

컴퓨터네트워크

과제 #02 보고서

이름	김대욱
학번	202255513
소속 학과/대학	정보의생명공학대학 정보컴퓨터공학부
분반	061

<과제 >

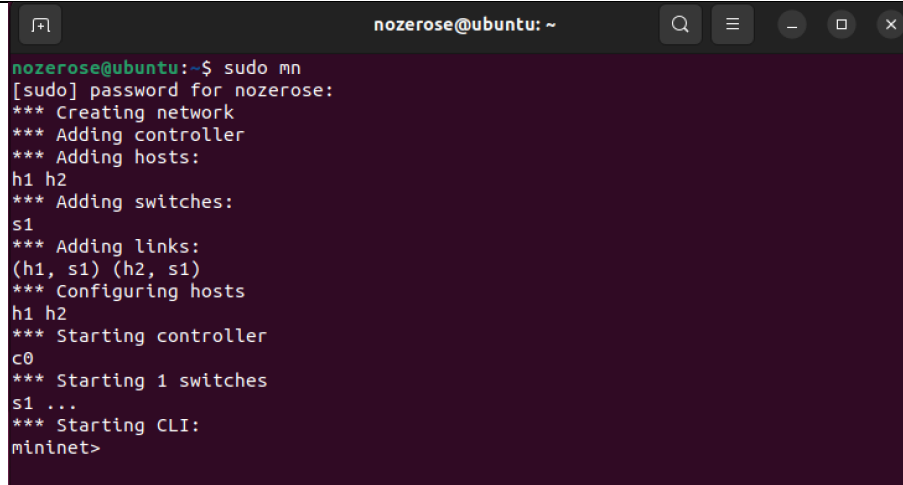
[Q 1] Mininet 네트워크 에뮬레이터 [배점: 40]

Mininet 네트워크 에뮬레이터를 설치하고 활용하는 과제입니다. Mininet 의 공식 홈페이지는 <http://mininet.org/> 입니다.

[TODO 1] Mininet 프로그램을 간단히 설명하세요 (용도, 특징, 장단점 등).

Mininet 은 개인 PC 에서도 쉽게 가상 네트워크(Virtual Network)를 구성하여, network 환경을 간단히 테스트 해볼 수 있는 emulator 이다. Open vSwitch 기반 OpenFlow 스위치와 ONOS, OpenDaylight 등의 SDN 컨트롤러를 지원하여 SDN 환경을 테스트할 수 있는 것이 큰 장점이다. 그러나, emulation 환경으로 실제 네트워킹 환경과의 성능 차이가 있다는 단점도 존재한다.

[TODO 2] Mininet 설치하기: <http://mininet.org/download/> 를 참고하여 Mininet 을 설치하세요. 기존에 사용하던 리눅스 VM 에 Mininet 을 직접 설치해도 되고, Mininet 이 설치된 VM 이미지를 다운받아 실행해도 됩니다. Mininet 을 설치한 후, 터미널에서 \$ sudo mn 을 입력하여 Mininet 을 실행하세요. 실행 직후에 출력되는 터미널 출력을 캡처하여 아래에 첨부하세요.



```
nozerose@ubuntu: ~  
nozerose@ubuntu:~$ sudo mn  
[sudo] password for nozerose:  
*** Creating network  
*** Adding controller  
*** Adding hosts:  
h1 h2  
*** Adding switches:  
s1  
*** Adding links:  
(h1, s1) (h2, s1)  
*** Configuring hosts  
h1 h2  
*** Starting controller  
c0  
*** Starting 1 switches  
s1 ...  
*** Starting CLI:  
mininet>
```

[TODO 3] \$ sudo mn 으로 Mininet 을 실행하면 기본 토폴로지가 자동으로 생성됩니다. nodes, dump, net, h1 ifconfig, h2 ifconfig 등의 명령을 사용하여 아래의 질문에 답하세요.

1. 생성된 호스트의 수는 총 몇 개? 2 개

2. 생성된 스위치의 수는 총 몇 개? 1 개

```
mininet> h1 ifconfig
h1-eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.0.1 netmask 255.0.0.0 broadcast 10.255.255.255
    inet6 fe80::1c92:33ff:fe42:8017 prefixlen 64 scopeid 0x20<link>
    ether 1e:92:33:42:80:17 txqueuelen 1000 (Ethernet)

mininet> h2 ifconfig
h2-eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.0.2 netmask 255.0.0.0 broadcast 10.255.255.255
    inet6 fe80::9c4f:c9ff:fe9e:7c13 prefixlen 64 scopeid 0x20<link>
    ether 9e:4f:c9:9e:7c:13 txqueuelen 1000 (Ethernet)
```

3. 생성된 모든 호스트에 대해 아래의 테이블을 완성하십시오:

호스트 이름(h1, h2, ...)	호스트의 IP 주소	호스트의 MAC 주소
h1	10.0.0.1	1e:92:33:42:80:17
h2	10.0.0.2	9e:4f:c9:9e:7c:13
...

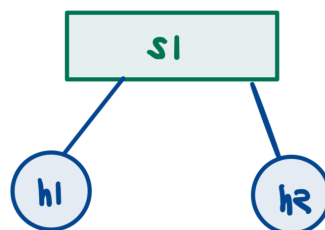
```
s1-eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet6 fe80::14d0:35ff:fee8:28c2 prefixlen 64 scopeid 0x20<link>
    ether 16:d0:35:e8:28:c2 txqueuelen 1000 (Ethernet)
    RX packets 13 bytes 1006 (1.0 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 36 bytes 3913 (3.9 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

s1-eth2: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet6 fe80::e47a:26ff:fe95:5852 prefixlen 64 scopeid 0x20<link>
    ether e6:7a:26:95:58:52 txqueuelen 1000 (Ethernet)
    RX packets 13 bytes 1006 (1.0 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 36 bytes 3913 (3.9 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

4. 스위치 s1에 대해 아래의 테이블을 완성하십시오.

호스트 h1에 연결된 스위치 포트(=NIC)의 MAC 주소	16:d0:35:e8:28:c2
호스트 h2에 연결된 스위치 포트(=NIC)의 MAC 주소	e6:7a:26:95:58:52
...	...

[TODO 4] Mininet 실행 시, 기본으로 생성되는 토폴로지를 그림으로 표현하세요. 참고로, 컨트롤러는 그림에 포함할 필요 없으며, 호스트는 원으로, 스위치는 사각형으로 그림 그리고, 원과 사각형의 중앙에는 h1, s1 등 해당 호스트/스위치의 이름을 입력하세요.



[Q 2] Wireshark [배점: 60]

Kali 리눅스 및 Mininet VM 에는 Wireshark 프로그램이 기본적으로 설치되어 있습니다. 프로그램을 실행하는 방법은 `$ sudo wireshark &` 입니다. Wireshark 이 설치되어 있지 않다면 공식홈페이지(<https://www.wireshark.org/>)에서 다운받아 설치하거나, `$ sudo apt install wireshark` 명령으로 직접 설치하세요(또는 인터넷을 검색하여 설치방법 찾아보기).

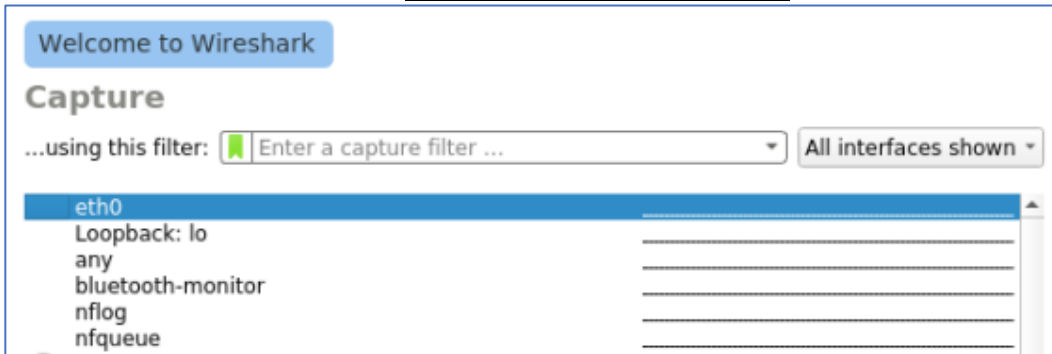
[TODO 1] 위에서 설명한 프로그램 실행 방법에서, 터미널 명령 마지막의 & 기호가 수행하는 기능은 무엇인지 설명하세요.

Linux 터미널에서 백그라운드(background)에서 프로세스를 실행하는 역할을 한다. 해당 기호를 사용하면, `$ sudo wireshark &` 명령어를 입력한 후에도 terminal 을 계속 사용할 수 있다.

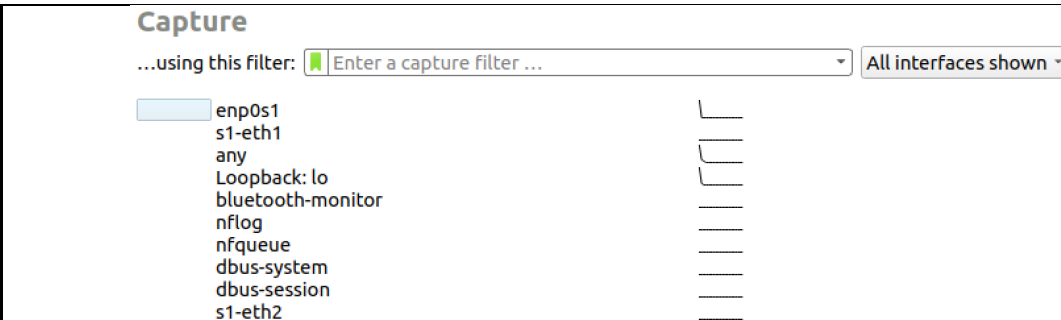
[TODO 2] Wireshark 프로그램을 간단히 설명하세요(사용 용도, 특징, 장/단점 등)

Wireshark 프로그램은 네트워크 패킷 분석 도구로, 네트워크 트래픽을 실시간으로 모니터링하고 프로토콜 분석 등의 기능을 사용할 수 있다. 특징으로는 다양한 프로토콜을 지원할 뿐만 아니라, 필터링 기능과 실시간 모니터링이 가능하다는 점이 있다. 네트워크 패킷을 깊게 분석할 수 있고 open source 라는 점이 장점으로 꼽히지만, wireshark 를 통한 네트워크 트래픽 분석으로 보안 문제가 발생할 수 있고 초보자에게는 다소 어려울 수 있다는 점이 단점으로 꼽힌다.

[TODO 3] Wireshark 프로그램을 실행하면 Capture List 화면이 나타나고, 캡처 가능한 인터페이스 목록이 아래와 같이 나열됩니다. 이 때, Mininet 이 실행되지 않은 상태라고 가정합니다.



이번에는, Wireshark 를 실행한 상태에서 Mininet 을 실행하세요. Mininet 을 실행하면, s1-eth1, s1-eth2 등 가상으로 생성한 스위치의 인터페이스가 캡처 가능한 인터페이스 목록(Capture List)에 포함되는 것을 알 수 있습니다. Mininet 에서 생성된 가상 스위치의 인터페이스가 보이도록 Capture List 화면을 캡처하여 아래에 첨부하세요



[TODO 4] Wireshark 프로그램의 Capture List 화면에서 s1-eth1 를 더블 클릭하여 해당 인터페이스에서 오고 가는 패킷의 캡처를 시작하세요. 다음으로, Mininet 에서 `mininet> h1 ping h2 -c 1` 명령을 입력하여 h1 에서 h2 로 1 회 PING 명령을 실행하세요. PING 명령으로 인해 생성/전송된 패킷이 캡처 된 내역이 보이도록 Wireshark 프로그램 화면을 캡처하여 아래에 첨부하세요.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	52:87:48:a4:43:df	Broadcast	ARP	42	Who has 10.0.0.2? Tell 10.0.0.1
2	0.005674654	66:ec:ea:ee:47:7f	52:87:48:a4:43:df	ARP	42	10.0.0.2 is at 66:ec:ea:ee:47:7f
3	0.005677988	10.0.0.1	10.0.0.2	ICMP	98	Echo (ping) request id=0xebd3, seq=1/256, ttl=64 (reply in 4)
4	0.011492979	10.0.0.2	10.0.0.1	ICMP	98	Echo (ping) reply id=0xebd3, seq=1/256, ttl=64 (request in 3)

[TODO 5] 위와 같은 상태에서(즉, [TODO 4]를 실행한 후), 첫 번째로 캡처 된 패킷을 클릭하면, 화면 중앙에 Frame 1, Ethernet II, Internet Protocol Version 4, Internet Control Message Protocol 과 같은 엔트리가 나타납니다. 이 중, Ethernet II 및 Internet Protocol Version 4 엔트리 내에 포함된 정보를 확인하고, 아래의 질문에 답하세요.

1. 패킷의 출발지 MAC 주소는 누구의 주소와 일치하는지? h1 의 MAC 주소
2. 패킷의 목적지 MAC 주소는 누구의 주소와 일치하는지? h2 의 MAC 주소
3. 패킷의 출발지 IP 주소는 누구의 주소와 일치하는지? h1 의 IP 주소
4. 패킷의 목적지 IP 주소는 누구의 주소와 일치하는지? h2 의 IP 주소

[TODO 6] Wireshark 프로그램 화면 상단의 단축 버튼 중에서 “Restart Current Capture”를 클릭하여 새로운 캡처를 시작하세요. 다음으로, 아래의 명령을 Mininet 에서 입력하세요.

- (1) `mininet> h1 python -m http.server 80 &`
- (2) `mininet> h2 wget -O - h1`

아래의 질문에 답하세요.

- 위의 명령어 (1)은 어떤 기능을 수행하는 명령어인지? python 내장 http 서버를 80 번 포트에서 백그라운드로 실행하는 명령어이다.
- 위의 명령어 (2)는 어떤 기능을 수행하는 명령어인지? h1 주소로 접속하고 해당 웹페이지 내용을 다운로드하는 명령어이다.
- (1), (2)번 명령을 실행한 후, Wireshark 에서 캡처된 패킷 목록을 보면, 첫번째 GET 패킷이 전송되기 전에 [SYN] → [SYN, ACK] → [ACK]의 세 개 패킷이 교환된 것을 알 수 있다. 이 세 개의 패킷은 각각 무슨 역할을 수행하는지?
 - (i) [SYN] : h2 가 h1 에게 연결을 요청하는데 사용한다.
 - (ii) [SYN, ACK] : h1 이 SYN 패킷을 받으면, 연결 요청을 수락하고 h2 에게 응답하기 위해 사용한다.
 - (iii) [ACK] : h2 는 h1 의 SYN-ACK 패킷을 받으면, 연결이 수립되었음을 확인하는 ACK 패킷을 다시 h1 에게 보낸다. 이로써, 데이터 전송을 위한 연결이 완료된다.