

WEB 3 Tier - 실습가이드

최초 작성일 : 2024/01/26

최종 제출일 : 2024/01/29

김민경

내용

I. 실습	2
1. DHCP 서버 설치하기	2
III. 과제	12
1. 문제 1번	12
2. 문제 2번	14

I. 실습

1. DHCP 서버 설치하기

1) WEB(U-D1)에 DHCP 설치하기

- 패키지 upgrade 하기

sudo apt-get upgrade

- DHCP 서버 설치하기

```
kim@kim-VirtualBox:~$ sudo apt-get install isc-dhcp-server
```

```
kim@kim-VirtualBox:~$ sudo apt-get install bind9
```

참고) bind9

DNS 네임 서버를 구축하고 레코드를 관리할 수 있도록 도와주는 패키지

2) WEB에 설치한 DHCP 설정하기

- 현재 window10과 U-D1(WEB)는 서로 다른 네트워크 대역에 있음
⇒ Relay Agent를 사용해야 함
- DHCP 활성화 확인하기 ⇒ 실패

```

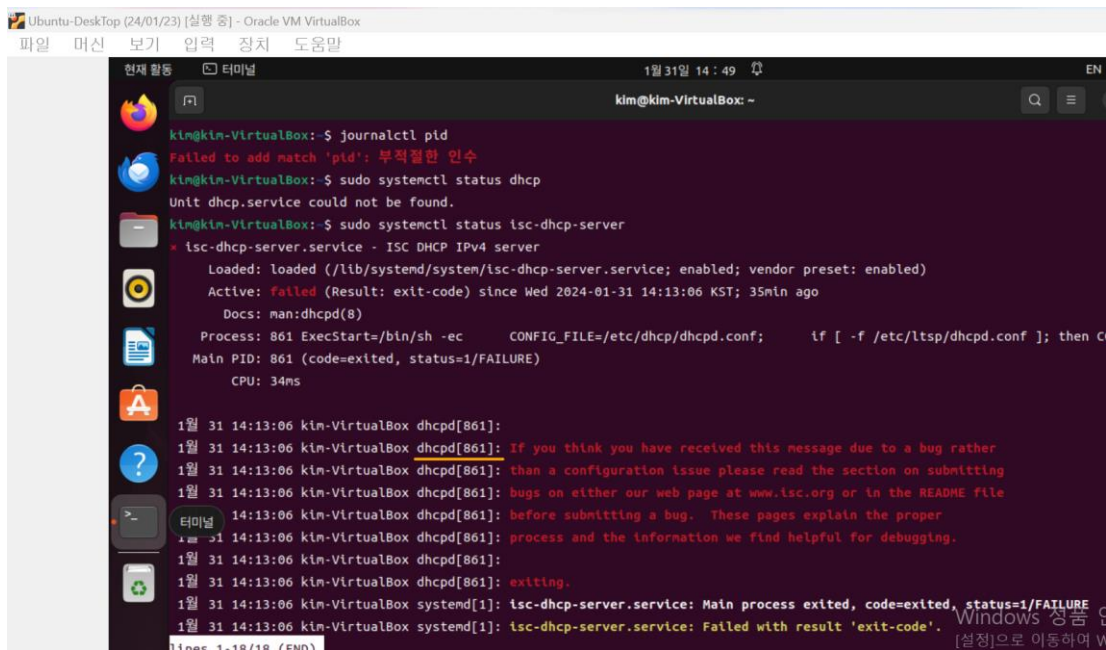
kim@kim-VirtualBox:~$ sudo systemctl status isc-dhcp-server
* isc-dhcp-server.service - ISC DHCP IPv4 server
   Loaded: loaded (/lib/systemd/system/isc-dhcp-server.service; enabled; vendor preset: enabled)
   Active: failed (Result: exit-code) since Wed 2024-01-31 14:13:06 KST; 24min ago
     Docs: man:dhcpd(8)
  Process: 861 ExecStart=/bin/sh -ec CONFIG_FILE=/etc/dhcp/dhcpd.conf; if [ -f /etc/ltsp/dhcpd.conf ]; then C
 Main PID: 861 (code=exited, status=1/FAILURE)
    CPU: 34ms

1월 31 14:13:06 kim-VirtualBox dhcpd[861]:
1월 31 14:13:06 kim-VirtualBox dhcpd[861]: If you think you have received this message due to a bug rather
1월 31 14:13:06 kim-VirtualBox dhcpd[861]: than a configuration issue please read the section on submitting
1월 31 14:13:06 kim-VirtualBox dhcpd[861]: bugs on either our web page at www.isc.org or in the README file
1월 31 14:13:06 kim-VirtualBox dhcpd[861]: before submitting a bug. These pages explain the proper
1월 31 14:13:06 kim-VirtualBox dhcpd[861]: process and the information we find helpful for debugging.
1월 31 14:13:06 kim-VirtualBox dhcpd[861]:
1월 31 14:13:06 kim-VirtualBox dhcpd[861]: exiting.
1월 31 14:13:06 kim-VirtualBox systemd[1]: isc-dhcp-server.service: Main process exited, code=exited, status=1/FAILURE
1월 31 14:13:06 kim-VirtualBox systemd[1]: isc-dhcp-server.service: Failed with result 'exit-code'.
lines 1-18/18 (END)

```

- journalctl로 오류 확인 및 수정하기

- 오류 확인하기

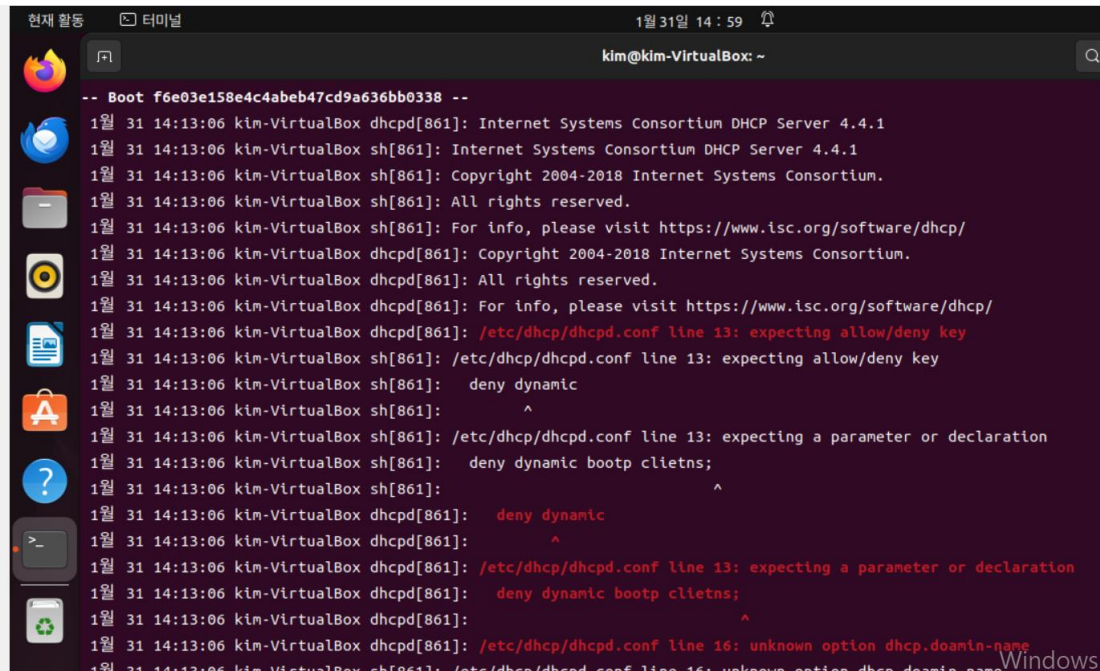


journalctl _PID={오류 번호 이름}

```

kim@kim-VirtualBox:~$ sudo journalctl _PID=861
12월 27 10:47:06 kim-VirtualBox dbus-daemon[861]: [session uid=1000]

```




The screenshot shows a terminal window titled 'kim@kim-VirtualBox: ~' with a search icon on the right. The terminal displays a series of log messages from the DHCP server. The messages include the server version (4.4.1), copyright information (2004-2018), and several error messages related to the configuration file `/etc/dhcp/dhcpd.conf`. The errors are: 'expecting allow/deny key' on line 13, 'expecting a parameter or declaration' on line 13, and 'unknown option dhcp.doamin-name' on line 16. The terminal also shows the command `deny dynamic` being entered. The left sidebar of the virtual machine interface is visible, showing various application icons. The top status bar indicates '현재 활동' (Currently Active) and the time '1월 31일 14:59'.

```
-- Boot f6e03e158e4c4abeb47cd9a636bb0338 --
1월 31 14:13:06 kim-VirtualBox dhcpd[861]: Internet Systems Consortium DHCP Server 4.4.1
1월 31 14:13:06 kim-VirtualBox sh[861]: Internet Systems Consortium DHCP Server 4.4.1
1월 31 14:13:06 kim-VirtualBox sh[861]: Copyright 2004-2018 Internet Systems Consortium.
1월 31 14:13:06 kim-VirtualBox sh[861]: All rights reserved.
1월 31 14:13:06 kim-VirtualBox sh[861]: For info, please visit https://www.isc.org/software/dhcp/
1월 31 14:13:06 kim-VirtualBox dhcpd[861]: Copyright 2004-2018 Internet Systems Consortium.
1월 31 14:13:06 kim-VirtualBox dhcpd[861]: All rights reserved.
1월 31 14:13:06 kim-VirtualBox dhcpd[861]: For info, please visit https://www.isc.org/software/dhcp/
1월 31 14:13:06 kim-VirtualBox dhcpd[861]: /etc/dhcp/dhcpd.conf line 13: expecting allow/deny key
1월 31 14:13:06 kim-VirtualBox sh[861]: /etc/dhcp/dhcpd.conf line 13: expecting allow/deny key
1월 31 14:13:06 kim-VirtualBox sh[861]: deny dynamic
1월 31 14:13:06 kim-VirtualBox sh[861]: ^
1월 31 14:13:06 kim-VirtualBox sh[861]: /etc/dhcp/dhcpd.conf line 13: expecting a parameter or declaration
1월 31 14:13:06 kim-VirtualBox sh[861]: deny dynamic bootp clietns;
1월 31 14:13:06 kim-VirtualBox sh[861]: ^
1월 31 14:13:06 kim-VirtualBox dhcpd[861]: deny dynamic
1월 31 14:13:06 kim-VirtualBox dhcpd[861]: ^
1월 31 14:13:06 kim-VirtualBox dhcpd[861]: /etc/dhcp/dhcpd.conf line 13: expecting a parameter or declaration
1월 31 14:13:06 kim-VirtualBox dhcpd[861]: deny dynamic bootp clietns;
1월 31 14:13:06 kim-VirtualBox dhcpd[861]: ^
1월 31 14:13:06 kim-VirtualBox dhcpd[861]: /etc/dhcp/dhcpd.conf line 16: unknown option dhcp.doamin-name
1월 31 14:13:06 kim-VirtualBox sh[861]: /etc/dhcp/dhcpd.conf line 16: unknown option dhcp.doamin-name
```

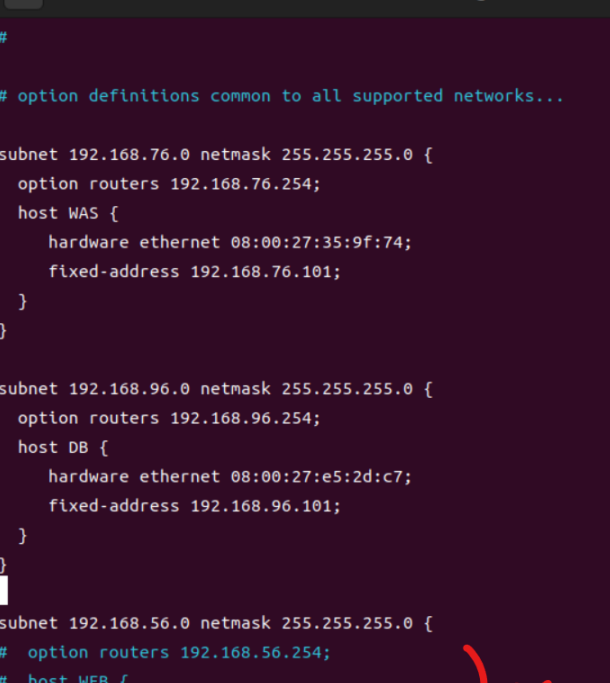
- 오류 수정하기

⇒ `/etc/dhcp/dhpd.conf` 파일에 문제가 있는 듯함

DHCP 서버 설정 파일

 (WEB)Ubuntu-DeskTop (24/01/23) [실행 중] - Oracle VM VirtualBox

파일 머신 보기 입력 장치 도움말



현재 활동 터미널 2월 1일 01

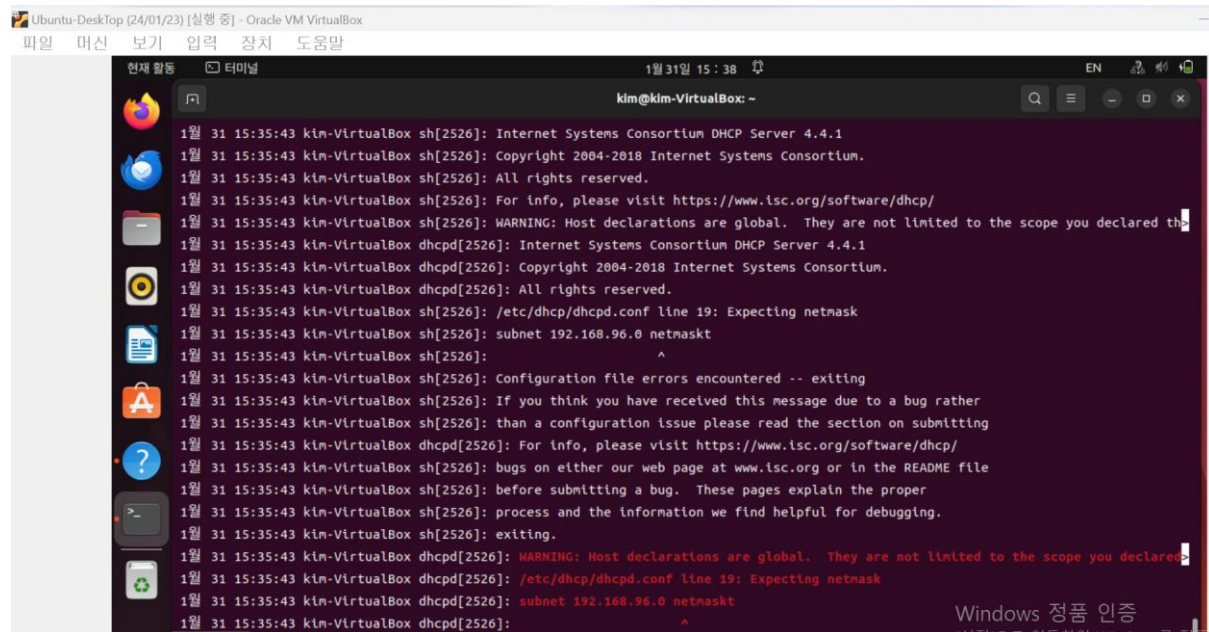
kim@kim-VirtualBox: ~

```
#  
# option definitions common to all supported networks...  
  
subnet 192.168.76.0 netmask 255.255.255.0 {  
    option routers 192.168.76.254;  
    host WAS {  
        hardware ethernet 08:00:27:35:9f:74;  
        fixed-address 192.168.76.101;  
    }  
}  
  
subnet 192.168.96.0 netmask 255.255.255.0 {  
    option routers 192.168.96.254;  
    host DB {  
        hardware ethernet 08:00:27:e5:2d:c7;  
        fixed-address 192.168.96.101;  
    }  
}  
  
subnet 192.168.56.0 netmask 255.255.255.0 {  
# option routers 192.168.56.254;  
# host WEB {  
#     hardware ethernet 08:00:27:63:ff:0b;  
#     fixed-address 192.168.56.101;  
# }
```

⇒ 자기 자신의 주소도 넣어줘야 함

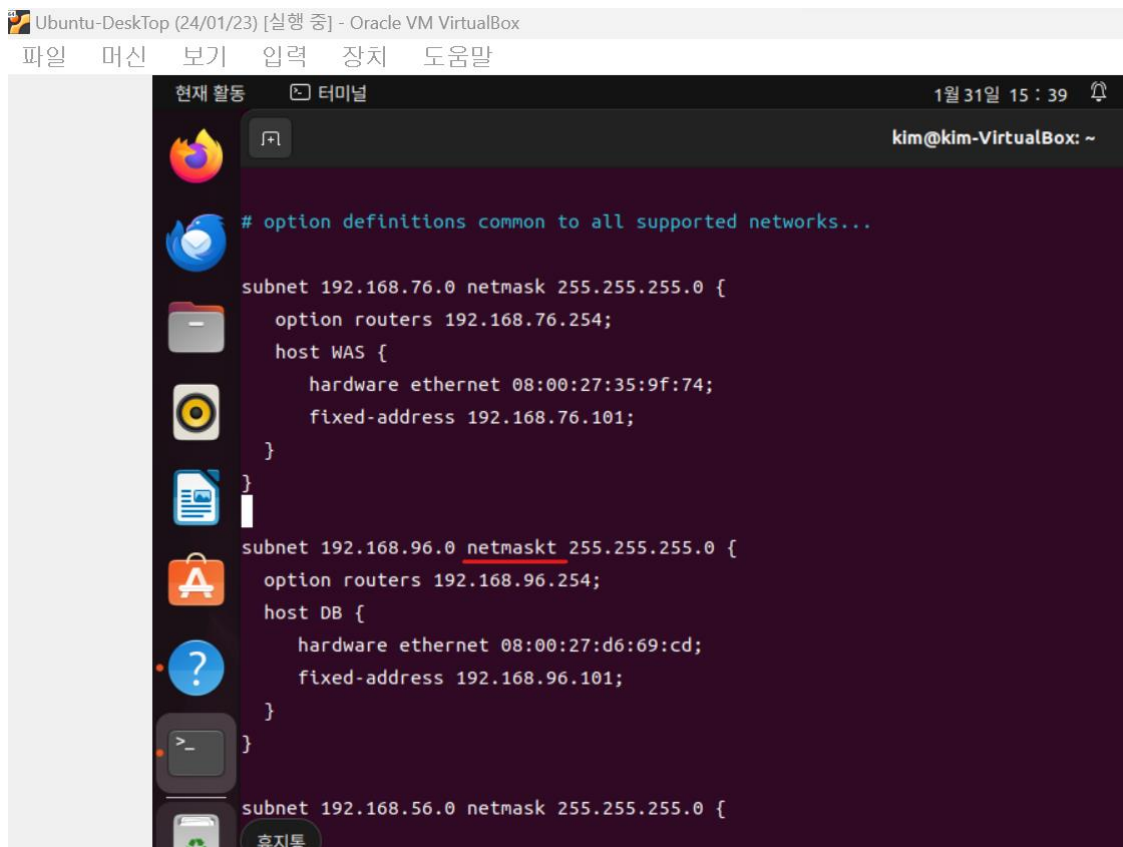
- DHCP 활성화 확인하기 ⇒ 또 실패

journalctl _PID={2526}



```
1월 31 15:35:43 kin-VirtualBox sh[2526]: Internet Systems Consortium DHCP Server 4.4.1
1월 31 15:35:43 kin-VirtualBox sh[2526]: Copyright 2004-2018 Internet Systems Consortium.
1월 31 15:35:43 kin-VirtualBox sh[2526]: All rights reserved.
1월 31 15:35:43 kin-VirtualBox sh[2526]: For info, please visit https://www.isc.org/software/dhcp/
1월 31 15:35:43 kin-VirtualBox sh[2526]: WARNING: Host declarations are global. They are not limited to the scope you declared the
1월 31 15:35:43 kin-VirtualBox dhcpd[2526]: Internet Systems Consortium DHCP Server 4.4.1
1월 31 15:35:43 kin-VirtualBox dhcpd[2526]: Copyright 2004-2018 Internet Systems Consortium.
1월 31 15:35:43 kin-VirtualBox dhcpd[2526]: All rights reserved.
1월 31 15:35:43 kin-VirtualBox sh[2526]: /etc/dhcp/dhcpd.conf line 19: Expecting netmask
1월 31 15:35:43 kin-VirtualBox sh[2526]: subnet 192.168.96.0 netmaskt
1월 31 15:35:43 kin-VirtualBox sh[2526]: ^
1월 31 15:35:43 kin-VirtualBox sh[2526]: Configuration file errors encountered -- exiting
1월 31 15:35:43 kin-VirtualBox sh[2526]: If you think you have received this message due to a bug rather
1월 31 15:35:43 kin-VirtualBox sh[2526]: than a configuration issue please read the section on submitting
1월 31 15:35:43 kin-VirtualBox dhcpd[2526]: For info, please visit https://www.isc.org/software/dhcp/
1월 31 15:35:43 kin-VirtualBox sh[2526]: bugs on either our web page at www.isc.org or in the README file
1월 31 15:35:43 kin-VirtualBox sh[2526]: before submitting a bug. These pages explain the proper
1월 31 15:35:43 kin-VirtualBox sh[2526]: process and the information we find helpful for debugging.
1월 31 15:35:43 kin-VirtualBox sh[2526]: exiting.
1월 31 15:35:43 kin-VirtualBox dhcpd[2526]: WARNING: Host declarations are global. They are not limited to the scope you declare
1월 31 15:35:43 kin-VirtualBox dhcpd[2526]: /etc/dhcp/dhcpd.conf line 19: Expecting netmask
1월 31 15:35:43 kin-VirtualBox dhcpd[2526]: subnet 192.168.96.0 netmaskt
1월 31 15:35:43 kin-VirtualBox dhcpd[2526]: ^
```

- /etc/dhcp/dhcpd.conf 파일에서 오류 수정



```
# option definitions common to all supported networks...

subnet 192.168.76.0 netmask 255.255.255.0 {
    option routers 192.168.76.254;
    host WAS {
        hardware ethernet 08:00:27:35:9f:74;
        fixed-address 192.168.76.101;
    }
}

subnet 192.168.96.0 netmaskt 255.255.255.0 {
    option routers 192.168.96.254;
    host DB {
        hardware ethernet 08:00:27:d6:69:cd;
        fixed-address 192.168.96.101;
    }
}

subnet 192.168.56.0 netmask 255.255.255.0 {
```

- DHCP 활성화 확인하기 ⇒ 성공

```

Ubuntu-Desktop (24/01/23) [실행 중] - Oracle VM VirtualBox
파일  머신  보기  입력  장치  도움말

현재 활동  터미널  1월 31일 15:39

kim@kim-VirtualBox: ~
kim@kim-VirtualBox:~$ sudo systemctl restart isc-dhcp-server
kim@kim-VirtualBox:~$ sudo systemctl status isc-dhcp-server
●isc-dhcp-server.service - ISC DHCP IPv4 server
   Loaded: loaded (/lib/systemd/system/isc-dhcp-server.service; enabled; vendor preset: enabled)
   Active: active (running) since Wed 2024-01-31 15:39:45 KST; 4s ago
     Docs: man:dhcpd(8)
    Main PID: 2555 (dhcpd)
       Tasks: 4 (limit: 2260)
      Memory: 2.5M
         CPU: 15ms
    CGroup: /system.slice/isc-dhcp-server.service
            └─2555 dhcpd -user dhcpd -group dhcpd -f -4 -pf /run/dhcp-server/dhcpd.pid -cf /etc/dhcp/dhcpd.conf

1월 31 15:39:45 kim-VirtualBox dhcpd[2555]: in your dhcpd.conf file for the network segment
1월 31 15:39:45 kim-VirtualBox dhcpd[2555]: to which interface enp0s8 is attached. **
1월 31 15:39:45 kim-VirtualBox dhcpd[2555]:
1월 31 15:39:45 kim-VirtualBox dhcpd[2555]: Listening on LPF/enp0s3/08:00:27:63:ff:0b/192.168.56.0/24
1월 31 15:39:45 kim-VirtualBox sh[2555]: Listening on LPF/enp0s3/08:00:27:63:ff:0b/192.168.56.0/24
1월 31 15:39:45 kim-VirtualBox sh[2555]: Sending on LPF/enp0s3/08:00:27:63:ff:0b/192.168.56.0/24
1월 31 15:39:45 kim-VirtualBox sh[2555]: Sending on Socket/fallback/fallback-net
1월 31 15:39:45 kim-VirtualBox dhcpd[2555]: Sending on LPF/enp0s3/08:00:27:63:ff:0b/192.168.56.0/24
1월 31 15:39:45 kim-VirtualBox dhcpd[2555]: Sending on Socket/fallback/fallback-net
1월 31 15:39:45 kim-VirtualBox dhcpd[2555]: Server starting service.
  
```

3) U-S2(라우터)에 DHCP 릴레이 에이전트 설치하기

- `sudo apt-get install isc-dhcp-relay`
- DHCP RELAY 설정하기

```
ubuntu@ubuntu:~$ sudo vim /etc/default/isc-dhcp-relay_
```

- Forward 할 DHCP 주소 & DHCP request를 전달할 인터페이스(dhcp 서버와 연결된 곳) 설정하기

```

Ubuntu-Server1 복제(router) (스냅샷 1/25) [실행 중] - Oracle VM VirtualBox
파일  머신  보기  입력  장치  도움말

# Defaults for isc-dhcp-relay initscript
# sourced by /etc/init.d/isc-dhcp-relay
# installed at /etc/default/isc-dhcp-relay by the maintainer scripts

#
# This is a POSIX shell fragment
#

# What servers should the DHCP relay forward requests to?
SERVERS="192.168.56.101"

# On what interfaces should the DHCP relay (dhrelay) serve DHCP requests?
INTERFACES="enp0s3"

# Additional options that are passed to the DHCP relay daemon?
OPTIONS=""
  
```

- Isc-dhcp-relay를 active 확인하기 ⇒ 실패

```

"/etc/default/isc-dhcp-relay" 16L, 442B written
ubuntu@ubuntu:~$ sudo systemctl status isc-dhcp-relay
* isc-dhcp-relay.service - ISC DHCP IPv4 relay
   Loaded: loaded (/lib/systemd/system/isc-dhcp-relay.service; enabled; vendor preset: enabled)
   Active: failed (Result: exit-code) since Wed 2024-01-31 06:52:53 UTC; 4min 25s ago
     Docs: man:dhcrelay(8)
   Process: 2248 ExecStart=/bin/sh -ec for I in $INTERFACES; do IFCMD="$IFCMD -i $I"; done;
   Main PID: 2248 (code=exited, status=1/FAILURE)
      CPU: 4ms

Jan 31 06:52:53 ubuntu systemd[1]: Started ISC DHCP IPv4 relay.
Jan 31 06:52:53 ubuntu systemd[1]: isc-dhcp-relay.service: Main process exited, code=exited, status=1/FAILURE
Jan 31 06:52:53 ubuntu systemd[1]: isc-dhcp-relay.service: Failed with result 'exit-code'.
lines 1-11/11 (END)

```

- 오류 확인하기

```

ubuntu@ubuntu:~$ journalctl _PID=2248
Jan 31 06:52:53 ubuntu dhcrelay[2248]: Internet Systems Consortium DHCP Relay Agent 4.4.1
Jan 31 06:52:53 ubuntu sh[2248]: Internet Systems Consortium DHCP Relay Agent 4.4.1
Jan 31 06:52:53 ubuntu sh[2248]: Copyright 2004-2018 Internet Systems Consortium.
Jan 31 06:52:53 ubuntu sh[2248]: All rights reserved.
Jan 31 06:52:53 ubuntu sh[2248]: For info, please visit https://www.isc.org/software/dhcp/
Jan 31 06:52:53 ubuntu sh[2248]: No servers specified.
Jan 31 06:52:53 ubuntu sh[2248]: If you think you have received this message due to a bug rather
Jan 31 06:52:53 ubuntu sh[2248]: than a configuration issue please read the section on submitting
Jan 31 06:52:53 ubuntu sh[2248]: bugs on either our web page at www.isc.org or in the README file
Jan 31 06:52:53 ubuntu sh[2248]: before submitting a bug. These pages explain the proper
Jan 31 06:52:53 ubuntu sh[2248]: process and the information we find helpful for debugging.
Jan 31 06:52:53 ubuntu sh[2248]: exiting.
Jan 31 06:52:53 ubuntu dhcrelay[2248]: Copyright 2004-2018 Internet Systems Consortium.
Jan 31 06:52:53 ubuntu dhcrelay[2248]: All rights reserved.
Jan 31 06:52:53 ubuntu dhcrelay[2248]: For info, please visit https://www.isc.org/software/dhcp/
Jan 31 06:52:53 ubuntu dhcrelay[2248]: No servers specified.
Jan 31 06:52:53 ubuntu dhcrelay[2248]:
Jan 31 06:52:53 ubuntu dhcrelay[2248]: If you think you have received this message due to a bug rather
Jan 31 06:52:53 ubuntu dhcrelay[2248]: than a configuration issue please read the section on submitting
Jan 31 06:52:53 ubuntu dhcrelay[2248]: bugs on either our web page at www.isc.org or in the README file
Jan 31 06:52:53 ubuntu dhcrelay[2248]: before submitting a bug. These pages explain the proper
Jan 31 06:52:53 ubuntu dhcrelay[2248]: process and the information we find helpful for debugging.
Jan 31 06:52:53 ubuntu dhcrelay[2248]: exiting.
lines 1-24/24 (END)

```

- 아래의 파일 삭제하기

```

E325: ATTENTION
Found a swap file by the name "/etc/default/.isc-dhcp-relay.swp"
   owned by: root   dated: Wed Jan 31 07:01:11 2024
   file name: /etc/default/isc-dhcp-relay
   modified: no
   user name: root   host name: ubuntu
   process ID: 2392 (STILL RUNNING)
While opening file "/etc/default/isc-dhcp-relay"
   dated: Wed Jan 31 06:57:10 2024

(1) Another program may be editing the same file. If this is the case,
    be careful not to end up with two different instances of the same
    file when making changes. Quit, or continue with caution.
(2) An edit session for this file crashed.
    If this is the case, use ":recover" or "vim -r /etc/default/isc-dhcp-relay"
    to recover the changes (see ":help recovery").
    If you did this already, delete the swap file "/etc/default/.isc-dhcp-relay.swp"
    to avoid this message.

Swap file "/etc/default/.isc-dhcp-relay.swp" already exists!
[O]pen Read-Only, [E]dit anyway, [R]ecover, [Q]uit, [A]bort:

```


- 아래 명령어로 삭제하기

```
ubuntu@ubuntu:~$ sudo rm /etc/default/.isc-dhcp-relay.swp
```

- 다시 활성화하고 active 확인하기 ⇒ 성공

```
sudo systemctl restart isc-dhcp-relay
```

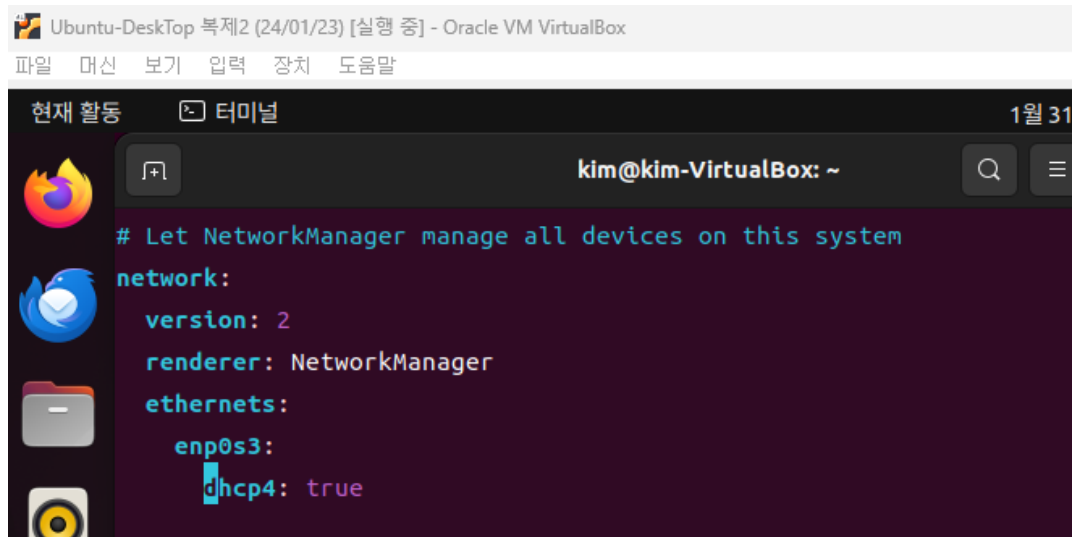
```
sudo systemctl status isc-dhcp-relay
```

```
ubuntu@ubuntu:~$ sudo systemctl start isc-dhcp-relay
ubuntu@ubuntu:~$
ubuntu@ubuntu:~$ sudo systemctl restart isc-dhcp-relay
ubuntu@ubuntu:~$ sudo systemctl status isc-dhcp-relay
• isc-dhcp-relay.service - ISC DHCP IPv4 relay
   Loaded: loaded (/lib/systemd/system/isc-dhcp-relay.service; enabled; vendor preset: enabled)
   Active: active (running) since Wed 2024-01-31 07:22:06 UTC; 5s ago
     Docs: man:dhcrelay(8)
    Main PID: 2516 (dhcrelay)
      Tasks: 4 (limit: 2221)
    Memory: 1.6M
       CPU: 11ms
```

4) WAS(U-D2)가 DHCP로부터 ip 할당받기

- netplan에서 dhcp 켜주기

```
sudo vim /etc/netplan/01-network-manager-all.yaml //netplan 편집기
```



```
sudo netplan apply
```

- but ip 할당이 X됨

```

link/ether 08:00:27:35:9f:74 brd ff:ff:ff:ff:ff:ff
kim@kim-VirtualBox:~$ 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: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:35:9f:74 brd ff:ff:ff:ff:ff:ff
kim@kim-VirtualBox:~$

```

- 오류 수정: /etc/default/isc-dhcp-relay에서 DHCP로 통신할 interface를 모두 넣기

```

Ubuntu-Server1 복제(router) (스냅샷 1/25) [실행 중] - Oracle VM VirtualBox
파일  머신  보기  입력  장치  도움말

# Defaults for isc-dhcp-relay initscript
# sourced by /etc/init.d/isc-dhcp-relay
# installed at /etc/default/isc-dhcp-relay by the maintainer scripts

#
# This is a POSIX shell fragment
#
# What servers should the DHCP relay forward requests to?
SERVERS="192.168.56.101"
# On what interfaces should the DHCP relay (dhrelay) serve DHCP requests?
INTERFACES="enp0s3 enp0s8 enp0s9"
# Additional options that are passed to the DHCP relay daemon?
OPTIONS=""

```

sudo netplan apply

- ip 다시 할당받기 ⇒ 성공

```

kim@kim-VirtualBox:/var/www/html/PHP$ 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: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:35:9f:74 brd ff:ff:ff:ff:ff:ff
    inet 192.168.76.101/24 brd 192.168.76.255 scope global dynamic noprefixroute enp0s3
        valid_lft 42659sec preferred_lft 42659sec
kim@kim-VirtualBox:/var/www/html/PHP$

```

5) DB(U-S1)가 DHCP로부터 ip 할당받기

- DB 서버의 netplan 수정하기

```
# This is the network config written by 'subiquity'
network:
  ethernets:
    enp0s3:
      #addresses: [192.168.96.101/24]
      #gateway4: 192.168.96.254
      #nameservers:
      # addresses: [8.8.8.8]
      dhcp4: true
  version: 2
```

- ip 할당 받아오기 ⇒ 성공

```
kim@kim-VirtualBox:~$ 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: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:35:9f:74 brd ff:ff:ff:ff:ff:ff
    inet 192.168.76.101/24 brd 192.168.76.255 scope global dynamic noprefixroute enp0s3
        valid_lft 43199sec preferred_lft 43199sec
```

III. 과제

1. 문제 1번

- 인터넷에 접속하여 패킷을 수집하고, 아래 조건 별로 각각 필터링 해본다.

- HTTP 프로토콜의 패킷
- 출발지 IP가 내 컴퓨터 주소인 패킷
- ARP와 ICMP를 제외한 모든 패킷
- 게이트웨이를 타겟으로 한 ARP 패킷

1) HTTP 프로토콜의 패킷

- HTTP 패킷만 필터링하기 위해 필터 바에 **http**를 입력하기

Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

No.	Time	Source	Destination	Protocol	Length	Info
29156	184.574113	172.30.1.8	23.41.83.26	HTTP	267	GET /ko-KR/livetile/preinstall?region=KR&appId=C98EAS80842088940508F071E1DA76512D21FE36&FORM%Threshold HTTP/1.1
29161	184.614516	172.30.1.8	23.41.83.26	HTTP/XOIL	223	HTTP/1.1 200 OK
44442	288.246493	172.30.1.8	23.2.16.56	HTTP	304	GET /c/msdownload/update/others/2024/01/40603782_68468984991ce78757f082426a7710b53854d62f.cab HTTP/1.1
44454	288.425186	172.30.1.8	23.2.16.56	HTTP	422	HTTP/1.1 200 OK (application/vnd.ms-cab-compressed)
44457	288.467998	172.30.1.8	23.2.16.56	HTTP	304	GET /c/msdownload/update/others/2024/01/40603781_7395e924cb07b1ad3ca9a2b403cbe452ca4e0ac.cab HTTP/1.1
44465	288.565261	172.30.1.8	23.2.16.56	HTTP	412	HTTP/1.1 200 OK (application/vnd.ms-cab-compressed)
44467	288.591242	172.30.1.8	23.2.16.56	HTTP	304	GET /c/msdownload/update/others/2024/01/40603099_cad8f3a3b6e0691137a92385653995574bf16b2.cab HTTP/1.1
44478	288.812629	172.30.1.8	23.2.16.56	HTTP	419	HTTP/1.1 200 OK (application/vnd.ms-cab-compressed)
44480	288.869588	172.30.1.8	23.2.16.56	HTTP	304	GET /c/msdownload/update/others/2024/01/40603098_2d3c15dd1f42a3eabc1e32804a769624e0476bad.cab HTTP/1.1
44494	289.036570	172.30.1.8	23.2.16.56	HTTP	419	HTTP/1.1 200 OK (application/vnd.ms-cab-compressed)
44496	289.108979	172.30.1.8	23.2.16.56	HTTP	304	GET /c/msdownload/update/others/2024/01/40602409_d1a47feb3a3e68e2431439c12823c0838cfd8e68.cab HTTP/1.1
44509	289.211864	172.30.1.8	23.2.16.56	HTTP	423	HTTP/1.1 200 OK (application/vnd.ms-cab-compressed)
44511	289.217085	172.30.1.8	23.2.16.56	HTTP	304	GET /c/msdownload/update/others/2024/01/40602408_1ee41c60f41a06e58bdcee57719d7ebc47af0aa.cab HTTP/1.1
44517	289.347407	172.30.1.8	23.2.16.56	HTTP	419	HTTP/1.1 200 OK (application/vnd.ms-cab-compressed)
44519	289.348626	172.30.1.8	23.2.16.56	HTTP	304	GET /d/msdownload/update/others/2024/01/40605663_e55aaade54d1a84f130e8c8c614d0859017ff041.cab HTTP/1.1
44525	289.408026	172.30.1.8	23.2.16.56	HTTP	1086	HTTP/1.1 200 OK (application/vnd.ms-cab-compressed)
44527	289.492277	172.30.1.8	23.2.16.56	HTTP	304	GET /d/msdownload/update/others/2024/01/40605459_2a87bdeae8e6a638c7cd85b43282e16302cbe65b0.cab HTTP/1.1
44535	289.632776	172.30.1.8	23.2.16.56	HTTP	1033	HTTP/1.1 200 OK (application/vnd.ms-cab-compressed)
44537	289.641590	172.30.1.8	23.2.16.56	HTTP	304	GET /c/msdownload/update/others/2024/01/40605339_3df539f2297dc78482cc47a867406b08c365098.cab HTTP/1.1
44545	289.924411	172.30.1.8	23.2.16.56	HTTP	1068	HTTP/1.1 200 OK (application/vnd.ms-cab-compressed)
44547	289.996218	172.30.1.8	23.2.16.56	HTTP	304	GET /d/msdownload/update/others/2024/01/40604732_0d1c6a0802238e3cc21f38bf4f09cae584746aa2.cab HTTP/1.1
44557	290.109029	172.30.1.8	23.2.16.56	HTTP	1052	HTTP/1.1 200 OK (application/vnd.ms-cab-compressed)
44559	290.239131	172.30.1.8	23.2.16.56	HTTP	304	GET /d/msdownload/update/others/2024/01/40604612_5e9430a9ee23e6b5950f53a14e6b5cb6706ef68.cab HTTP/1.1
44570	290.338178	172.30.1.8	23.2.16.56	HTTP	1083	HTTP/1.1 200 OK (application/vnd.ms-cab-compressed)
44572	290.340111	172.30.1.8	23.2.16.56	HTTP	304	GET /d/msdownload/update/others/2024/01/40604018_b2b8f9e7fd692e6d162ffe1fd4402fed6080e0a7.cab HTTP/1.1
44607	290.441095	172.30.1.8	23.2.16.56	HTTP	1049	HTTP/1.1 200 OK (application/vnd.ms-cab-compressed)

> Frame 29156: 267 bytes on wire (2136 bits), 267 bytes captured (2136 bits) on interface \Device\NPF_{2CDC8C30-AA79-4017-A950-5...}

> Ethernet II, Src: IntelCor_1a:f7:f2 (e4:0d:36:1a:f7:f2), Dst: Mercury_09:b5:49 (b4:a9:4f:09:b5:49)

> Internet Protocol Version 4, Src: 172.30.1.8, Dst: 23.41.83.26

> Transmission Control Protocol, Src Port: 59419, Dst Port: 80, Seq: 1, Ack: 1, Len: 213

> Hypertext Transfer Protocol

0000 b4 a9 4f 09 b5 49 e4 0d 36 1a f7 f2 08 00 45 00 ...O I... 6....E

0010 00 fd fe 97 40 00 00 00 00 00 ac 1a 01 08 17 29 ...@.....)

0020 53 1a e8 1b 00 50 9d ec af a2 cd ac 9c 15 50 18 S...Y...P

0030 01 00 18 59 00 00 47 45 54 20 2f 6b 6f 2d 4b 52 ...GE T /ko-KR

0040 2f 6c 69 76 65 74 69 6c 65 2f 70 72 65 69 6e 73 /livetile/preins

0050 74 61 6c 6c 3f 72 65 67 69 6f 6e 3d 4b 52 61 call?reg IonaK8a

0060 70 70 69 64 3d 43 39 38 45 41 35 42 30 38 34 32 ppIdC98 EAS80842

0070 44 42 42 39 34 30 35 42 42 46 30 37 31 45 31 44 D8894058 BF07E1D

- 해당 패킷의 자세한 정보는 다음과 같이 살펴볼 수 있음 (아래 패킷의 포트는 80)

> Frame 29156: 267 bytes on wire (2136 bits), 267 bytes captured (2136 bits) on interface \Device\NPF_{2CDC8C30-AA79-4017-A950-5...}

> Ethernet II, Src: IntelCor_1a:f7:f2 (e4:0d:36:1a:f7:f2), Dst: Mercury_09:b5:49 (b4:a9:4f:09:b5:49)

> Internet Protocol Version 4, Src: 172.30.1.8, Dst: 23.41.83.26

> Transmission Control Protocol, Src Port: 59419, Dst Port: 80, Seq: 1, Ack: 1, Len: 213

Source Port: 59419

Destination Port: 80

[Stream index: 213]

[Conversation completeness: Complete, WITH_DATA (31)]

[TCP Segment Len: 213]

Sequence Number: 1 (relative sequence number)

Sequence Number (raw): 2649534370

[Next Sequence Number: 214 (relative sequence number)]

Acknowledgment Number: 1 (relative ack number)

Acknowledgment number (raw): 3450641429

0101 = Header Length: 20 bytes (5)

> Flags: 0x018 (PSH, ACK)

Window: 256

[Calculated window size: 65536]

[Window size scaling factor: 256]

Checksum: 0x1859 [unverified]

[Checksum Status: Unverified]

Urgent Pointer: 0

> [Timestamps]

> [SEQ/ACK analysis]

TCP payload (213 bytes)

> Hypertext Transfer Protocol

2) 출발지 ip가 내 컴퓨터 주소인 패킷

- 필터바에 다음과 같이 입력

ip.src == {내 pc의 ip}

No.	Time	Source	Destination	Protocol	Length	Info
29116	182.123577	172.30.1.8	172.64.150.28	QUIC	127	Handshake, DCID=01b715a00100ba4dc8b737a07f00
29117	182.123894	172.30.1.8	172.64.150.28	QUIC	124	Protected Payload (KP0), DCID=01b715a00100ba
29118	182.124346	172.30.1.8	172.64.150.28	QUIC	1292	Protected Payload (KP0), DCID=01b715a00100ba
29119	182.124400	172.30.1.8	172.64.150.28	QUIC	1292	Protected Payload (KP0), DCID=01b715a00100ba
29120	182.124424	172.30.1.8	172.64.150.28	QUIC	1292	Protected Payload (KP0), DCID=01b715a00100ba
29121	182.124451	172.30.1.8	172.64.150.28	QUIC	780	Protected Payload (KP0), DCID=01b715a00100ba
29126	182.127209	172.30.1.8	172.64.150.28	QUIC	86	Protected Payload (KP0), DCID=01b715a00100ba
29127	182.127331	172.30.1.8	172.64.150.28	QUIC	89	Protected Payload (KP0), DCID=01b715a00100ba
29130	182.159798	172.30.1.8	172.64.150.28	QUIC	86	Protected Payload (KP0), DCID=01b715a00100ba
29131	182.303719	172.30.1.8	108.177.97.188	TCP	55	[TCP Keep-Alive] 58037 → 443 [ACK] Seq=1 Acl

- 내 컴퓨터 ip는 cmd에서 확인 가능

```
무선 LAN 어댑터 Wi-Fi:
연결별 DNS 접미사. . . . . :
링크-로컬 IPv6 주소 . . . . . : fe80::6121:1ace:39fa:4447%6
IPv4 주소 . . . . . : 172.30.1.8
서브넷 마스크 . . . . . : 255.255.255.0
기본 게이트웨이 . . . . . : 172.30.1.254

이더넷 어댑터 Bluetooth 네트워크 연결:
미디어 상태 . . . . . : 미디어 연결 끊김
연결별 DNS 접미사. . . . . :
```

3) ARP & ICMP를 제외한 모든 패킷

- 필터바에 다음과 같이 입력

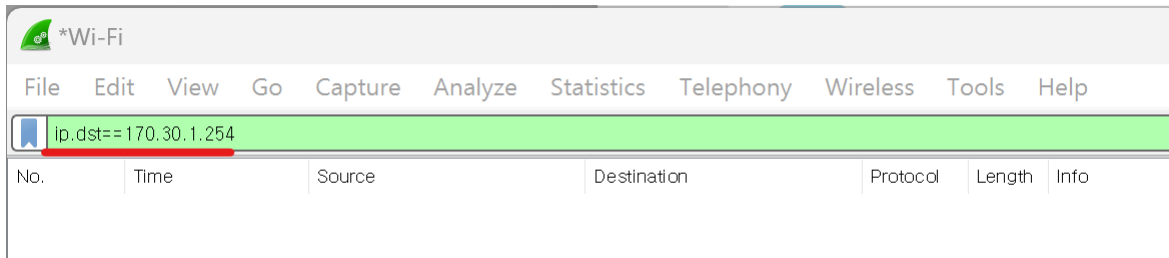
not (arp or icmp)

No.	Time	Source	Destination	Protocol	Length	Info
29131	182.303719	172.30.1.8	108.177.97.188	TCP	55	[TCP Keep-Alive] 58037 → 443 [ACK] Seq=1 Ack=1 Win=510 Len=1
29132	182.335461	172.30.1.8	172.64.150.28	QUIC	83	Protected Payload (KP0), DCID=01b715a00100ba4dc8b737a07f009fc212d48081
29133	182.338093	172.64.150.28	172.30.1.8	QUIC	65	Protected Payload (KP0)
29134	182.363716	108.177.97.188	172.30.1.8	TCP	66	[TCP Keep-Alive ACK] 443 → 58037 [ACK] Seq=1 Ack=2 Win=265 Len=0 SLE=1
29135	182.539942	172.30.1.8	172.64.150.28	QUIC	83	Protected Payload (KP0), DCID=01b715a00100ba4dc8b737a07f009fc212d48081
29136	182.551258	172.64.150.28	172.30.1.8	QUIC	65	Protected Payload (KP0)
29137	182.753484	172.30.1.8	172.64.150.28	QUIC	83	Protected Payload (KP0), DCID=01b715a00100ba4dc8b737a07f009fc212d48081

4) 게이트웨이를 타겟으로 한 ARP 패킷

- 필터바에 다음과 같이 입력

ip.dst=={내 PC의 gw}



- 아무것도 뜨지 않음

2. 문제 2번

Nslookup을 사용해 다음 내용을 확인

- Google의 Mail server 개수
- Naver의 Nameserver 개수
- 도메인의 모든 레코드를 한 번에 출력하는 명령어는? (help로 옵션확인)

1) Google의 Mail server 개수

•

```
관리자: 명령 프롬프트 - nslookup

미디어 상태 : 미디어 연결 끊김
연결별 DNS 접미사 :

C:\Windows\System32>
C:\Windows\System32>nslookup
기본 서버: kns.kornet.net
Address: 168.126.63.1

> set q=mx
> gmail.com
서버: kns.kornet.net
Address: 168.126.63.1

권한 없는 응답:
gmail.com MX preference = 5, mail exchanger = gmail-smtp-in.l.google.com
gmail.com MX preference = 20, mail exchanger = alt2.gmail-smtp-in.l.google.com
gmail.com MX preference = 40, mail exchanger = alt4.gmail-smtp-in.l.google.com
gmail.com MX preference = 10, mail exchanger = alt1.gmail-smtp-in.l.google.com
gmail.com MX preference = 30, mail exchanger = alt3.gmail-smtp-in.l.google.com

alt1.gmail-smtp-in.l.google.com internet address = 142.250.141.26
alt2.gmail-smtp-in.l.google.com internet address = 142.250.115.26
alt3.gmail-smtp-in.l.google.com internet address = 108.177.104.27
alt4.gmail-smtp-in.l.google.com internet address = 142.250.152.27
alt3.gmail-smtp-in.l.google.com AAAA IPv6 address = 2607:f8b0:4003:c04::1a
>
```

2) naver의 nameserver 개수

```
> set q=ns
> naver.com
서버:      kns.kornet.net
Address:    168.126.63.1

권한 없는 응답:
naver.com      nameserver = ns2.naver.com
naver.com      nameserver = ns1.naver.com

ns1.naver.com  internet address = 125.209.248.6
ns2.naver.com  internet address = 125.209.249.6
>
```

3) 도메인의 모든 레코드를 한 번에 출력하는 명령어

```
관리자: 명령 프롬프트 - nslookup
>
> help
명령: (식별자는 대문자로 표시되고 []는 선택 사항을 나타냄)
NAME          - 기본 서버를 사용하는 호스트/도메인 NAME에 대한 정보 인쇄
NAME1 NAME2    - 위와 같지만 NAME2를 서버로 사용
help 또는 ?    - 일반 명령에 대한 정보 인쇄
set OPTION     - 옵션 설정
all            - 옵션, 현재 서버 및 호스트 인쇄
[no]debug      - 디버깅 정보 인쇄
[no]d2         - 자세한 디버깅 정보 인쇄
[no]defname     - 각 쿼리에 도메인 이름 추가
[no]recurse    - 쿼리에 대해 재귀 응답 요청
[no]search     - 도메인 검색 목록 사용
[no]vc         - 항상 가상 회로 사용
domain=NAME     - 기본 도메인 이름을 NAME으로 설정
srchlist=N1[/N2/.../N6] - 도메인을 N1로, 검색 목록을 N1,N2 등으로 설정
root=NAME       - 루트 서버를 NAME으로 설정
retry=X        - 다시 시도 횟수를 X로 설정
timeout=X      - 초기 시간 제한 간격을 X초로 설정
type=X         - 쿼리 유형 설정(예: A,AAAA,ANY,CNAME,MX,NS,PTR,SOA,SRV)
querytype=X    - type과 동일함
class=X        - 쿼리 클래스 설정(예: IN (Internet), ANY)
[no]mxfr       - MS 빠른 영역 전송 사용
ixfr=X        - IXFR 전송 요청에서 사용할 현재 버전
server NAME    - 현재 기본 서버를 사용하여 기본 서버를 NAME으로 설정
ls server NAME - 초기 서버를 사용하여 기본 서버를 NAME으로 설정
root          - 현재 기본 서버를 루트로 설정
ls [opt] DOMAIN [> FILE] - DOMAIN에 있는 주소 나열(선택 사항: FILE에 출력)
-a            - 정식 이름 및 별칭 나열
-d            - 모든 레코드 나열
-t TYPE       - 주어진 RFC 레코드 형식의 레코드 나열(예: A,CNAME,MX,NS,PTR 등)
view FILE     - 'ls' 출력 파일 정렬 및 pg로 보기
exit          - 프로그램 끝내기
```

```
> ls google.com
[kns.kornet.net]
*** 도메인 google.com을(를) 나열할 수 없습니다. BAD ERROR VALUE
DNS 서버가 영역 google.com을(를) 사용 중인 컴퓨터에 전송하는 것을 거부했습니다.
잘못된 경우에는 IP 주소 168.126.63.1의 DNS에서 google.com의 영역 전송 보안 설정을
확인하십시오.
```