

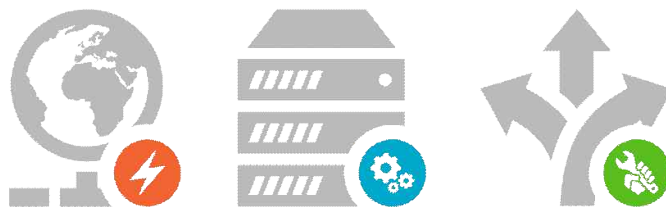
## IV

### 서버 구축 기초

11 서버 구축 실습용 네트워크 토폴로지 구축

12 Telnet, FTP, HTTP 설정

13 DNS 설정



## 11 서버 구축 실습용 네트워크 토폴로지 구축

## ★ 가상 컴퓨터 생성 및 설치

버추얼박스를 이용하여 용도에 맞춰 가상머신을 생성한다. 실습용 가상머신을 생성할 때는 가능한 시스템 자원을 적게 사용할 수 있도록 구성한다. 클라이언트용 가상머신은 웹브라우저 등을 사용할 경우가 많으므로 X 윈도 기반으로 설치하고, 서버의 경우 X 윈도 없이 가볍게 설치할 것을 권장한다.

또한 비슷한 용도로 사용되는 가상머신은 기준이 되는 가상머신을 만들고, 기본 가상머신을 복제하여 필요한 패키지나 설정을 추가하여 사용하면 더욱 효율적이다.

가상머신의 생성 및 관리 등은 [I 수업 준비]를 참고한다.



## ■ TIP - 가상머신 생성 시 유의 사항

GNS와 VirtualBox를 연동하게 실행할 경우에는 VirtualBox에서 실행되는 가상 컴퓨터의 개수 및 가상 컴퓨터의 RAM, HDD 설정 등에 유의해야 한다. 가상 컴퓨터에 할당된 RAM이 1024MByte라면 실제 호스트 컴퓨터의 RAM 1024MByte가 가상 컴퓨터에 할당된다.

전체 RAM		전체 RAM		
호스트 컴퓨터	가상머신	호스트 컴퓨터	가상머신	가상머신
7168MByte	1024MByte	6144MByte	1024MByte	1024MByte

또한 가상 컴퓨터의 HDD 설정도 비슷한 상황이 발생하지만 HDD의 경우 가상머신의 HDD 설정을 동적 할당으로 할 경우 가상머신의 HDD 전체 크기를 50GByte로 설정했다 하더라도 실제 가상 컴퓨터에서 사용하는 만큼의 HDD만 사용하게 된다. 가능한 동적 할당 방식으로 HDD를 생성한다.

원활한 실습을 위해 호스트 컴퓨터의 RAM 용량은 최소 8GByte(16GByte 권장), SSD 용량은 최소 256GByte(512GByte 이상 권장)이다.

## ■ TIP - 실습을 위한 가상머신 준비

가상머신을 여러 개 이용하여 실습하다보면 다양한 원인으로 가상머신에 문제가 생기는 경우가 발생한다. 이럴 경우 많은 시간이 소요 되므로 사전에 제작한 가상머신을 아래와 같이 ova 파일로 실습용 컴퓨터의 특정 디렉터리에 저장해 둔다.

실습 중 문제가 생긴 가상머신은 삭제하고, 저장해 둔 OVA 파일을 새로 불러들여서 바로 실습을 이어갈 수 있다.

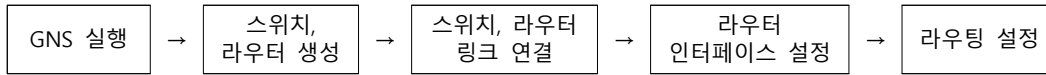
이름	수정한 날짜	유형	크기
VBox_2018_Attack_Kali.ova	2018-08-28 오후 3:16	Open Virtualizatio...	5,725,198...
VBox_2018_Metasploitable.ova	2018-07-28 오후 12:56	Open Virtualizatio...	875,673KB
VBox_2018_SecurityOnion.ova	2018-08-09 오후 9:02	Open Virtualizatio...	2,788,484...
VBox_2018_Untangle.ova	2018-05-16 오후 3:23	Open Virtualizatio...	1,890,762...
VBox_2019_Client_Mint.ova	2019-07-24 오후 11:00	Open Virtualizatio...	3,035,420...
VBox_2020_abc.com_Ubuntu.ova	2020-01-09 오후 3:12	Open Virtualizatio...	1,341,761...
VBox_2020_DNS_Ubuntu.ova	2020-01-12 오후 3:49	Open Virtualizatio...	1,337,130...
VBox_2020_xyz.com_Ubuntu.ova	2020-01-09 오후 10:10	Open Virtualizatio...	1,354,899...

8개 항목

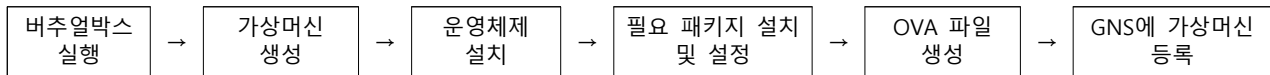
## 1. 실습용 네트워크 토폴로지 및 호스트 구성

[네트워크 구성도]를 참고하여 스위치, 라우터를 이용한 네트워크를 구축하고, 생성한 가상머신을 네트워크와 연결한다. 실습은 네트워크 구축, 서버 구축, 네트워크와 서버 연동의 단계로 진행한다.

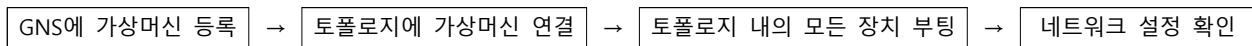
## \* 네트워크 구축 과정



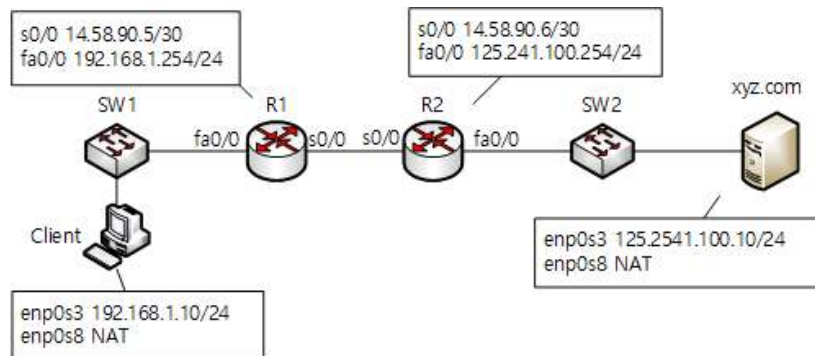
## \* 클라이언트 및 서버 구축 과정



## \* 네트워크와 클라이언트, 서버 연동



## ■ 네트워크 구성도

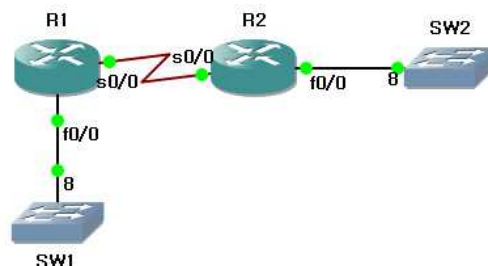


장치명	포트	IP주소	비고
R1	s0/0	14.58.90.5/30	
	fa0/0	192.168.1.254/24	
R2	s0/0	14.58.90.6/30	
	fa0/0	125.241.100.254/24	

장치명	포트	IP주소	비고
Client	enp0s3	192.168.1.10/24	클라이언트
xyz.com	enp0s3	125.241.100.10/24	다양도 서버
관리자 계정 정보 : root / sunrin, sunrin / sunrin			
★ s0/0 = Serial0/0    ★ fa0/0 = fastethernet0/0			

## 2. 네트워크 구축

[네트워크 구성도]를 다음과 같이 토폴로지를 구성하고 라우터 R1, R2의 인터페이스별 주소 설정, 라우팅 설정을 진행한다.



① 라우터 R1의 Fastethernet0/0, Serial0/0의 IP주소를 설정한다.

## ■ Fastethernet0/0 인터페이스 설정

```

R1>enable
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#interface fastethernet 0/0
R1(config-if)#ip address 192.168.1.254 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#
*Mar 1 02:06:05.559: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Mar 1 02:06:06.559: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
R1(config-if)#do write
Building configuration...
[OK]
R1(config-if)#
  
```

## ■ Serial0/0 인터페이스 설정

```

R1>enable
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#interface serial 0/0
R1(config-if)#ip address 14.58.90.5 255.255.255.252
R1(config-if)#no shutdown
R1(config-if)#
*Mar 1 00:18:43.631: %LINK-3-UPDOWN: Interface Serial0/0, changed state to up
R1(config-if)#
*Mar 1 00:18:44.635: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0, changed state to up
R1(config-if)#do write
Building configuration...
[OK]
R1(config-if)#
*Mar 1 00:19:12.515: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0, changed state to down
R1(config-if)#

```

## ② 라우터 R1의 라우팅을 설정한다.(RIP)

```

R1(config)#router rip
R1(config-router)#version 2
R1(config-router)#no auto-summary
R1(config-router)#network 14.58.90.4
R1(config-router)#network 192.168.1.0
R1(config-router)#do write
Building configuration...
[OK]
R1(config-router)#

```

## ③ 라우터 R2의 Fastethernet0/0, Serial0/0의 IP주소를 설정한다.

## ■ Fastethernet0/0 인터페이스 설정

```

R2>enable
R2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#interface fastethernet0/0
R2(config-if)#ip address 125.241.100.254 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#
*Mar 1 00:44:29.787: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Mar 1 00:44:30.787: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
R2(config-if)#do write
Building configuration...
[OK]
R2(config-if)#

```

## ■ Serial0/0 인터페이스 설정

```

R2>enable
R2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#interface serial0/0
R2(config-if)#ip address 14.58.90.6 255.255.255.252
R2(config-if)#no shutdown
R2(config-if)#
*Mar 1 00:45:56.699: %LINK-3-UPDOWN: Interface Serial0/0, changed state to up
R2(config-if)#
*Mar 1 00:45:57.703: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0, changed state to up
R2(config-if)#

```



## ④ 라우터 R2의 라우팅을 설정한다.(RIP)

```

R2
R2(config)#router rip
R2(config-router)#version 2
R2(config-router)#no auto-summary
R2(config-router)#network 14.58.90.4
R2(config-router)#network 125.241.100.0
R2(config-router)#do write
Building configuration...
[OK]
R2(config-router)#

```

## ⑤ show ip route 명령을 통해 생성된 라우팅 테이블을 확인할 수 있다.

```

R2
R2#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

    125.0.0.0/24 is subnetted, 1 subnets
C       125.241.100.0 is directly connected, FastEthernet0/0
R       192.168.1.0/24 [120/1] via 14.58.90.5, 00:00:10, Serial0/0
    14.0.0.0/30 is subnetted, 1 subnets
GatewayC       14.58.90.4 is directly connected, Serial0/0
R2#
    125.0.0.0/24 is subnetted, 1 subnets
R       125.241.100.0 [120/1] via 14.58.90.6, 00:00:16, Serial0/0
C       192.168.1.0/24 is directly connected, FastEthernet0/0
    14.0.0.0/30 is subnetted, 1 subnets
C       14.58.90.4 is directly connected, Serial0/0
R1#

```

## ⑥ 라우터 R1, R2에서 상대방의 라우터에 설정된 네트워크의 게이트웨이로 ping을 보내 연결 상태를 확인한다.

```

R1
R1#ping 125.241.100.254

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 125.241.100.254, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/6/24 ms
R1#

R2
R2#ping 192.168.1.254

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.254, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/38/64 ms
R2#

```

## ⑦ 라우터 R1, R2에서 상대방의 라우터에 설정된 네트워크의 게이트웨이로 trace를 확인한다.

```

R1
R1#trace 125.241.100.254

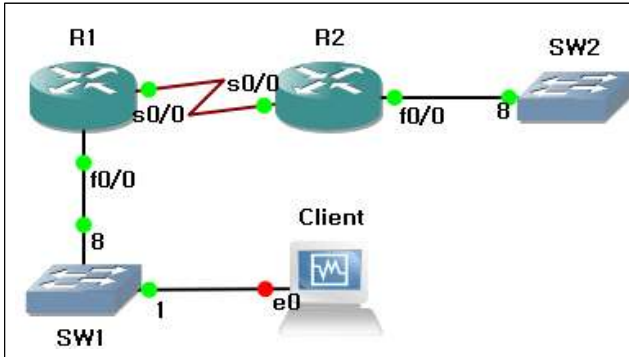
Type escape sequence to abort.
Tracing the route to 125.241.100.254

 0  14.58.90.6 44 msec 32 msec 24 msec
R1#

```

### 3. Client 네트워크 설정

[네트워크 구성도]를 다음과 같이 토폴로지에 Client를 추가하고 SW1과 연결한다. 가상머신의 생성, GNS 등록 등은 [I 수업 준비]를 참고한다. 워크북에서 Client 가상머신으로 사용한 리눅스 배포판 및 네트워크 설정 정보를 아래의 표를 참고한다.

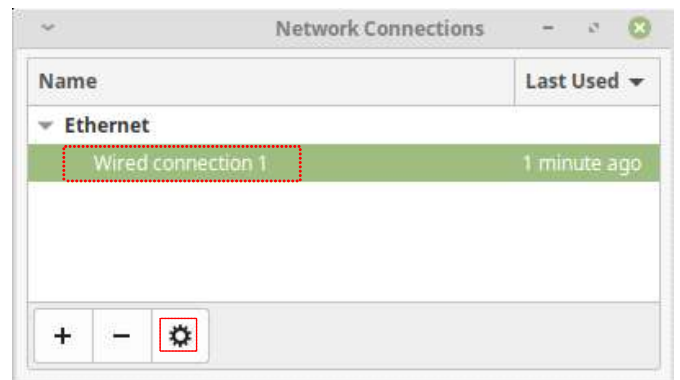
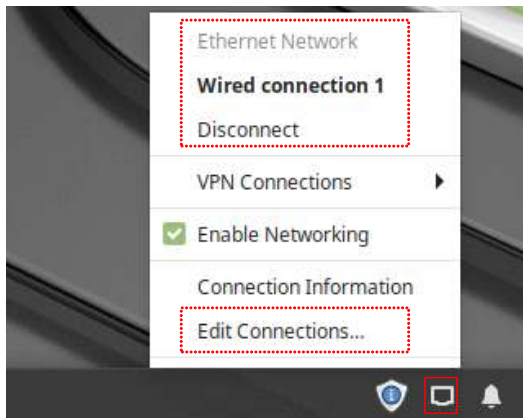


장치명	네트워크 인터페이스	IP주소	용도
Client	enp0s3(Ethernet0)	192.168.1.10/24	GNS용
	enp0s8(Ethernet1)	NAT	인터넷용
관리자 계정 정보(ID/Password) : root / sunrin, sunrin / sunrin			
배포처 : <a href="https://linuxmint.com/">https://linuxmint.com/</a>			
설치 ISO : linuxmint-19.1-xfce-64bit.iso			

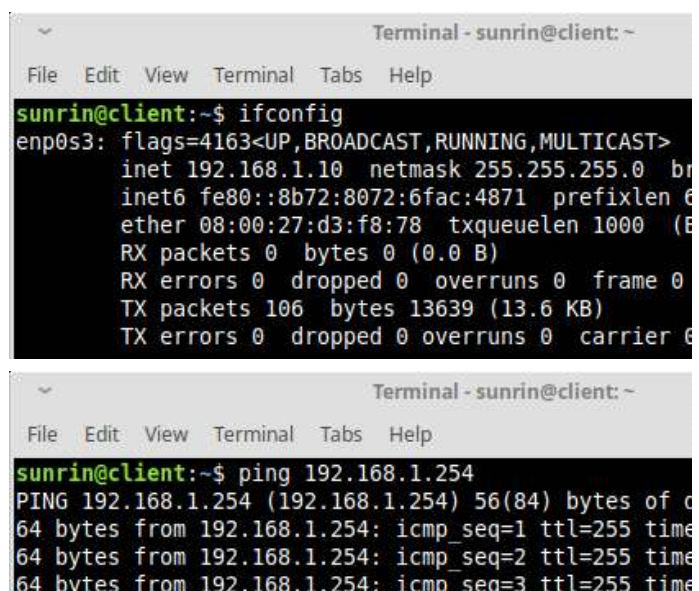
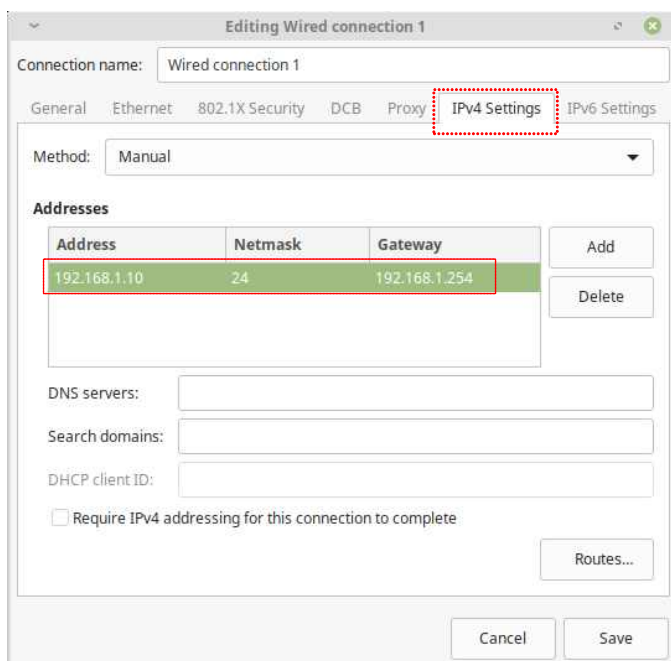
※ 사용한 배포판은 실습 목적 및 호스트 시스템의 사양에 따라 적절하게 선정한다.

토폴로지에 Client를 추가하고 부팅하여 네트워크 설정을 토폴로지의 정보에 맞게 변경한다. 네트워크 설정 방법은 대부분의 리눅스 배포판이 비슷하지만, 아이콘의 위치나 모양 등은 조금씩 다를 수 있다.

- Client의 네트워크 설정을 위해 화면 우측 하단의 아이콘을 클릭한다. 현재 Ethernet Network는 [Wired connection 1] 활성화 된 것을 확인할 수 있다.  
[Edit Connections] 아이콘을 클릭하여 네트워크 연결을 설정한다.
- [Wired connection 1]을 선택 후, 하단의 아이콘을 클릭하여 네트워크 정보를 편집한다.

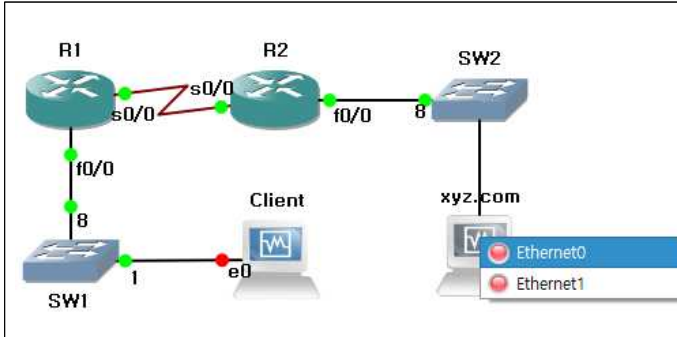


- 여러 탭 중 [IPv4 Settings]를 선택하고, 네트워크 정보를 참고하여 IP주소를 설정한다.
- ifconfig, ping 명령을 이용해 네트워크 설정을 확인한다.



## 4. xyz.com - 네트워크 설정

[네트워크 구성도]를 참고하여 다음과 같이 토폴로지에 xyz.com을 추가하고 SW2와 연결한다. 가상머신의 생성, GNS 등록 등은 [I 수업 준비]를 참고한다. xyz.com 가상머신에 대한 정보를 참고하여 네트워크 설정을 변경한다. 네트워크 설정 변경은 선택한 리눅스 배포판의 설정 방법을 참고한다.



장치명	네트워크 인터페이스	IP주소	용도
xyz.com	enp0s3(Ethernet0)	125.241.100.10/24	GNS용
	enp0s8(Ethernet1)	NAT	인터넷용
관리자 계정 정보(ID/Password) : root / sunrin, sunrin / sunrin 배포처 : <a href="https://ubuntu.com/download/server">https://ubuntu.com/download/server</a> 버전 : Ubuntu Server 18.04.4 LTS 설치 ISO : ubuntu-18.04.3-live-server-amd64.iso			

※ 사용한 배포판은 실습 목적 및 호스트 시스템의 사양에 따라 적절하게 선정한다.

xyz.com을 서버로 활용하기 위해 여러 가지 패키지를 설치해야 한다. xyz.com에 필요한 패키지를 설치하는 과정은 다음과 같다. 패키지 설치를 위한 NAT 설정 및 활용은 [I 수업 준비 - 04 GNS에 VirtualBox 가상머신 등록하기, 16쪽~20쪽]을 참고한다.

네트워크 설정 → enp0s3 down → enp0s8 up → 패키지 설치 또는 업데이트 → enp0s8 down → enp0s3 up

① ip link 또는 ifconfig -a 명령을 통해 네트워크 인터페이스 정보를 확인한다.

```
root@xyz:~# ip link
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: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP mode DEFAULT group default qlen 1000
    link/ether 08:00:27:d6:4d:0a brd ff:ff:ff:ff:ff:ff
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP mode DEFAULT group default qlen 1000
    link/ether 08:00:27:9b:f9:7d brd ff:ff:ff:ff:ff:ff
```

② 위의 네트워크 정보를 참고하여 IP주소 설정을 하고, 패키지 설치에 사용할 인터페이스만 활성화한다.

```
root@xyz:~# vi /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.
# 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:
    enp0s3:
      dhcp4: no
      addresses: [125.241.100.10/24]
      gateway4: 125.241.100.254
      nameservers:
        addresses: [8.8.8.8]
    enp0s8:
      dhcp4: true

  version: 2

root@xyz:~# netplan apply
root@xyz:~# ifconfig enp0s3 down
root@xyz:~# ifconfig
enp0s8: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.3.15 netmask 255.255.255.0 broadcast 10.0.3.255
    inet6 fe80::a00:27ff:fe9b:f97d prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:9b:f9:7d txqueuelen 1000 (Ethernet)
    RX packets 59 bytes 9823 (9.8 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 90 bytes 8457 (8.4 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@xyz:~# ping www.google.com
PING www.google.com (172.217.26.4) 56(84) bytes of data:
64 bytes from nrt20s02-in-f4.1e100.net (172.217.26.4): icmp_seq=1 ttl=54 time=70.4 ms
```



## 12 Telnet, FTP, HTTP 설정

### 1. xyz.com – telnet

서버에 원격으로 접속하기 위한 방법으로 telnet을 사용할 수 있다. 오래전부터 사용되는 방법이지만 telnet을 통해 전송되는 데이터가 평문이기 때문에 스니핑 등의 공격으로 중요한 정보가 노출될 수 있다. 최근에는 서버에 원격으로 접속할 때 telnet 보다는 SSH를 주로 사용한다. 실습에서는 SSH와의 비교를 위해 telnet을 사용하며, 세부적인 설정은 필요에 따라 추가한다.

- ① apt install telnetd -y 명령을 이용해 telnet을 설치한다.

```
root@xyz:~# apt install telnetd -y
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  telnetd
0 upgraded, 1 newly installed, 0 to remove and 65 not upgraded.
Need to get 39.3 kB of archives.
After this operation, 110 kB of additional disk space will be used.
Get:1 http://kr.archive.ubuntu.com/ubuntu bionic/universe amd64 telnetd amd64 0.17-41 [39.3 kB]
```

- ② systemctl status inetd 명령을 이용해 서비스 상태를 확인한다.

```
root@xyz:~# systemctl status inetd
• inetd.service - Internet superserver
  Loaded: loaded (/lib/systemd/system/inetd.service; enabled; vendor preset: enabled)
  Active: active (running) since Tue 2020-02-25 13:21:10 UTC; 31s ago
    Docs: man:inetd(8)
  Main PID: 719 (inetd)
    Tasks: 1 (limit: 1108)
  CGroup: /system.slice/inetd.service
          └─719 /usr/sbin/inetd
```

- ③ 설치 및 실행을 확인했으니 GNS 내의 다른 장치에서 접속할 수 있도록 enp0s3만 활성화한다.

```
root@xyz:~# ifconfig enp0s8 down
root@xyz:~# ifconfig enp0s3 up
```

- ④ Client에서 터미널을 이용하여 xyz.com(125.241.100.10)으로 접속한다.

```
sunrin@client:~$ telnet 125.241.100.10
Trying 125.241.100.10...
Connected to 125.241.100.10.
Escape character is '^]'.
Ubuntu 18.04.3 LTS
xyz login: sunrin
Password:
Last login: Tue Feb 25 13:12:04 UTC 2020 on pts/0
Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 4.15.0-88-generic x86_64)
```

systemctl status inetd 명령어로 상태를 확인한다. inetd – in.telnetd가 실행되었으며, 192.168.1.10과 연결된 상태임을 확인할 수 있다.

```
sunrin@xyz:~$ systemctl status inetd
• inetd.service - Internet superserver
  Loaded: loaded (/lib/systemd/system/inetd.service; enabled; vendor preset: en
  Active: active (running) since Tue 2020-02-25 13:21:10 UTC; 8min ago
    Docs: man:inetd(8)
  Main PID: 719 (inetd)
    Tasks: 2 (limit: 1108)
  CGroup: /system.slice/inetd.service
          └─719 /usr/sbin/inetd
            └─1055 in.telnetd:

Feb 25 13:21:09 xyz systemd[1]: Starting Internet superserver...
Feb 25 13:21:10 xyz systemd[1]: Started Internet superserver.
Feb 25 13:27:53 xyz in.telnetd[1055]: connect from 192.168.1.10 (192.168.1.10)
Feb 25 13:28:03 xyz telnetd[1055]: doit: getnameinfo: Success
Feb 25 13:28:08 xyz login[1059]: pam_unix(login:session): session opened for use
```



ps tree 명령어로 inetd -> in.telnetd -> login -> bash -> ps tree 프로세스가 실행된 것을 확인할 수 있다.

```
sunrin@xyz:~$ ps tree
systemd--accounts-daemon--2*[{accounts-daemon}]
      |
      |--atd
      |--cron
      |--dbus-daemon
      |--inetd--in.telnetd--login--bash--ps tree
      |--login--bash
      |--lvm2d
      |--lxcfs--2*[{lxcfs}]
      |--networkd-dispatcher--{networkd-dispatcher}
      |--polkitd--2*[{polkitd}]
      |--rsyslogd--3*[{rsyslogd}]
      |--snapd--8*[{snapd}]
      |--sshd
      |--2*[systemd--(sd-pam)]
      |--systemd-journald
      |--systemd-logind
      |--systemd-networkd
      |--systemd-resolved
      |--systemd-timesyn--{systemd-timesyn}
      |--systemd-udev
      |--unattended-upgr--{unattended-upgr}
```

## 2. xyz.com - ftp

서버와 클라이언트 간에 파일을 주고받기 위한 방법으로 FTP를 사용할 수 있다. FTP는 Telnet과 비슷하게 접속할 수 있으며, 파일을 주고받기 위한 명령을 사용할 수 있다. 실습에서는 vsftpd를 사용하며, 세부적인 설정은 필요에 따라 추가한다.

- ① 패키지 설치를 위해 인터넷 접속을 위한 enp0s8만 활성화한다.

```
root@xyz:~# ifconfig enp0s3 down
root@xyz:~# ifconfig enp0s8 up
```

- ② apt install telnetd -y 명령을 이용해 telnet을 설치한다.

```
root@xyz:~# apt install vsftpd
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  ssl-cert
Suggested packages:
  openssl-blacklist
The following NEW packages will be installed:
  ssl-cert vsftpd
0 upgraded, 2 newly installed, 0 to remove and 65 not upgraded.
Need to get 132 kB of archives.
After this operation, 398 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
```

- ③ systemctl status vsftpd 명령을 이용해 서비스 상태를 확인한다.

```
root@xyz:~# systemctl status vsftpd
● vsftpd.service - vsftpd FTP server
   Loaded: loaded (/lib/systemd/system/vsftpd.service; enabled; vendor preset: enabled)
   Active: active (running) since Tue 2020-02-25 14:03:44 UTC; 3min 45s ago
 Main PID: 1512 (vsftpd)
   Tasks: 1 (limit: 1108)
  CGroup: /system.slice/vsftpd.service
          └─1512 /usr/sbin/vsftpd /etc/vsftpd.conf

Feb 25 14:03:44 xyz systemd[1]: Starting vsftpd FTP server...
Feb 25 14:03:44 xyz systemd[1]: Started vsftpd FTP server.
```

- ④ 설치 및 실행을 확인했으니 GNS 내의 다른 장치에서 접속할 수 있도록 enp0s3만 활성화한다.

```
root@xyz:~# ifconfig enp0s8 down
root@xyz:~# ifconfig enp0s3 up
```

⑤ Client에서 터미널을 이용하여 xyz.com(125.241.100.10)으로 접속한다.

```
sunrin@client:~$ ftp 125.241.100.10
Connected to 125.241.100.10.
220 (vsFTPd 3.0.3)
Name (125.241.100.10:sunrin): sunrin
331 Please specify the password.
Password:
230 Login successful.
```

### 과제 - 1

ftp도 telnet와 마찬가지로 평문으로 데이터를 전송하기 때문에 보안상 취약하다. 이를 보완한 SFTP(Secure File Transfer Protocol)을 활용할 수 있다.

다음 사용자가 xyz.com에 SFTP를 사용할 수 있도록 구성하고, 수행 과정을 아래에 캡처하여 붙여넣기 하시오.

ID	Password	home directory	home directory 접근권한	비고
ftpuser	sunrin	/home/ftpuser	700 (RWX --- ---)	다른 사항은 기본값

#### SFTP(Secure File Transfer Protocol)

회할 수 있는 데이터 스트림을 통해 파일 접근, 파일 전송, 파일 관리를 제공하는 네트워크 프로토콜이다. 국제 인터넷 표준화 기구(IETF)가 보안 파일 전송 기능을 제공할 목적으로 시큐어 셸 프로토콜 (SSH) 버전 2.0의 확장으로 설계하였다.

#### SFTP 설정

```
root@xyz:~# vi /etc/ssh/sshd_config
```

```
# SFTP Configuration_
Match group sftp
ChrootDirectory /home
X11Forwarding no
AllowTcpForwarding no
ForceCommand internal-sftp
-- INSERT --
```

129

```
root@xyz:~# service ssh restart
```

#### 사용자 및 그룹 추가, 사용자 권한 설정

```
root@xyz:~# addgroup sftp
Adding group `sftp' (GID 1001) ...
Done.
root@xyz:~# useradd -m ftpuser -g sftp
root@xyz:~# passwd ftpuser
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
root@xyz:~# chmod 700 /home/ftpuser/
```

#### Client에서 ftpuser로 SFTP 접속 결과

```
sunrin@client:~$ sftp ftpuser@125.241.100.10
The authenticity of host '125.241.100.10 (125.241.100.10)' can't be established.
ECDSA key fingerprint is SHA256:xsBHnTHW+VQ8Btqq0E93LBd0ubbdqeXwthHA7uC4Gfw.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '125.241.100.10' (ECDSA) to the list of known hosts.
ftpuser@125.241.100.10's password:
Connected to 125.241.100.10.
sftp> █
```

#### SFTP 접속 상태에서의 ssh 서비스 상태 확인

```
sunrin@xyz:~$ systemctl status sshd
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enab
   Active: active (running) since Tue 2020-02-25 15:02:49 UTC; 16min ago
   Process: 1871 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
   Main PID: 1882 (sshd)
   Tasks: 1 (limit: 1108)
   CGroup: /system.slice/ssh.service
           └─1882 /usr/sbin/sshd -D

Feb 25 15:02:49 xyz systemd[1]: Starting OpenBSD Secure Shell server...
Feb 25 15:02:49 xyz sshd[1882]: Server listening on 0.0.0.0 port 22.
Feb 25 15:02:49 xyz sshd[1882]: Server listening on :: port 22.
Feb 25 15:02:49 xyz systemd[1]: Started OpenBSD Secure Shell server.
Feb 25 15:18:53 xyz sshd[1937]: Accepted password for ftpuser from 192.168.1.10
Feb 25 15:18:53 xyz sshd[1937]: pam_unix(sshd:session): session opened for user
```

## 퀴즈 - 1

xyz.com(125.241.100.10)으로 SFTP 접속을 하는 과정에서 표시된 것과 같은 과정을 거쳤다. 이 과정은 어떤 과정인지 설명하시오.

```
sunrin@client:~$ sftp ftpuser@125.241.100.10
The authenticity of host '125.241.100.10 (125.241.100.10)' can't be established.
ECDSA key fingerprint is SHA256:xsBHntHW+VQ8Btqq0E93LBd0ubbdqeXwthHA7uC4Gfw.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '125.241.100.10' (ECDSA) to the list of known hosts.
ftpuser@125.241.100.10's password:
Connected to 125.241.100.10.
sftp>
```

SFTP는 SSH를 기반으로 동작한다. SFTP의 동작과정에서 xyz.com의 공개키를 확인하고, 이를 이용하여 암호화 통신을 하게 된다.

## 3. xyz.com - http

HTTP 서비스를 위해 NGiNX, Lighttpd, Apache 등을 이용할 수 있다. 이번 실습에서는 Apache를 이용하여 HTTP 서비스를 설정하며 세 부적인 설정은 필요에 따라 추가한다.

- ① 패키지 설치를 위해 인터넷 접속을 위한 enp0s8만 활성화한다.

```
root@xyz:~# ifconfig enp0s3 down
root@xyz:~# ifconfig enp0s8 up
```

- ② apt install apache2 명령을 이용해 apache를 설치한다.

```
root@xyz:~# apt install apache2
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  apache2-bin apache2-data apache2-utils libapr1 libaprutil1 libaprutil1-dbd-sqlite3
  libaprutil1-ldap liblua5.2-0
Suggested packages:
  www-browser apache2-doc apache2-suexec-pristine | apache2-suexec-custom
The following NEW packages will be installed:
  apache2 apache2-bin apache2-data apache2-utils libapr1 libaprutil1 libaprutil1-dbd-sqlite3
  libaprutil1-ldap liblua5.2-0
0 upgraded, 9 newly installed, 0 to remove and 65 not upgraded.
Need to get 1,713 kB of archives.
After this operation, 6,917 kB of additional disk space will be used.
Do you want to continue? [Y/n]
```

- ③ systemctl status vsftpd 명령을 이용해 서비스 상태를 확인한다.

```
root@xyz:~# systemctl status apache2
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor preset: enabled)
   Drop-In: /lib/systemd/system/apache2.service.d
            └─apache2-systemd.conf
   Active: active (running) since Tue 2020-02-25 15:41:07 UTC; 22min ago
   Main PID: 2767 (apache2)
     Tasks: 55 (limit: 1108)
    CGroup: /system.slice/apache2.service
            └─2767 /usr/sbin/apache2 -k start
               2769 /usr/sbin/apache2 -k start
               2770 /usr/sbin/apache2 -k start

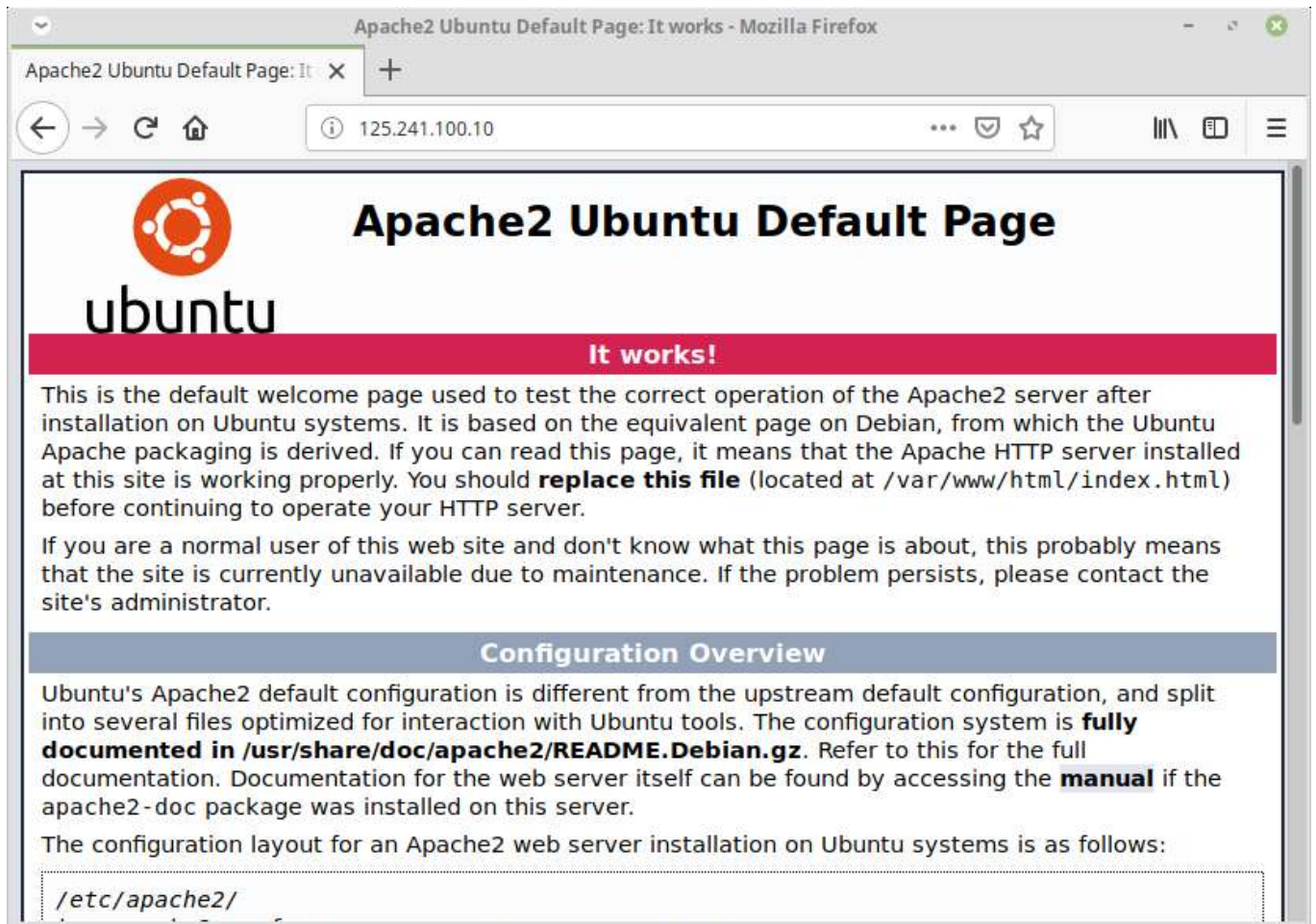
Feb 25 15:41:07 xyz systemd[1]: Starting The Apache HTTP Server...
Feb 25 15:41:07 xyz apachectl[2744]: AH00558: apache2: Could not reliably determine the server's ful
Feb 25 15:41:07 xyz systemd[1]: Started The Apache HTTP Server.
```

※ 시스템 상황에 따라 방화벽 설정 변경이 필요할 수 있다.

- ④ 설치 및 실행을 확인했으니 GNS 내의 다른 장치에서 접속할 수 있도록 enp0s3만 활성화한다.

```
root@xyz:~# ifconfig enp0s8 down
root@xyz:~# ifconfig enp0s3 up
```

⑤ Client에서 웹 브라우저를 이용하여 xyz.com(125.241.100.10)으로 접속한다.



## 과제 - 2

다음 정보를 참고하여 xyz.com(125.241.100.10)의 index.html 파일을 수정하고, Client에서 웹 브라우저로 접속한 화면을 캡처하여 붙여넣기 하시오.

www home directory	index.html 포함 내용	비고
/var/www/html/index.html	host name : xyz.com ip address : 125.241.100.10	기본 HTML Tag만 사용

index.html 파일 내용

```
<html>
<head><title>xyz.com</title></head>
<body>hostname : xyz.com<br><br>
      ip address : 125.241.100.10<br>
</body>
</html>
```

Client에서 웹 브라우저로  
접속한 결과





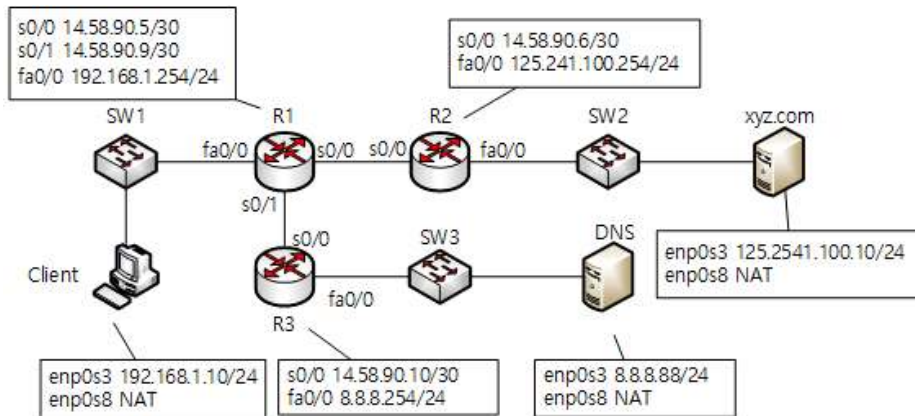
## 13 DNS 설정

앞에서 HTTP, FTP, Telnet 서비스를 설정하였고, 서버의 IP주소를 이용하여 해당 서비스를 이용할 수 있었다. 하지만 IP주소는 사용자들이 기억하기 불편하여 주로 도메인 이름을 사용한다. 도메인 이름을 사용하기 위해서는 2가지의 설정을 해야 한다. 첫 번째는 DNS 서버 설정이다. 두 번째는 설정된 DNS 서버의 IP주소를 클라이언트의 네트워크 설정에 반영하는 것이다.

### 1. 실습용 네트워크 토폴로지 및 호스트 구성

위에서 구성한 토폴로지에 아래와 같이 라우터, 스위치, DNS 서버를 추가한다. 라우터 설정 및 DNS 서버 추가는 위의 [11 서버 구축 실습용 네트워크 토폴로지 구축]을 참고한다.

#### ■ 네트워크 구성도



장치명	포트	IP주소	비고
R1	s0/0	14.58.90.5/30	
	s0/1	14.58.90.9/30	
	fa0/1	192.168.1.254/24	
R2	s0/0	14.58.90.6/30	
	fa0/0	125.241.100.254/24	
R3	s0/0	14.58.90.10/30	
	fa0/0	8.8.8.254/24	

장치명	포트	IP주소	비고
Client	enp0s3	192.168.1.10/24	클라이언트
DNS	enp0s3	8.8.8.88/24	DNS 서버
xyz.com	enp0s3	125.241.100.10/24	다양도 서버

관리자 계정 정보 : root / sunrin

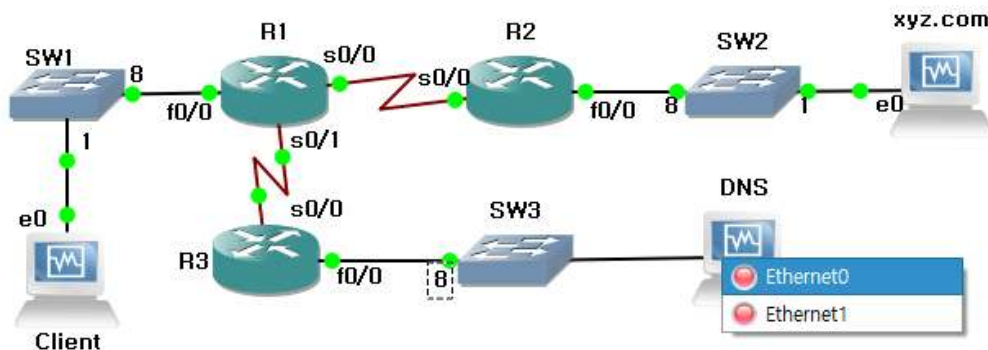
★ s0/0 = Serial0/0 ★ fa0/0 = fastethernet0/0

DNS 실습 과정은 다음과 같으며, 선택한 배포판에 따라 세부 과정은 달라질 수 있다. 세부적인 설정은 배포판의 DNS 설정 메뉴얼을 참고한다.

네트워크 설정 → bind 설치 → DNS서버 환경 설정 → zone 파일 생성 → 방화벽 설정 → 호스트에서 접속

### 2. DNS 추가

[네트워크 구성도]를 다음과 같이 토폴로지에 라우터 R3, 스위치 SW3, dns를 추가한다. 가상머신의 생성, GNS 등록 등은 [I 수업 준비]를 참고한다. dns 가상머신에 대한 정보를 참고하여 네트워크 설정을 변경한다. 네트워크 설정 변경은 선택한 리눅스 배포판의 설정 방법을 참고한다.



장치명	네트워크 인터페이스	IP주소	용도	관리자 계정 정보(ID/Password) : root / sunrin, sunrin / sunrin
dns	enp0s3(Ethernet0)	8.8.8.88/24	GNS용	배포처 : <a href="https://ubuntu.com/download/server">https://ubuntu.com/download/server</a>
	enp0s8(Ethernet1)	NAT	인터넷용	버전 : Ubuntu Server 18.04.4 LTS 설치 ISO : ubuntu-18.04.3-live-server-amd64.iso

※ 사용한 배포판은 실습 목적 및 호스트 시스템의 사양에 따라 적절하게 선정한다.

## 가. 네트워크 설정

- ① 라우터 R1의 Serial0/1의 IP주소를 설정한다.

```
R1
R1(config)#interface serial 0/1
R1(config-if)#ip address 14.58.90.9 255.255.255.252
R1(config-if)#no shutdown
R1(config-if)#
*Mar 1 01:21:55.095: %LINK-3-UPDOWN: Interface Serial0/1, changed state to up
R1(config-if)#
*Mar 1 01:21:56.099: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1, changed state to up
R1(config-if)#do write
Building configuration...
[OK]
R1(config-if)#
```

- ② 라우터 R1의 라우팅을 설정한다.(RIP)

```
R1
R1(config)#router rip
R1(config-router)#network 14.58.90.8
R1(config-router)#do write
Building configuration...
[OK]
R1(config-router)#
```

- ③ 라우터 R3의 Fastethernet0/0, Serial0/0의 IP주소를 설정한다.

```
R3
R3(config)#interface fastethernet 0/0
R3(config-if)#ip address 8.8.8.254 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#
*Mar 1 00:56:26.575: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Mar 1 00:56:27.575: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
R3(config-if)#interface serial 0/0
R3(config-if)#ip address 14.58.90.10 255.255.255.252
R3(config-if)#no shutdown
R3(config-if)#
*Mar 1 00:57:13.747: %LINK-3-UPDOWN: Interface Serial0/0, changed state to up
R3(config-if)#
*Mar 1 00:57:14.751: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0, changed state to up
R3(config-if)#do write
Building configuration...
[OK]
R3(config-if)#
```

- ④ 라우터 R3의 라우팅을 설정한다.(RIP)

```
R3
R3(config)#router rip
R3(config-router)#version 2
R3(config-router)#no auto-summary
R3(config-router)#network 14.58.90.8
R3(config-router)#network 8.8.8.0
R3(config-router)#do write
Building configuration...
[OK]
R3(config-router)#
```

⑤ show ip route 명령을 통해 생성된 라우팅 테이블을 확인할 수 있다.

```

R3#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

8.0.0.0/24 is subnetted, 1 subnets
8.8.8.0 is directly connected, FastEthernet0/0
125.0.0.0/24 is subnetted, 1 subnets
125.241.100.0 [120/2] via 14.58.90.9, 00:00:02, Serial0/0
192.168.1.0/24 [120/1] via 14.58.90.9, 00:00:02, Serial0/0
14.0.0.0/30 is subnetted, 2 subnets
14.58.90.8 is directly connected, Serial0/0
14.58.90.4 [120/1] via 14.58.90.9, 00:00:02, Serial0/0

R3#

R2#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

8.0.0.0/24 is subnetted, 1 subnets
8.8.8.0 [120/2] via 14.58.90.5, 00:00:25, Serial0/0
125.0.0.0/24 is subnetted, 1 subnets
125.241.100.0 is directly connected, FastEthernet0/0
192.168.1.0/24 [120/1] via 14.58.90.5, 00:00:25, Serial0/0
14.0.0.0/30 is subnetted, 2 subnets
14.58.90.8 [120/1] via 14.58.90.5, 00:00:25, Serial0/0
14.58.90.4 is directly connected, Serial0/0

R2#

R1#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

8.0.0.0/24 is subnetted, 1 subnets
8.8.8.0 is directly connected, FastEthernet0/0
125.0.0.0/24 is subnetted, 1 subnets
125.241.100.0 is directly connected, FastEthernet0/0
192.168.1.0/24 is directly connected, FastEthernet0/0
14.0.0.0/30 is subnetted, 2 subnets
14.58.90.8 is directly connected, Serial0/1
14.58.90.4 is directly connected, Serial0/0

R1#
  
```

라우터 R1, R2, R3는 직접 연결된 네트워크는 C로 표시하며, Rip를 통해 확인한 라우팅 경로는 레코드 앞에 R로 표시되어 있다. 라우팅 설정이 완료되고 일정 시간이 후에 라우터끼리 서로 라우팅 테이블을 교환하여 모든 네트워크에 대한 라우팅 테이블을 구성한 것을 확인할 수 있다.

#### 나. DNS 서버 네트워크 설정

dns를 서버로 활용하기 위해 여러 가지 패키지를 설치해야 한다. dns에 필요한 패키지를 설치하는 과정은 다음과 같다. 패키지 설치를 위한 NAT 설정 및 활용은 [I 수업 준비 - 04 GNS에 VirtualBox 가상머신 등록하기, 16쪽~20쪽]을 참고한다.

네트워크 설정 → enp0s3 down → enp0s8 up → 패키지 설치 또는 업데이트 → enp0s8 down → enp0s3 up

① ip link 또는 ifconfig -a 명령을 통해 네트워크 인터페이스 정보를 확인한다.

```

root@dns:~# ip link
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: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP mode DEFAULT group default qlen 1000
    link/ether 08:00:27:82:37:1e brd ff:ff:ff:ff:ff:ff
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP mode DEFAULT group default qlen 1000
    link/ether 08:00:27:3b:5f:37 brd ff:ff:ff:ff:ff:ff
root@dns:~#
  
```

② 위의 네트워크 정보를 참고하여 IP주소 설정을 하고, 패키지 설치에 사용할 인터페이스만 활성화한다.

```
root@dns:~# vi /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.
# 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:
    enp0s3:
      addresses: [8.8.8.88/24]
      gateway4: 8.8.8.254
      nameservers:
        addresses: [8.8.8.88]
      dhcp4: no
    enp0s8:
      dhcp4: yes

  version: 2
```

```
root@dns:~# netplan apply
```

```
root@dns:~# ifconfig enp0s3 down
```

```
root@dns:~# ifconfig
enp0s8: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.3.15 netmask 255.255.255.0 broadcast 10.0.3.255
    inet6 fe80::a00:27ff:fe3b:5f37 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:3b:5f:37 txqueuelen 1000 (Ethernet)
    RX packets 14 bytes 2106 (2.1 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 29 bytes 2626 (2.6 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
```

③ ping을 이용하여 외부 인터넷으로 접속 상태를 확인한다.

```
root@dns:~# ping www.google.com
PING www.google.com (172.217.175.4) 56(84) bytes of data.
64 bytes from nrt20s18-in-f4.1e100.net (172.217.175.4): icmp_seq=1 ttl=54 time=39.7 ms
64 bytes from nrt20s18-in-f4.1e100.net (172.217.175.4): icmp_seq=2 ttl=54 time=37.4 ms
64 bytes from nrt20s18-in-f4.1e100.net (172.217.175.4): icmp_seq=3 ttl=54 time=37.1 ms
```

#### 다. DNS 설정

① apt install bind9 명령을 이용해 bind9을설치한다.

```
root@dns:~# apt install bind9
Reading package lists... Done
Building dependency tree
Reading state information... Done
Suggested packages:
  resolvconf
The following NEW packages will be installed:
  bind9
0 upgraded, 1 newly installed, 0 to remove and 86 not upgraded.
Need to get 398 kB of archives.
After this operation, 1,918 kB of additional disk space will be used.
Get:1 http://kr.archive.ubuntu.com/ubuntu bionic-updates/main amd64 bind9 amd64 1:9.11.3+dfsg-1ubuntu1.11 [398 kB]
```

② systemctl status bind9 명령을 이용해 서비스 상태를 확인한다.

```
root@dns:~# systemctl status bind9
● bind9.service - BIND Domain Name Server
   Loaded: loaded (/lib/systemd/system/bind9.service; enabled; vendor preset: enabled)
   Active: active (running) since Wed 2020-02-26 20:47:03 KST; 1min 17s ago
     Docs: man:named(8)
   Main PID: 1869 (named)
    Tasks: 4 (limit: 1108)
   CGroup: /system.slice/bind9.service
           └─1869 /usr/sbin/named -f -u bind
```



③ 설치 및 실행을 확인했으니 GNS 내의 다른 장치에서 접속할 수 있도록 enp0s3만 활성화한다.

```
root@dns:~# ifconfig enp0s8 down
root@dns:~# ifconfig enp0s3 up
```

④ vi /etc/bind/named.conf.options로 설정 파일을 편집한다.

아래의 옵션 중 "recursion no" 항목은 이 서버에 정의되지 않은 도메인 요청을 거부하도록 설정한 것이다. 일반적인 설정은 "recursion yes"로 설정하고, forwarders에 다른 네임 서버를 지정한다. 현재 환경에서는 다른 네임서버가 없으므로 아래와 같이 설정하였다.

```
root@dns:~# vi /etc/bind/named.conf.options
```

```
options {
    directory "/var/cache/bind";

    // If there is a firewall between you and nameservers you want
    // to talk to, you may need to fix the firewall to allow multiple
    // ports to talk.  See http://www.kb.cert.org/vuls/id/800113

    // If your ISP provided one or more IP addresses for stable
    // nameservers, you probably want to use them as forwarders.
    // Uncomment the following block, and insert the addresses replacing
    // the all-0's placeholder.

    // forwarders {
    //     0.0.0.0;
    // };

    //=====
    // If BIND logs error messages about the root key being expired,
    // you will need to update your keys.  See https://www.isc.org/bind-keys
    //=====
    dnssec-validation auto;

    auth-nxdomain no;    # conform to RFC1035
    listen-on-v6 { any; };

    //recursion yes; # if requested not defined this dns server, this server request to forward
    recursion no;

    listen-on port 53 { any; };
    allow-query { any; };
    // forwarders { 8.8.8.254; }; # another dns server list, but this case not useful
};
```

⑤ vi /etc/bind/named.conf.local로 zone 파일 경로와 파일명을 지정한다. xyz.com, abc.com에 대해 정방향, 역방향 모두 지정하였다.

```
root@dns:~# vi /etc/bind/named.conf.local
```

```
// forward zone config

zone "abc.com" IN {
    type master;
    file "/etc/bind/abc.com.zone";
};

zone "xyz.com" IN {
    type master;
    file "/etc/bind/xyz.com.zone";
};

// backward zone config

zone "100.100.210.in-addr.arpa" IN {
    type master;
    file "/etc/bind/abc.com.rev";
};

zone "100.241.125.in-addr.arpa" IN {
    type master;
    file "/etc/bind/xyz.com.rev";
};
```

- ⑥ vi /etc/bind/xyz.com.zone 로 다음과 같이 정방향 조회 영역을 생성한다.

```
root@dns:~# vi /etc/bind/xyz.com.zone

$TTL      86400
@ IN SOA xyz.com. root.xyz.com. (
    2001202 ; Serial
    14400   ; Refresh
    14400   ; Retry
    1209600 ; Expire
    86400   ) ; Negative Cache TTL

; dns server
@ IN NS ns.xyz.com.

; ip address of dns server
ns IN A 8.8.8.88

; A Record list
@ IN A 125.241.100.10
www IN A 125.241.100.10
```

- ⑦ vi /etc/bind/xyz.com.zone.rev 로 다음과 같이 역방향 조회 영역을 생성한다.

```
root@dns:~# vi /etc/bind/xyz.com.zone.rev _

$TTL      86400
@ IN SOA xyz.com. root.xyz.com. (
    2001202 ; serial
    3600    ; refresh
    900     ; retry
    604800  ; expire
    86400   ; minium ttl
)

; dns server
@ IN NS ns.xyz.com.

; ip address of dns server
88 IN PTR ns.xyz.com.

; A Record list
10 IN PTR www.xyz.com.
```

- ⑧ 구문 오류를 테스트한다. 오류가 있는 경우 오류 사항을 확인하여 수정한다.

```
root@dns:~# named-checkconf
root@dns:~# named-checkzone xyz.com /etc/bind/xyz.com.zone
zone xyz.com/IN: loaded serial 2001202
OK

root@dns:~# systemctl reload bind9
```

- ⑩ Client의 네트워크 설정에서 DNS servers에 8.8.8.88을 추가하고, nslookup www.xyz.com으로 네임서버의 반환값이 올바른지 확인한다. 웹브라우저에서 IP주소가 아닌 www.xyz.com으로 접속한다.

```
sunrin@client:~$ nslookup www.xyz.com
Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
Name:   www.xyz.com
Address: 125.241.100.10
```



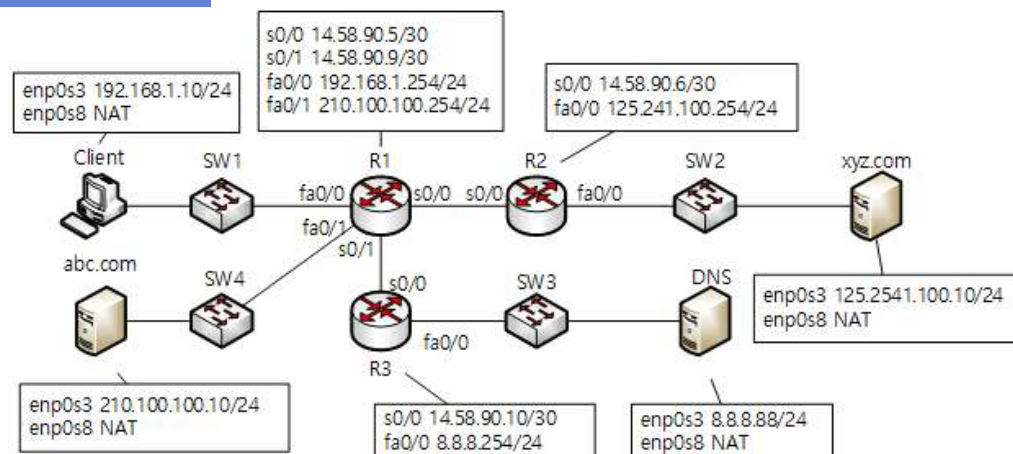
### 과제 - 3

위의 DNS 설정 중 /etc/bind/named.conf.local에서 xyz.com 뿐만 아니라 abc.com.zone, abc.com.zone.rev 파일을 지정하였다. 다음 정보를 참고하여 abc.com.zone, abc.com.zone.rev 파일을 생성하고, nslookup www.abc.com 명령으로 확인하시오.

장치명	IP주소	Gateway주소
abc.com	210.100.100.10/24	210.100.100.254

ls /etc/bind/abc* 명령 결과	<pre> root@dns:~# ls /etc/bind/ abc.com.zone      db.0      db.empty  named.conf      named.conf.options  xyz abc.com.zone.rev  db.127    db.local  named.conf.default-zones  rndc.key            z bind.keys         db.255    db.root   named.conf.local  xyz.com.zone        zo </pre>
cat /etc/bind/abc.com.zone 명령 결과	<pre> root@dns:~# cat /etc/bind/abc.com.zone \$TTL      86400 @ IN SOA abc.com. root.abc.com. (         2001201 ; Serial         14400 ; Refresh         14400 ; Retry         1209600 ; Expire         86400 ) ; Negative Cache TTL  ; dns server @ IN NS ns.abc.com.  ; ip address of dns server ns IN A 8.8.8.88  ; A Record list @ IN A 210.100.100.10 www IN A 210.100.100.10 </pre>
cat /etc/bind/abc.com.zone.rev 명령 결과	<pre> root@dns:/etc/bind# cat abc.com.zone.rev \$TTL      86400 @ IN SOA abc.com. root.abc.com. (         2001201 ; serial         3600 ; refresh         900 ; retry         604800 ; expire         86400 ; minium ttl )  ; dns server @ IN NS ns.abc.com.  ; ip address of dns server 88 IN PTR ns.abc.com.  ; A Record list 10 IN PTR www.abc.com. </pre>

### 직접해보기



왼쪽의 네트워크 토폴로지를 참고하여 abc.com을 추가하시오. abc.com에 telnet, ftp, sftp, http를 설정하시오. 라우터 R1의 fa0/0을 설정하고, RIP의 설정을 변경하시오.