查看Nginx
sudo systemctl start nginx
sudo systemctl status nginx
```

ref.1 (https://magiclen.org/ubuntu-server-nginx/)

clt

/etc/netplan/00-installer-config.yaml

```
# This is the network config written by 'subiquity'
network:
  ethernets:
    eth0:
      dhcp4: true
      match:
              macaddress: "00:0c:29:55:c0:bc"
      nameservers:
              addresses: [192.168.3.254]
      set-name: eth0
```

測試一下是否可過

```
ping 8.8.8.8
# or
traceroute -I 8.8.8.8
```

測試dns是否成功

```
q56101078@clt:~$ host www.q56101078.nasa
www.q56101078.nasa has address 192.168.3.1
```

ref. (https://magiclen.org/ubuntu-server-dns/)
ref. (https://www.youtube.com/watch?v=oNXEY1zsBaA)

https://www.server-world.info/en/note?os=Ubuntu_19.04&p=dns&f=2 (https://www.server-world.info/en/note?os=Ubuntu_19.04&p=dns&f=2)

https://www.linuxtechi.com/install-configure-bind-9-dns-server-ubuntu-debian/
(https://www.linuxtechi.com/install-configure-bind-9-dns-server-ubuntu-debian/)

問題:

1. nslookup fail
   https://askubuntu.com/questions/1040595/dns-at-systemds-127-0-0-53-is-ignoring-some-lookups (https://askubuntu.com/questions/1040595/dns-at-systemds-127-0-0-53-is-ignoring-some-lookups)

2. wan 不見
   註解 /etc/resolv.conf 裡的東西
   重新跑 `sudo apt-get update`