LFCS- Network

1. Configure Networking, Start/Stop/Check Status of Network Services

2. Packet Filtering

3. Configure SSH Servers and Clients

1. Configure IPv4 and IPv6 networking and hostname resolution

32bit

IPv4 : 192. 168. 1. 101 / 16

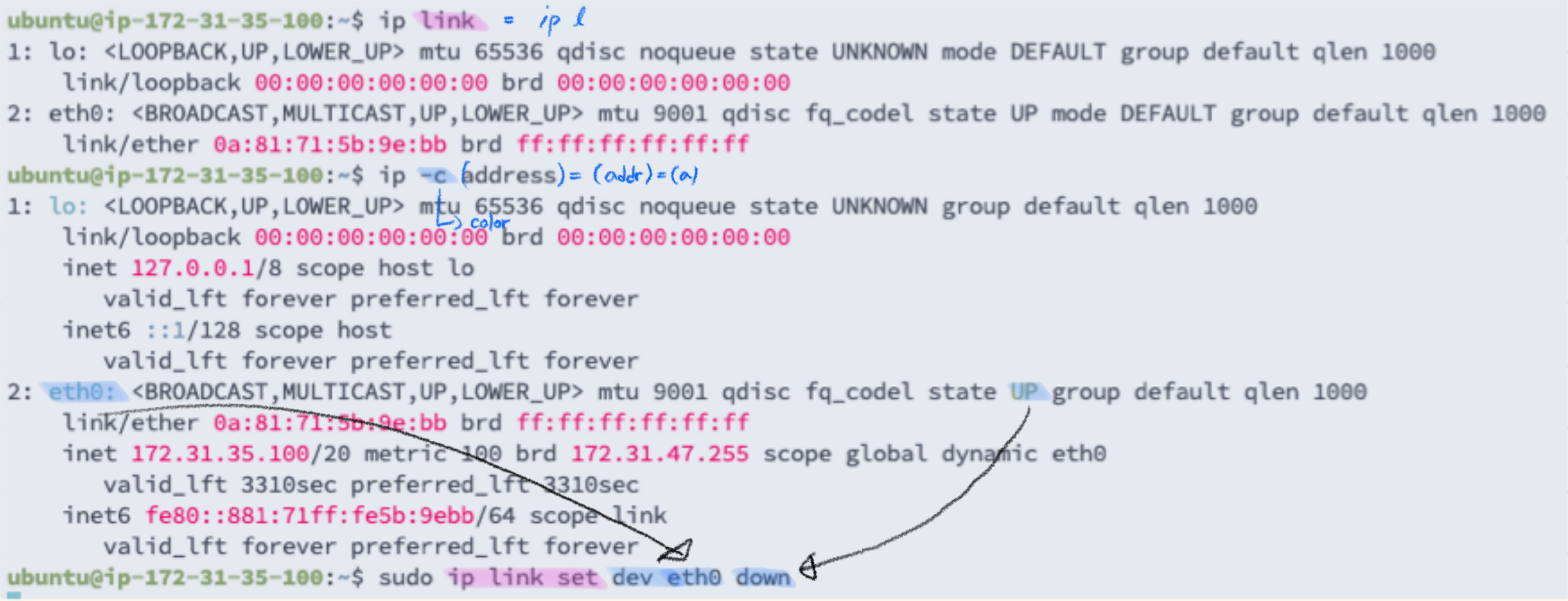
prefix

128bit

연속된 0 축약 가능

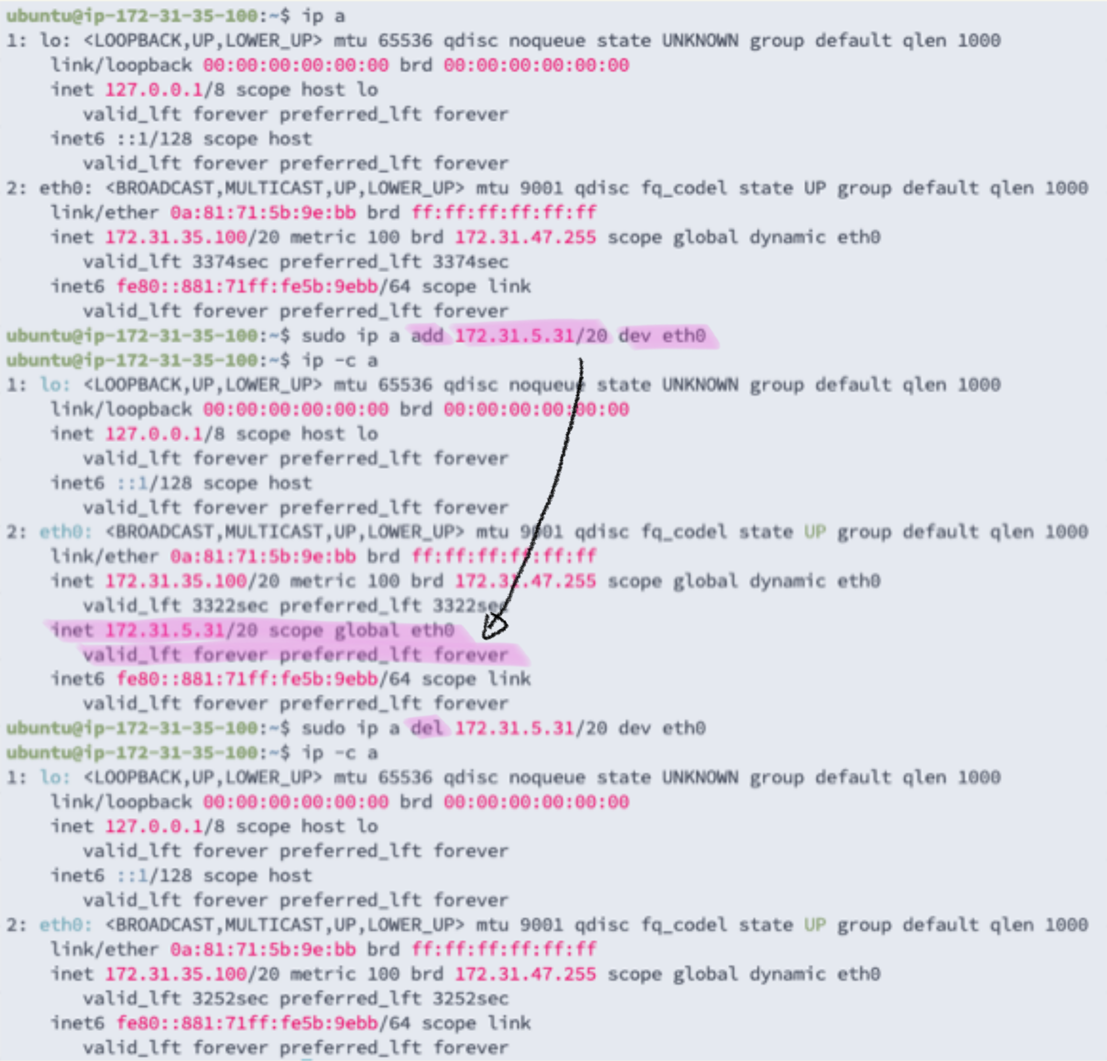
IPv6 : 2001 : 0da8 : 0000 : ··· : 0000 : 00A1 /64

축약 ⇒ 2001 : da8 : : A1 /64



```
ubuntu@ip-172-31-35-100:~$ ip link  = ip l
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN mode DEFAULT group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc fq_codel state UP mode DEFAULT group default qlen 1000
    link/ether 0a:81:71:5b:9e:bb brd ff:ff:ff:ff:ff:ff
ubuntu@ip-172-31-35-100:~$ ip -c (address)=(addr)=(a)
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc fq_codel state UP group default qlen 1000
    link/ether 0a:81:71:5b:9e:bb brd ff:ff:ff:ff:ff:ff
    inet 172.31.35.100/20 metric 100 brd 172.31.47.255 scope global dynamic eth0
       valid_lft 3310sec preferred_lft 3310sec
    inet6 fe80::881:71ff:fe5b:9ebb/64 scope link
       valid_lft forever preferred_lft forever
ubuntu@ip-172-31-35-100:~$ sudo ip link set dev eth0 down
```

↳ ec2에 하면 안됨...
재부팅으로 해결



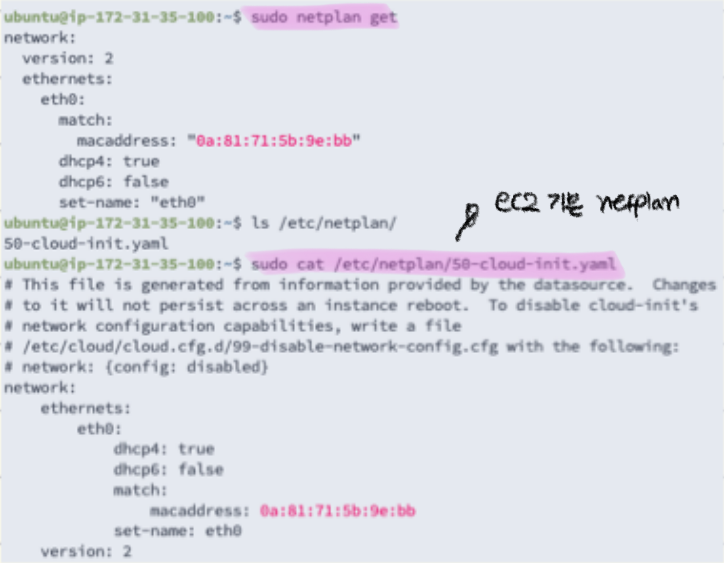
```
ubuntu@ip-172-31-35-100:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc fq_codel state UP group default qlen 1000
    link/ether 0a:81:71:5b:9e:bb brd ff:ff:ff:ff:ff:ff
    inet 172.31.35.100/20 metric 100 brd 172.31.47.255 scope global dynamic eth0
       valid_lft 3374sec preferred_lft 3374sec
    inet6 fe80::881:71ff:fe5b:9ebb/64 scope link
       valid_lft forever preferred_lft forever
ubuntu@ip-172-31-35-100:~$ sudo ip a add 172.31.5.31/20 dev eth0
ubuntu@ip-172-31-35-100:~$ ip -c a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc fq_codel state UP group default qlen 1000
    link/ether 0a:81:71:5b:9e:bb brd ff:ff:ff:ff:ff:ff
    inet 172.31.35.100/20 metric 100 brd 172.31.47.255 scope global dynamic eth0
       valid_lft 3322sec preferred_lft 3322sec
    inet 172.31.5.31/20 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::881:71ff:fe5b:9ebb/64 scope link
       valid_lft forever preferred_lft forever
ubuntu@ip-172-31-35-100:~$ sudo ip a del 172.31.5.31/20 dev eth0
ubuntu@ip-172-31-35-100:~$ ip -c a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc fq_codel state UP group default qlen 1000
    link/ether 0a:81:71:5b:9e:bb brd ff:ff:ff:ff:ff:ff
    inet 172.31.35.100/20 metric 100 brd 172.31.47.255 scope global dynamic eth0
       valid_lft 3252sec preferred_lft 3252sec
    inet6 fe80::881:71ff:fe5b:9ebb/64 scope link
       valid_lft forever preferred_lft forever
```

참고: ip로 설정하면 재부팅시 사라진다.

```
ip a
ip l
ip -c a
ip a add { ip } dev {ni name}
     del
ip r = (route)
```

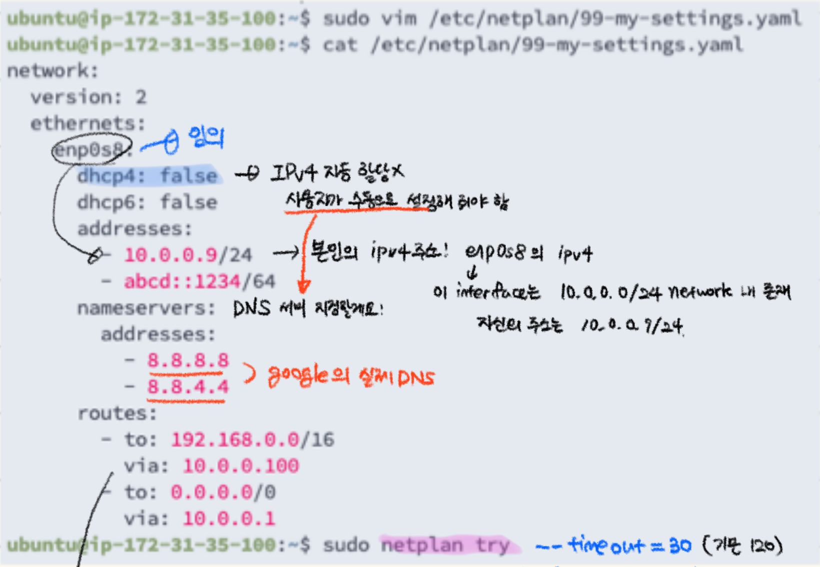
netplan

netplan ? ubuntu's basic network setting manager → not like 'ip', netplan is permanent settings



```
ubuntu@ip-172-31-35-100:~$ sudo netplan get
network:
  version: 2
  ethernets:
    eth0:
      match:
        macaddress: "0a:81:71:5b:9e:bb"
      dhcp4: true
      dhcp6: false
      set-name: "eth0"
ubuntu@ip-172-31-35-100:~$ ls /etc/netplan/
50-cloud-init.yaml
ubuntu@ip-172-31-35-100:~$ sudo cat /etc/netplan/50-cloud-init.yaml
# This file is generated from information provided by the datasource.  Changes
# to it will not persist across an instance reboot.  To disable cloud-init's
# network configuration capabilities, write a file
# /etc/cloud/cloud.cfg.d/99-disable-network-config.cfg with the following:
# network: {config: disabled}
network:
    ethernets:
        eth0:
            dhcp4: true
            dhcp6: false
            match:
                macaddress: 0a:81:71:5b:9e:bb
            set-name: eth0
    version: 2
```

ec2 기본 netplan



```
ubuntu@ip-172-31-35-100:~$ sudo vim /etc/netplan/99-my-settings.yaml
ubuntu@ip-172-31-35-100:~$ cat /etc/netplan/99-my-settings.yaml
network:
  version: 2
  ethernets:
    enp0s8:
      dhcp4: false
      dhcp6: false
      addresses:
        - 10.0.0.9/24
        - abcd::1234/64
      nameservers:
        addresses:
          - 8.8.8.8
          - 8.8.4.4
      routes:
        - to: 192.168.0.0/16
          via: 10.0.0.100
        - to: 0.0.0.0/0
          via: 10.0.0.1
ubuntu@ip-172-31-35-100:~$ sudo netplan try
```

enp0s8 → 임의

dhcp4: false → IPv4 자동 할당X
사용자가 수동으로 설정해 줘야 함

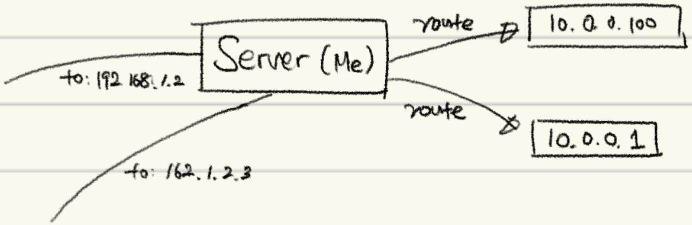
10.0.0.9/24 → 본인의 ipv4주소! enp0s8의 ipv4
↓
이 interface는 10.0.0.0/24 network 내 존재
자신의 주소는 10.0.0.9/24

nameservers: DNS 서버 지정할게요!

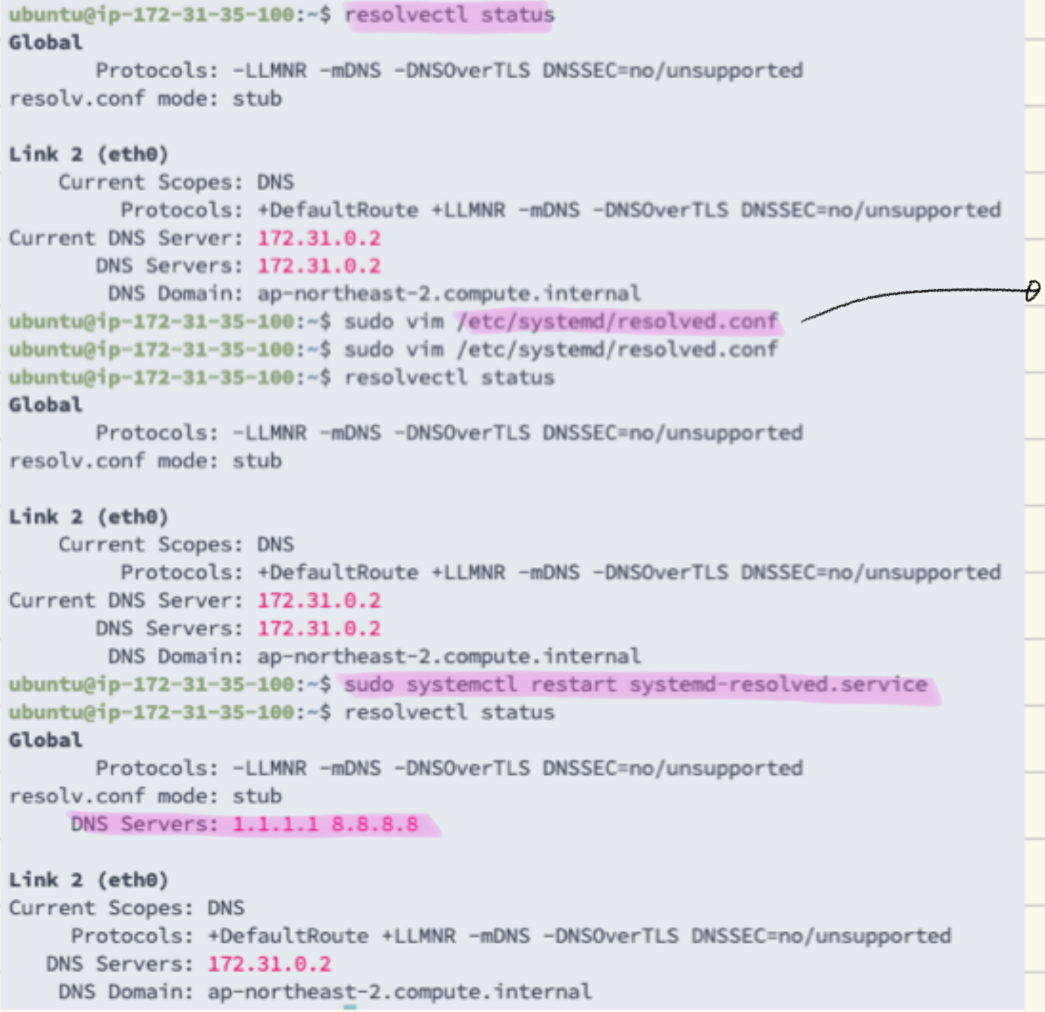
8.8.8.8, 8.8.4.4) google의 실제 DNS

netplan try --timeout=30 (기본 120)

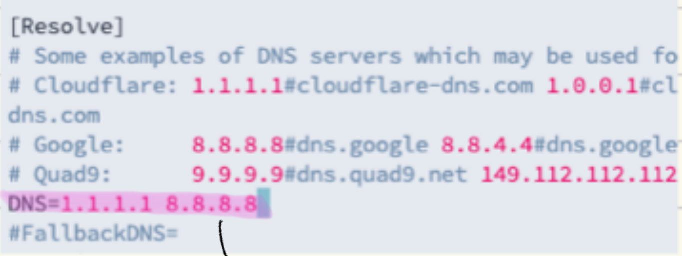
apply (바로적용, 위험)



Global DNS

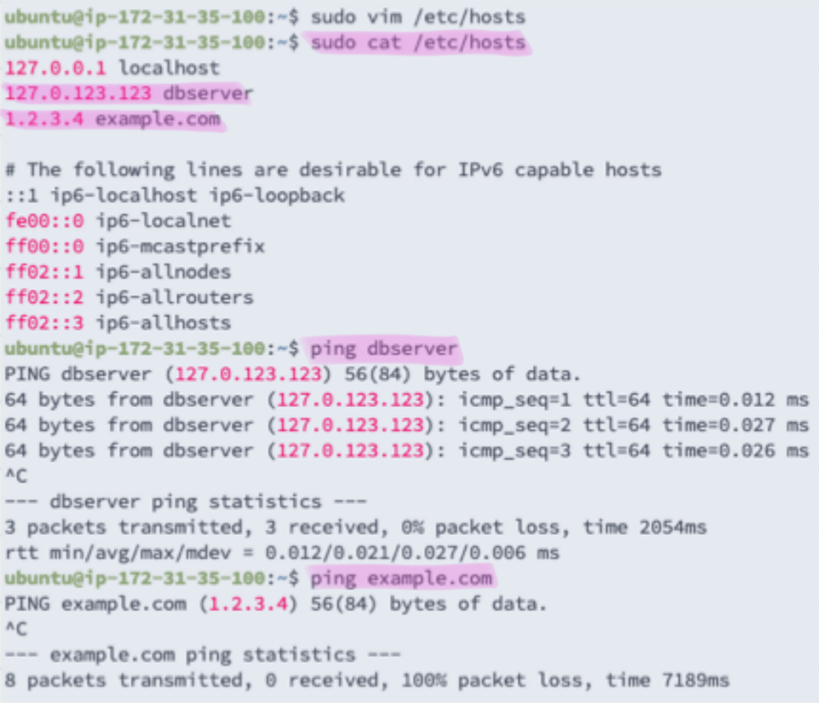


```
ubuntu@ip-172-31-35-100:~$ resolvectl status
Global
       Protocols: -LLMNR -mDNS -DNSOverTLS DNSSEC=no/unsupported
resolv.conf mode: stub

Link 2 (eth0)
    Current Scopes: DNS
         Protocols: +DefaultRoute +LLMNR -mDNS -DNSOverTLS DNSSEC=no/unsupported
Current DNS Server: 172.31.0.2
       DNS Servers: 172.31.0.2
        DNS Domain: ap-northeast-2.compute.internal
ubuntu@ip-172-31-35-100:~$ sudo vim /etc/systemd/resolved.conf
ubuntu@ip-172-31-35-100:~$ sudo vim /etc/systemd/resolved.conf
ubuntu@ip-172-31-35-100:~$ resolvectl status
Global
       Protocols: -LLMNR -mDNS -DNSOverTLS DNSSEC=no/unsupported
resolv.conf mode: stub

Link 2 (eth0)
    Current Scopes: DNS
         Protocols: +DefaultRoute +LLMNR -mDNS -DNSOverTLS DNSSEC=no/unsupported
Current DNS Server: 172.31.0.2
       DNS Servers: 172.31.0.2
        DNS Domain: ap-northeast-2.compute.internal
ubuntu@ip-172-31-35-100:~$ sudo systemctl restart systemd-resolved.service
ubuntu@ip-172-31-35-100:~$ resolvectl status
Global
       Protocols: -LLMNR -mDNS -DNSOverTLS DNSSEC=no/unsupported
resolv.conf mode: stub
     DNS Servers: 1.1.1.1 8.8.8.8

Link 2 (eth0)
Current Scopes: DNS
     Protocols: +DefaultRoute +LLMNR -mDNS -DNSOverTLS DNSSEC=no/unsupported
   DNS Servers: 172.31.0.2
    DNS Domain: ap-northeast-2.compute.internal
```



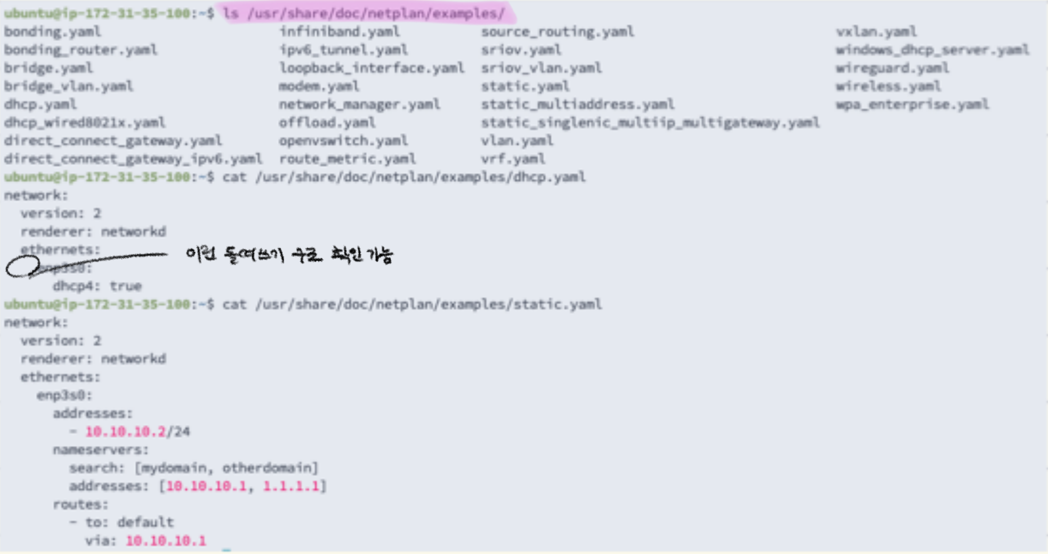
```
[Resolve]
# Some examples of DNS servers which may be used fo
# Cloudflare: 1.1.1.1#cloudflare-dns.com 1.0.0.1#cl
dns.com
# Google:     8.8.8.8#dns.google 8.8.4.4#dns.google
# Quad9:      9.9.9.9#dns.quad9.net 149.112.112.112
DNS=1.1.1.1 8.8.8.8
#FallbackDNS=
```

DNS global setting



```
ubuntu@ip-172-31-35-100:~$ sudo vim /etc/hosts
ubuntu@ip-172-31-35-100:~$ sudo cat /etc/hosts
127.0.0.1 localhost
127.0.123.123 dbserver
1.2.3.4 example.com

# The following lines are desirable for IPv6 capable hosts
::1 ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
ff02::3 ip6-allhosts
ubuntu@ip-172-31-35-100:~$ ping dbserver
PING dbserver (127.0.123.123) 56(84) bytes of data.
64 bytes from dbserver (127.0.123.123): icmp_seq=1 ttl=64 time=0.012 ms
64 bytes from dbserver (127.0.123.123): icmp_seq=2 ttl=64 time=0.027 ms
64 bytes from dbserver (127.0.123.123): icmp_seq=3 ttl=64 time=0.026 ms
^C
--- dbserver ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2054ms
rtt min/avg/max/mdev = 0.012/0.021/0.027/0.006 ms
ubuntu@ip-172-31-35-100:~$ ping example.com
PING example.com (1.2.3.4) 56(84) bytes of data.
^C
--- example.com ping statistics ---
8 packets transmitted, 0 received, 100% packet loss, time 7189ms
```

사용자 초기 파일 구성 예시 !



```
ubuntu@ip-172-31-35-100:~$ ls /usr/share/doc/netplan/examples/
bonding.yaml                       infiniband.yaml            source_routing.yaml                             vxlan.yaml
bonding_router.yaml                ipv6_tunnel.yaml           sriov.yaml                                      windows_dhcp_server.yaml
bridge.yaml                        loopback_interface.yaml    sriov_vlan.yaml                                 wireguard.yaml
bridge_vlan.yaml                   modem.yaml                 static.yaml                                     wireless.yaml
dhcp.yaml                          network_manager.yaml       static_multiaddress.yaml                        wpa_enterprise.yaml
dhcp_wired8021x.yaml               offload.yaml               static_singlenic_multiip_multigateway.yaml
direct_connect_gateway.yaml        openvswitch.yaml           vlan.yaml
direct_connect_gateway_ipv6.yaml   route_metric.yaml          vrf.yaml
ubuntu@ip-172-31-35-100:~$ cat /usr/share/doc/netplan/examples/dhcp.yaml
network:
  version: 2
  renderer: networkd
  ethernets:
    enp3s0:
      dhcp4: true
ubuntu@ip-172-31-35-100:~$ cat /usr/share/doc/netplan/examples/static.yaml
network:
  version: 2
  renderer: networkd
  ethernets:
    enp3s0:
      addresses:
        - 10.10.10.2/24
      nameservers:
        search: [mydomain, otherdomain]
        addresses: [10.10.10.1, 1.1.1.1]
      routes:
        - to: default
          via: 10.10.10.1
```

이런 들여쓰기 구조 확인 가능

sudo ss -ltunp

number

process (sudo)

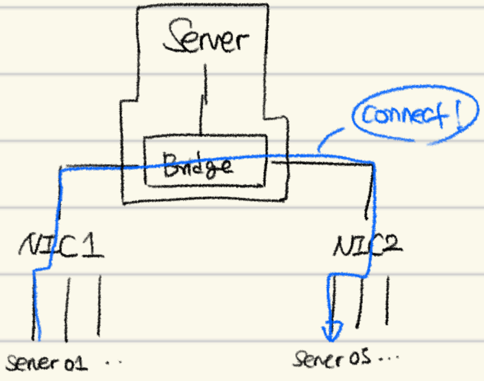
listen

tcp. udp

2. Packet Filtering (LAB2)

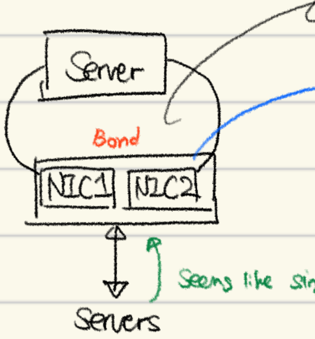
1. Configure Bridge and Bonding Devices

Bridge



glue two or more networks

Bond



Seems like single NIC

1. fault tolerance
2. high throughput
3. Reliability

two or more connections to a network

Bonding modes, 0 to 6

0 : round-robin ▨ ▨

1 : Active Backup ▨ □

2 : XOR

3 : Broadcast

only

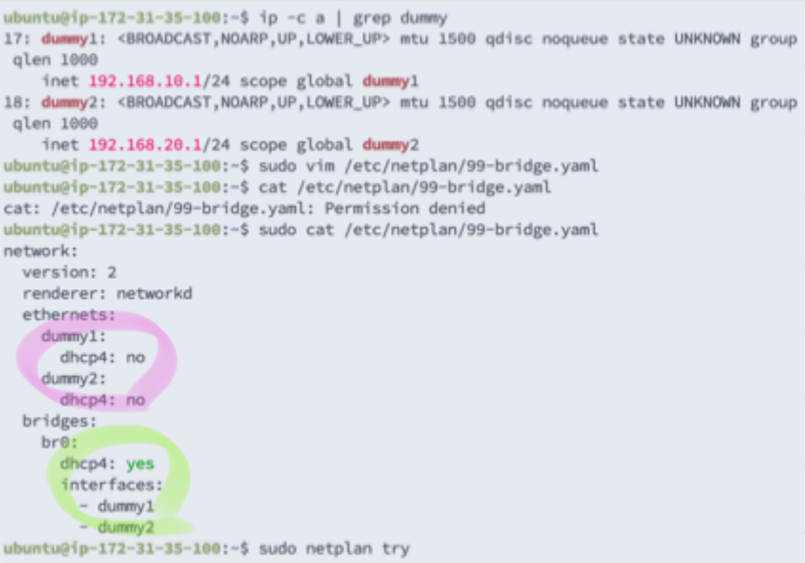
4 : IEEE 802.3ad / LACP (실제 network throughput ↑)

5 : ATLB

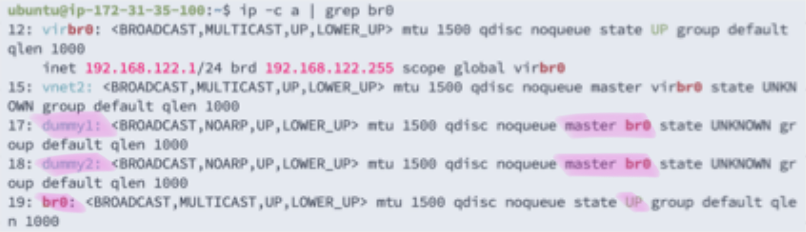
6 : ALB

2. Demo. – Bridge & Bond

Bridge

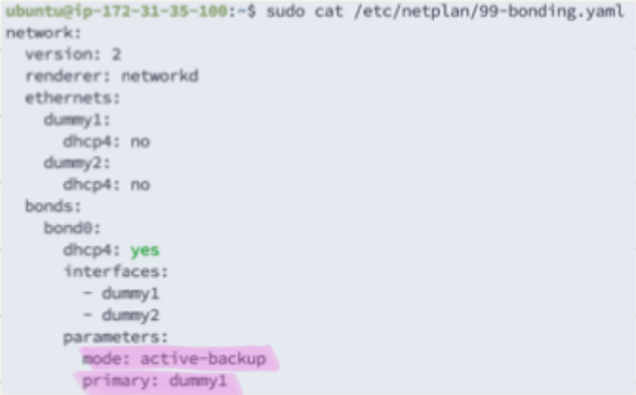


```
ubuntu@ip-172-31-35-100:~$ ip -c a | grep dummy
17: dummy1: <BROADCAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc noqueue state UNKNOWN group
 qlen 1000
    inet 192.168.10.1/24 scope global dummy1
18: dummy2: <BROADCAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc noqueue state UNKNOWN group
 qlen 1000
    inet 192.168.20.1/24 scope global dummy2
ubuntu@ip-172-31-35-100:~$ sudo vim /etc/netplan/99-bridge.yaml
ubuntu@ip-172-31-35-100:~$ cat /etc/netplan/99-bridge.yaml
cat: /etc/netplan/99-bridge.yaml: Permission denied
ubuntu@ip-172-31-35-100:~$ sudo cat /etc/netplan/99-bridge.yaml
network:
  version: 2
  renderer: networkd
  ethernets:
    dummy1:
      dhcp4: no
    dummy2:
      dhcp4: no
  bridges:
    br0:
      dhcp4: yes
      interfaces:
        - dummy1
        - dummy2
ubuntu@ip-172-31-35-100:~$ sudo netplan try
```

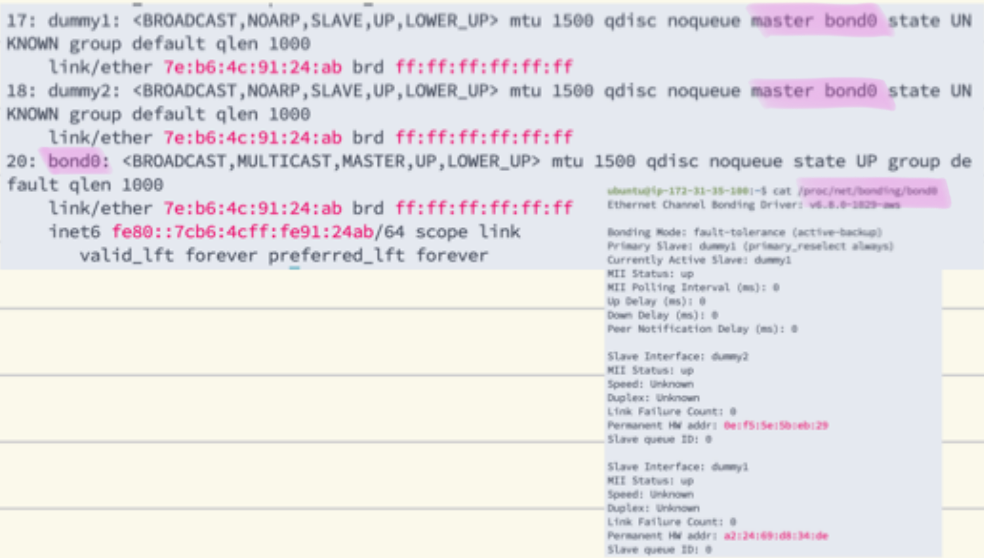


```
ubuntu@ip-172-31-35-100:~$ ip -c a | grep br0
12: virbr0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
qlen 1000
    inet 192.168.122.1/24 brd 192.168.122.255 scope global virbr0
15: vnet2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue master virbr0 state UNKN
OWN group default qlen 1000
17: dummy1: <BROADCAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc noqueue master br0 state UNKNOWN gr
oup default qlen 1000
18: dummy2: <BROADCAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc noqueue master br0 state UNKNOWN gr
oup default qlen 1000
19: br0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qle
n 1000
```

Bond



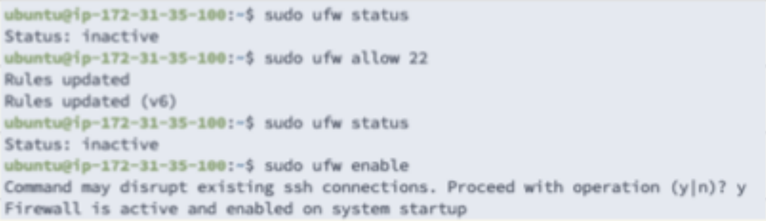
```
ubuntu@ip-172-31-35-100:~$ sudo cat /etc/netplan/99-bonding.yaml
network:
  version: 2
  renderer: networkd
  ethernets:
    dummy1:
      dhcp4: no
    dummy2:
      dhcp4: no
  bonds:
    bond0:
      dhcp4: yes
      interfaces:
        - dummy1
        - dummy2
      parameters:
        mode: active-backup
        primary: dummy1
```



```
17: dummy1: <BROADCAST,NOARP,SLAVE,UP,LOWER_UP> mtu 1500 qdisc noqueue master bond0 state UN
KNOWN group default qlen 1000
    link/ether 7e:b6:4c:91:24:ab brd ff:ff:ff:ff:ff:ff
18: dummy2: <BROADCAST,NOARP,SLAVE,UP,LOWER_UP> mtu 1500 qdisc noqueue master bond0 state UN
KNOWN group default qlen 1000
    link/ether 7e:b6:4c:91:24:ab brd ff:ff:ff:ff:ff:ff
20: bond0: <BROADCAST,MULTICAST,MASTER,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group de
fault qlen 1000
    link/ether 7e:b6:4c:91:24:ab brd ff:ff:ff:ff:ff:ff
    inet6 fe80::7cb6:4cff:fe91:24ab/64 scope link
       valid_lft forever preferred_lft forever
```

```
ubuntu@ip-172-31-35-100:~$ cat /proc/net/bonding/bond0
Ethernet Channel Bonding Driver: v6.8.0-1029-aws

Bonding Mode: fault-tolerance (active-backup)
Primary Slave: dummy1 (primary_reselect always)
Currently Active Slave: dummy1
MII Status: up
MII Polling Interval (ms): 0
Up Delay (ms): 0
Down Delay (ms): 0
Peer Notification Delay (ms): 0

Slave Interface: dummy2
MII Status: up
Speed: Unknown
Duplex: Unknown
Link Failure Count: 0
Permanent HW addr: 0e:f5:5e:5b:eb:29
Slave queue ID: 0

Slave Interface: dummy1
MII Status: up
Speed: Unknown
Duplex: Unknown
Link Failure Count: 0
Permanent HW addr: a2:24:69:d8:34:de
Slave queue ID: 0
```

3. Packet Filtering

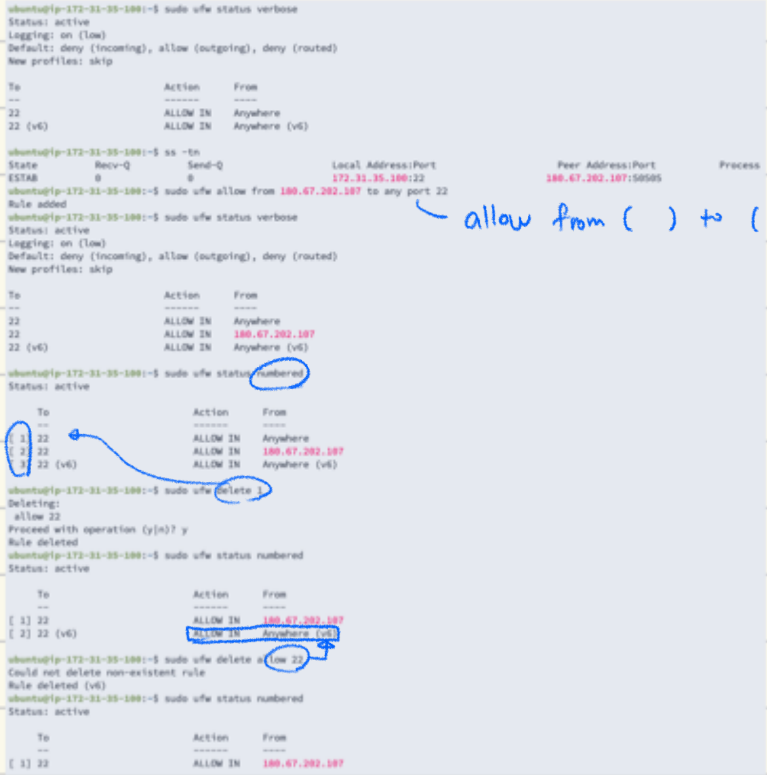


```
ubuntu@ip-172-31-35-100:~$ sudo ufw status
Status: inactive
ubuntu@ip-172-31-35-100:~$ sudo ufw allow 22
Rules updated
Rules updated (v6)
ubuntu@ip-172-31-35-100:~$ sudo ufw status
Status: inactive
ubuntu@ip-172-31-35-100:~$ sudo ufw enable
Command may disrupt existing ssh connections. Proceed with operation (y|n)? y
Firewall is active and enabled on system startup
```

Status

allow 22

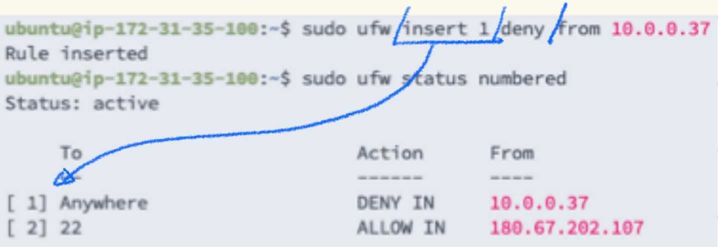
enable



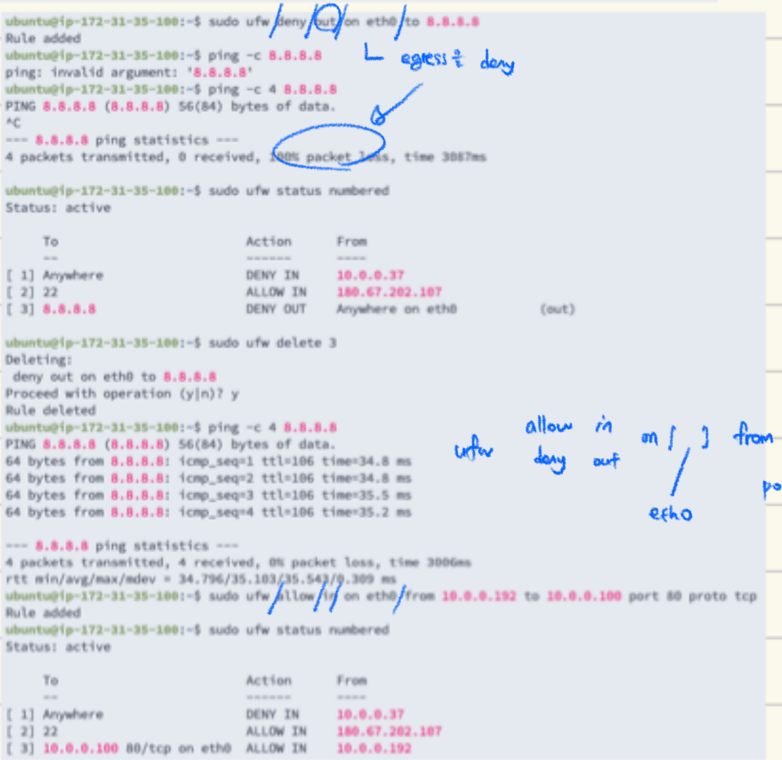
```
ubuntu@ip-172-31-35-100:~$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), deny (routed)
New profiles: skip

To                         Action      From
--                         ------      ----
22                         ALLOW IN    Anywhere
22 (v6)                    ALLOW IN    Anywhere (v6)

ubuntu@ip-172-31-35-100:~$ ss -tn
State      Recv-Q      Send-Q           Local Address:Port          Peer Address:Port       Process
ESTAB      0           0                172.31.35.100:22            180.67.202.107:50505
ubuntu@ip-172-31-35-100:~$ sudo ufw allow from 180.67.202.107 to any port 22
Rule added
ubuntu@ip-172-31-35-100:~$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), deny (routed)
New profiles: skip

To                         Action      From
--                         ------      ----
22                         ALLOW IN    Anywhere
22                         ALLOW IN    180.67.202.107
22 (v6)                    ALLOW IN    Anywhere (v6)

ubuntu@ip-172-31-35-100:~$ sudo ufw status numbered
Status: active

     To                         Action      From
     --                         ------      ----
[ 1] 22                         ALLOW IN    Anywhere
[ 2] 22                         ALLOW IN    180.67.202.107
[ 3] 22 (v6)                    ALLOW IN    Anywhere (v6)

ubuntu@ip-172-31-35-100:~$ sudo ufw delete 1
Deleting:
 allow 22
Proceed with operation (y|n)? y
Rule deleted
ubuntu@ip-172-31-35-100:~$ sudo ufw status numbered
Status: active

     To                         Action      From
     --                         ------      ----
[ 1] 22                         ALLOW IN    180.67.202.107
[ 2] 22 (v6)                    ALLOW IN    Anywhere (v6)

ubuntu@ip-172-31-35-100:~$ sudo ufw delete allow 22
Could not delete non-existent rule
Rule deleted (v6)
ubuntu@ip-172-31-35-100:~$ sudo ufw status numbered
Status: active

     To                         Action      From
     --                         ------      ----
[ 1] 22                         ALLOW IN    180.67.202.107
```

status verbose

allow from ( ) to ( ) port ( )



```
ubuntu@ip-172-31-35-100:~$ sudo ufw insert 1 deny from 10.0.0.37
Rule inserted
ubuntu@ip-172-31-35-100:~$ sudo ufw status numbered
Status: active

     To                         Action      From
     --                         ------      ----
[ 1] Anywhere                   DENY IN     10.0.0.37
[ 2] 22                         ALLOW IN    180.67.202.107
```



```
ubuntu@ip-172-31-35-100:~$ sudo ufw deny out on eth0 to 8.8.8.8
Rule added
ubuntu@ip-172-31-35-100:~$ ping -c 8.8.8.8
ping: invalid argument: '8.8.8.8'
ubuntu@ip-172-31-35-100:~$ ping -c 4 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
^C
--- 8.8.8.8 ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time 3087ms

ubuntu@ip-172-31-35-100:~$ sudo ufw status numbered
Status: active

     To                         Action      From
     --                         ------      ----
[ 1] Anywhere                   DENY IN     10.0.0.37
[ 2] 22                         ALLOW IN    180.67.202.107
[ 3] 8.8.8.8                    DENY OUT    Anywhere on eth0           (out)

ubuntu@ip-172-31-35-100:~$ sudo ufw delete 3
Deleting:
 deny out on eth0 to 8.8.8.8
Proceed with operation (y|n)? y
Rule deleted
ubuntu@ip-172-31-35-100:~$ ping -c 4 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=106 time=34.8 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=106 time=34.8 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=106 time=35.5 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=106 time=35.2 ms

--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
rtt min/avg/max/mdev = 34.796/35.103/35.543/0.309 ms
ubuntu@ip-172-31-35-100:~$ sudo ufw allow in on eth0 from 10.0.0.192 to 10.0.0.100 port 80 proto tcp
Rule added
ubuntu@ip-172-31-35-100:~$ sudo ufw status numbered
Status: active

     To                         Action      From
     --                         ------      ----
[ 1] Anywhere                   DENY IN     10.0.0.37
[ 2] 22                         ALLOW IN    180.67.202.107
[ 3] 10.0.0.100 80/tcp on eth0  ALLOW IN    10.0.0.192
```

L egress은 deny

ufw allow in on [ ] from [ ] to [ ]
deny out
etho
port( ) proto ( )
22 tcp