리눅스 기초 강의자료
(2 일차)

목차 – 2일차

1. 리눅스 설치 시 관련 패키지 설명
2. Ext4 File System 설명
3. 리눅스 명령어 설명
4. Ubuntu Network 설정
5. 원격접속 (Telnet, SSH)
6. tcpdump 를 통한 패킷 스니핑

리눅스 설치 시 관련 패키지 설명

net-tools

설명:

- net-tools는 네트워크 관련 유틸리티를 제공하는 패키지
- 해당 패키지는 네트워크 인터페이스의 상태를 확인하고 관리하는데 사용

주요 기능:

- ifconfig: 네트워크 인터페이스의 정보를 표시하고 설정
- netstat: 네트워크 연결, 라우팅 테이블, 인터페이스 상태 등의 정보를 표시
- route: 라우팅 테이블을 보고 관리
- arp: ARP 캐시를 보고 관리

사용 예시:

- 네트워크 인터페이스의 IP 주소 확인: `ifconfig`
- 현재 열린 네트워크 연결 확인: `netstat -tuln`
- 라우팅 테이블 확인: `route -n`

리눅스 설치 시 관련 패키지 설명

openssh-server

설명:

- openssh-server는 SSH 프로토콜을 구현한 서버 측 소프트웨어.
- 해당 패키지는 원격 시스템에 안전하게 연결할 수 있도록 SSH 프로토콜을 지원하는 서버를 구축하게 도와줌

주요 기능:

- 원격 접속을 허용하여 안전한 쉘 및 명령 실행 환경을 제공
- 다양한 인증 방법을 지원하여 사용자 인증을 보호 (예: 패스워드, 공개 키 등)
- 데이터 암호화를 통해 네트워크 상에서 보안된 통신을 제공
- 파일 전송 및 관리를 위한 SCP (Secure Copy Protocol) 및 SFTP (SSH File Transfer Protocol) 서비스를 제공

리눅스 설치 시 관련 패키지 설명

vim

설명:
텍스트 편집기로, 다양한 키보드를 통해 작업을 할 때 사용

모드:
1) 기본 모드: 이 모드에서는 편집을 위한 명령을 입력 가능
2) 입력 모드: 텍스트를 입력할 수 있는 모드
3) 명령 모드: 명령을 실행할 수 있는 모드로, 파일 저장, 검색 및 치환 등의 작업을 수행

키 바인딩: Vim은 키보드로 다양한 작업을 수행할 수 있는 키 바인딩을 제공 (텍스트를 지우거나 복사하는 등의 작업 등)

문법 강조: Vim은 코드 편집을 위해 문법 강조 기능을 제공. 이 기능을 통해 프로그래머는 코드 구문을 빠르게 이해하고 수정 가능

터미널 및 GUI 지원: Vim은 터미널 기반 및 GUI 환경에서 모두 사용 가능 (사용자가 선호하는 환에서 사용 가능함을 의미)

자습서 및 문서: Vim은 다양한 자습서 및 문서가 존재하여 사용자가 Vim을 배우고 익힐 수 있도록 도와줌.

플러그인 및 확장성: Vim은 다양한 플러그인을 통해 기능을 확장 가능. (사용자가 필요에 따라 Vim을 사용자 정의하고 개선)

Vim은 초기에는 배우기 어려울 수 있지만, 익숙해지면 매우 효율적인 편집 도구로써 사용 가능

File System 설명

Linux File System 1

파일 시스템이란?

- 컴퓨터에서 파일이나 자료를 쉽게 발견 할 수 있도록 유지, 관리하는 방법
- 커널 영역에서 동작
- 파일을 빠르게 읽기, 쓰기, 삭제 등 기본적인 기능의 원활한 수행을 목적
    - HDD 메모리 관리와 용량의 효율적 사용

파일 시스템 특징

- 계층적 디렉터리 구조
- 디스크 파티션 별 한개씩 Mapping

File System 설명

Linux File System 2

OS 별 File System 종류

- Windows : FAT(FAT12/16/32,exFAT), NTFS
- Linux : ext(ext2/3/4)
- Mac OS : HFS, HFS+

File System 설명

Linux File System 3

ext4 (Extended 4 File System)

- 파일 시스템은 ext3 파일 시스템에 기초하여 여러사항이 개선
- 대용량 파일 시스템 및 대용량 파일 지원,
- 디스크 공간의 빠르고 효과적인 할당,
- 디렉토리에 있는 하위 디렉토리 수 제한 없음
- 빠른 파일 시스템 확인
- 강력한 저널링(Journaling) 기능이 포함
    - 일정부분을 기록을 위해 남겨두어 백업 및 복구 능력을 개선하는 방법
    - 시스템이 비정상 종료로 다시 부팅 될 때 **로그(Log)**에
      기록된 내용을 참고로 하여 파일 시스템을 복구

File System 설명

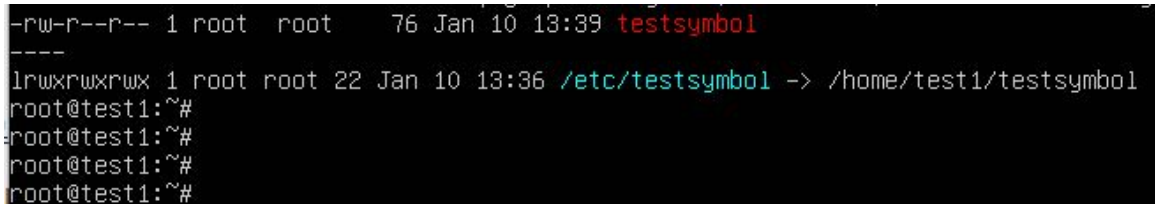
Linux File System 4

ext3 (Extended 3 File System)

- ext2 파일 시스템을 기반
- 저널링 파일시스템 기능 도입

ext2 (Extended 3 File System)

- 일반 파일, 디렉토리, 심볼릭 링크 (원본파일을 가리키는 바로가기 파일) 등을 포함하여 표준 Unix 파일 유형을 지원
- 255 자의 긴 파일 허용



< 심볼릭 링크 >

Ext4 File System 설명

Linux File System 5 – Ext Size 비교

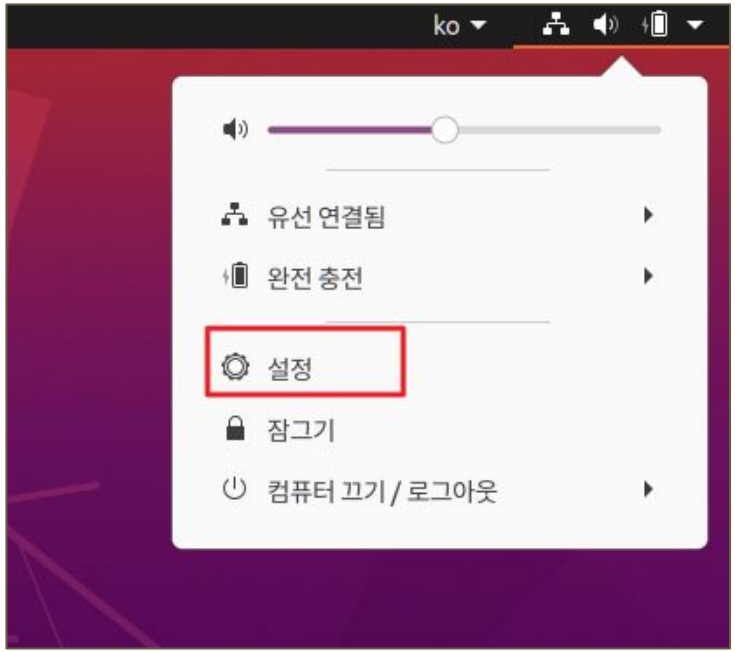
	Ext2	Ext3	Ext4
Introduced	in 1993	in 2001 (2.4.15)	in 2006 (2.6.19) in 2008 (2.6.28)
Max file size	16GB ~ 2TB	16GB ~ 2TB	16GB ~ 16TB
Max file system size	2TB ~ 32TB	2TB ~ 32TB	1EB
Feature	no Journaling	Journaling	Extents Multiblock allocation Delayed allocation

리눅스 명령어 설명

명령어	설명	명령어 사용법
cd	현재 작업 디렉토리를 변경합니다.	cd /home
sudo	슈퍼 유저 혹은 다른 사용자 권한으로 명령을 실행합니다.	sudo -s / sudo -i 등
mkdir	새로운 디렉토리를 생성합니다.	mkdir [directory]
rm	파일이나 디렉토리를 삭제합니다.	rm [file1]
rmdir	빈 디렉토리를 삭제합니다.	rmdir [directory]
cp	파일이나 디렉토리를 복사합니다.	cp [원본파일] [복사 또는 디렉토리 위치/파일명]
mv	파일이나 디렉토리를 이동하거나 이름을 변경합니다.	mv [원본파일] [변경 파일명 또는 디렉토리 위치/파일명]
ls	현재 디렉토리의 파일 및 디렉토리 목록을 표시합니다.	ls / ls -al
cat	파일의 내용을 화면에 출력합니다.	cat [출력파일]
grep	파일이나 텍스트에서 특정 패턴을 검색합니다.	cat /var/log | grep “특정문구”
tail	파일의 마지막 부분을 출력합니다.	tail -F /var/log/syslog
more	파일의 내용을 페이지 단위로 출력합니다	more /var/log/syslog
find	파일 시스템에서 파일이나 디렉토리를 검색합니다.	find / -name “*특정파일명*”
vi/vim	텍스트 편집기로서 다양한 편집 작업을 수행합니다.	vi [file1]
> (Redirection Operator)	명령어의 출력을 파일에 덮어씁니다.	echo 123 > a.txt
>> (Append Redirection Operator)	기존 파일의 끝에 새로운 내용을 추가합니다. 만약 파일이 존재하지 않는다면 새로운 파일을 생성	echo 123 >> a.txt
apt	패키지 관리자인 Advanced Package Tool을 사용하여 소프트웨어를 설치, 업데이트 및 제거합니다.	apt install / apt update / apt remove 등

Ubuntu Network 설정

1. Ubuntu 20.04 Desktop 의 Network 설정 (GUI) – 1

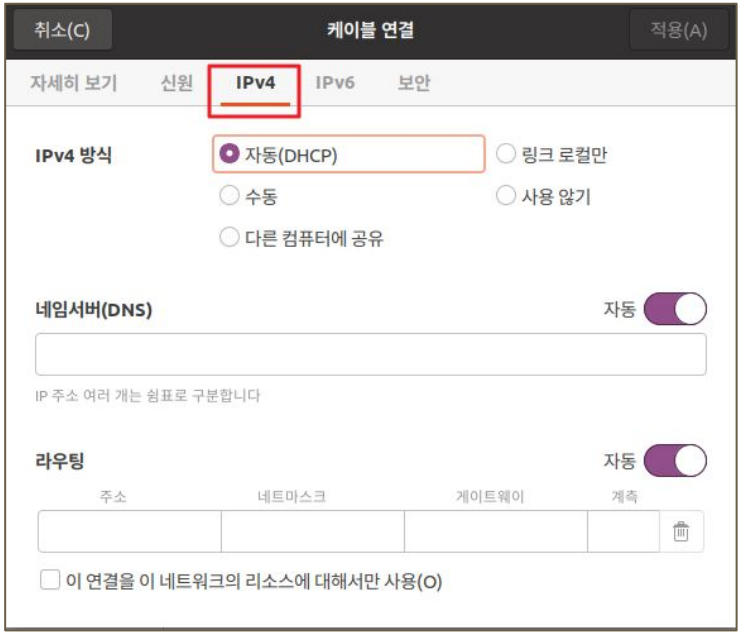


< 1 >

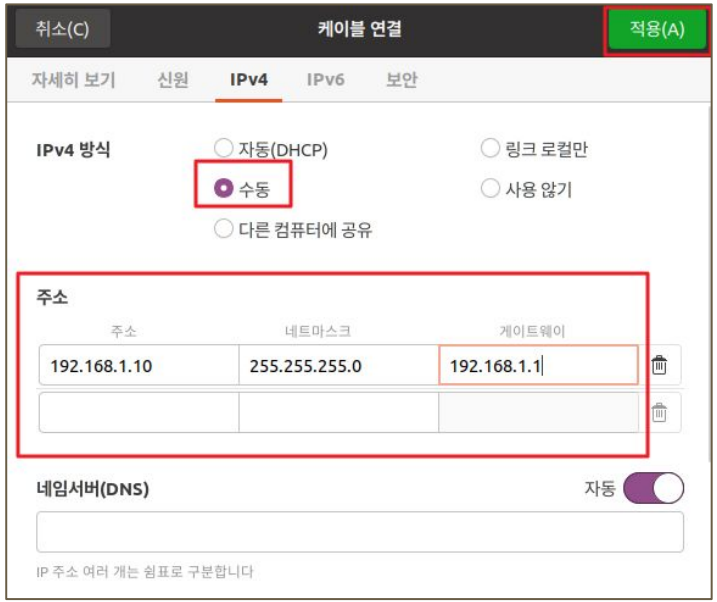
< 2 >

Ubuntu Network 설정

1. Ubuntu 20.04 Desktop 의 Network 설정 (GUI) – 2



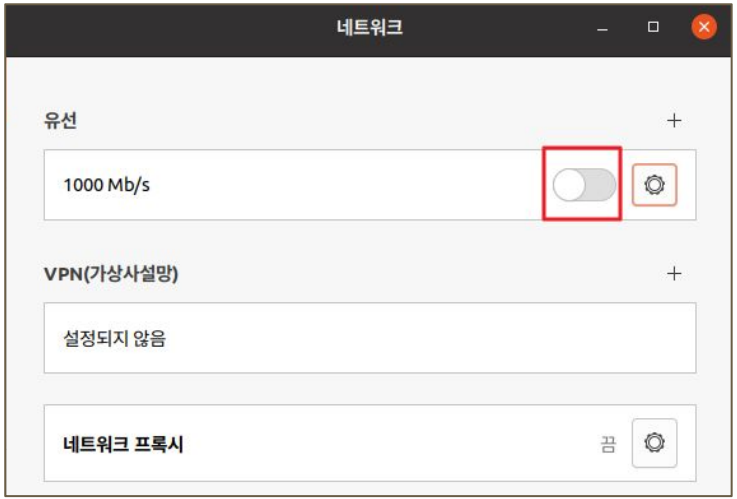
< 3 – DHCP (Default)>



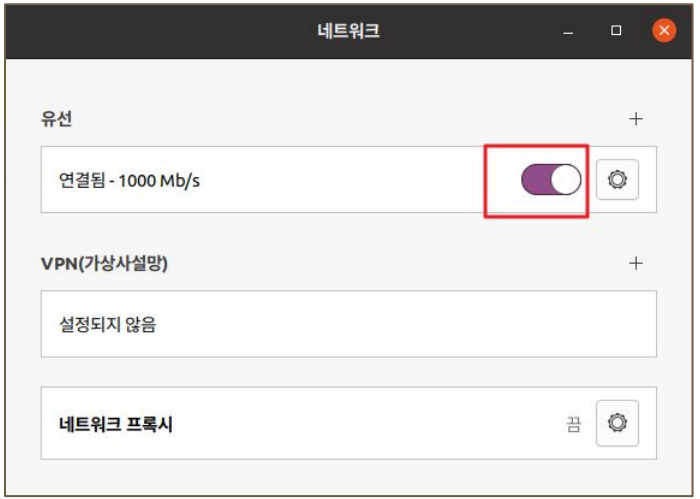
< 4 – 고정 IP >

Ubuntu Network 설정

1. Ubuntu 20.04 Desktop 의 Network 설정 (GUI) – 3



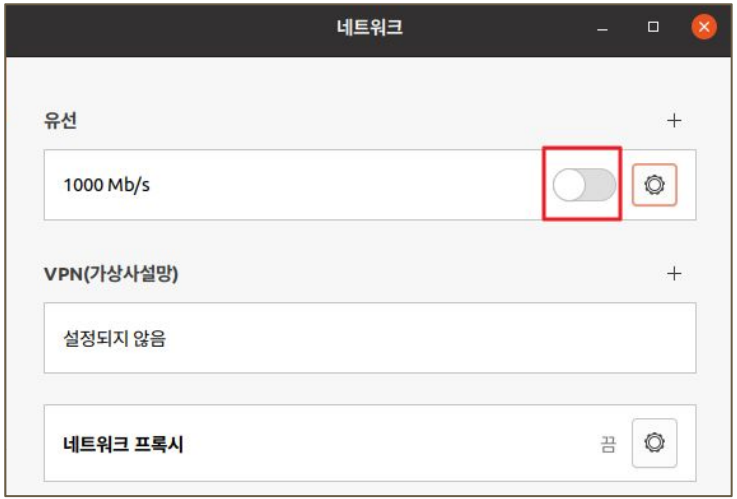
< 5 – Network Off 변경>



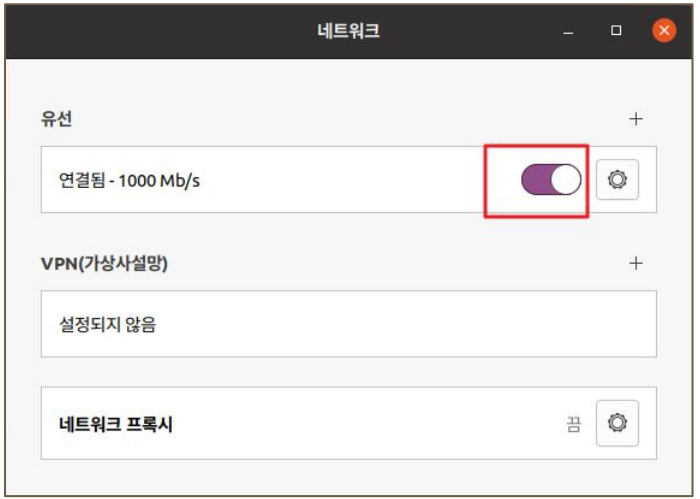
< 6 – Network On 재변경 >

Ubuntu Network 설정

1. Ubuntu 20.04 Desktop 의 Network 설정 (GUI) – 4



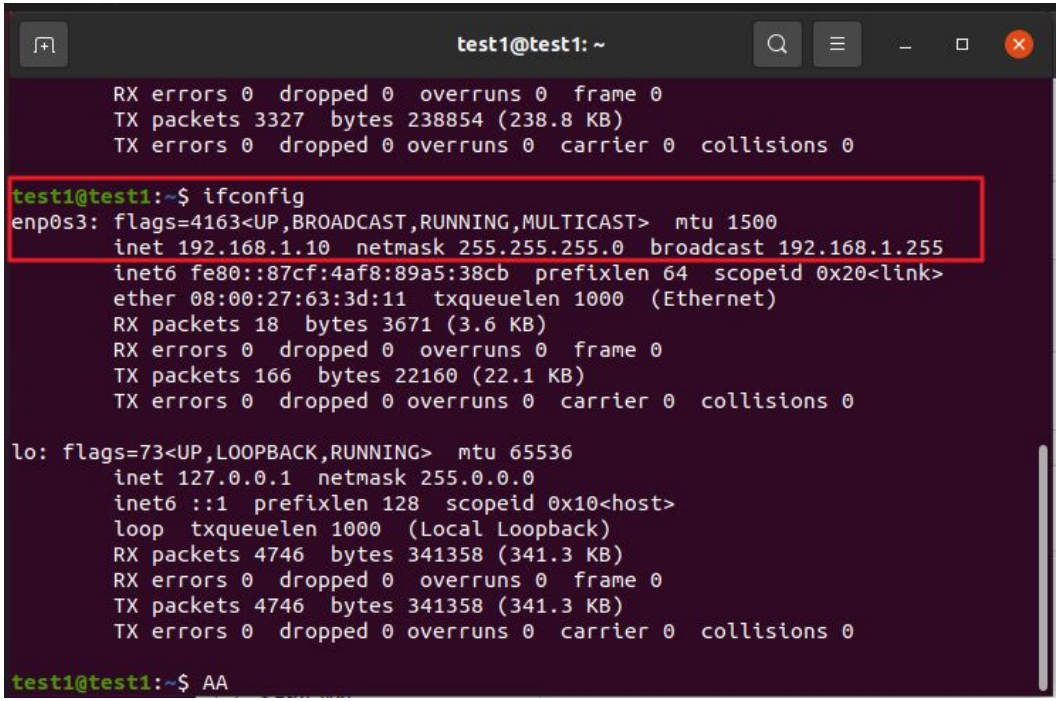
< 5 – Network Off 변경>



< 6 – Network On 재변경 >

Ubuntu Network 설정

1. Ubuntu 20.04 Desktop 의 Network 설정 (GUI) – 5



< 7 – Terminal 에서 IP 확인>

Ubuntu Network 설정

Ubuntu 20.04 / 18.04 Server 의 Network 설정 (CLI) > vim 편집 화면

```
# This is the network config written by 'subiquity'
network:
  ethernets:
    enp0s3:
      dhcp4: true
  version: 2
```

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

DHCP (Default)

```
# This is the network config written by 'subiquity'
network:
  ethernets:
    enp0s3:
      dhcp4: no
      addresses: ["192.168.1.10/24"]
      gateway4: "192.168.1.1"
      nameservers:
        addresses: ["164.124.101.2"]
  version: 2
```

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

고정 IP

Ubuntu Network 설정

Ubuntu 22.04의 고정 IP 설정 > 설정 포맷 참고용도

```
network:
  ethernets:
    eth0:
      dhcp4: true
  version: 2
```

<1 – DHCP (Default) – 설정포맷 >

```
network:
  renderer: networkd
  ethernets:
    eth0:
      addresses:
        - 192.168.10.5/24
      nameservers:
        addresses: [1.1.1.1,8.8.8.8]
      routes:
        - to: default
          via: 192.168.1.1
  version: 2
```

< 2 – 고정 IP – 설정 포맷 >

```
netplan apply
```

< 3 – IP 설정 적용 명령어 >

Ubuntu Network 설정

Ubuntu 20.04 / 18.04 Server 의 Network 설정 (CLI) > 설정 포맷 참고용도

```
network:
  ethernets:
    eth0:
      dhcp4: true
      nameservers:
        addresses: ["164.124.101.2"]
  version: 2
```

<1 – DHCP (Default) – 설정포맷 >

```
network:
  ethernets:
    eth0:
      dhcp4: no
      addresses:
["192.168.1.10/24"]
      gateway4: "192.168.1.1"
      nameservers:
        addresses: ["164.124.101.2"]
  version: 2
```

< 2 – 고정 IP – 설정 포맷 >

```
netplan apply
```

< 3– IP 설정 적용 명령어 >

Ubuntu Network 설정

Ubuntu 16.04 / 14.04 Server 의 Network 설정 (CLI) > 설정 포맷 참고용도

```
auto enp0s3
iface enp0s3 inet dhcp
```

<1 – /etc/network/interfaces >
DHCP – 설정 포맷

```
auto enp0s3
iface enp0s3 inet dhcp
address 192.168.1.10
netmask 255.255.255.0
gateway 192.168.1.1
dns-nameservers 164.124.101.2
```

< 2 – /etc/network/interfaces >
고정 IP – 설정 포맷

```
/etc/init.d/networking restart
```

< 3– IP 설정 적용 명령어 >

```
ifdown enp0s3 && ip addr flush enp0s3 && ifup enp0s3
```

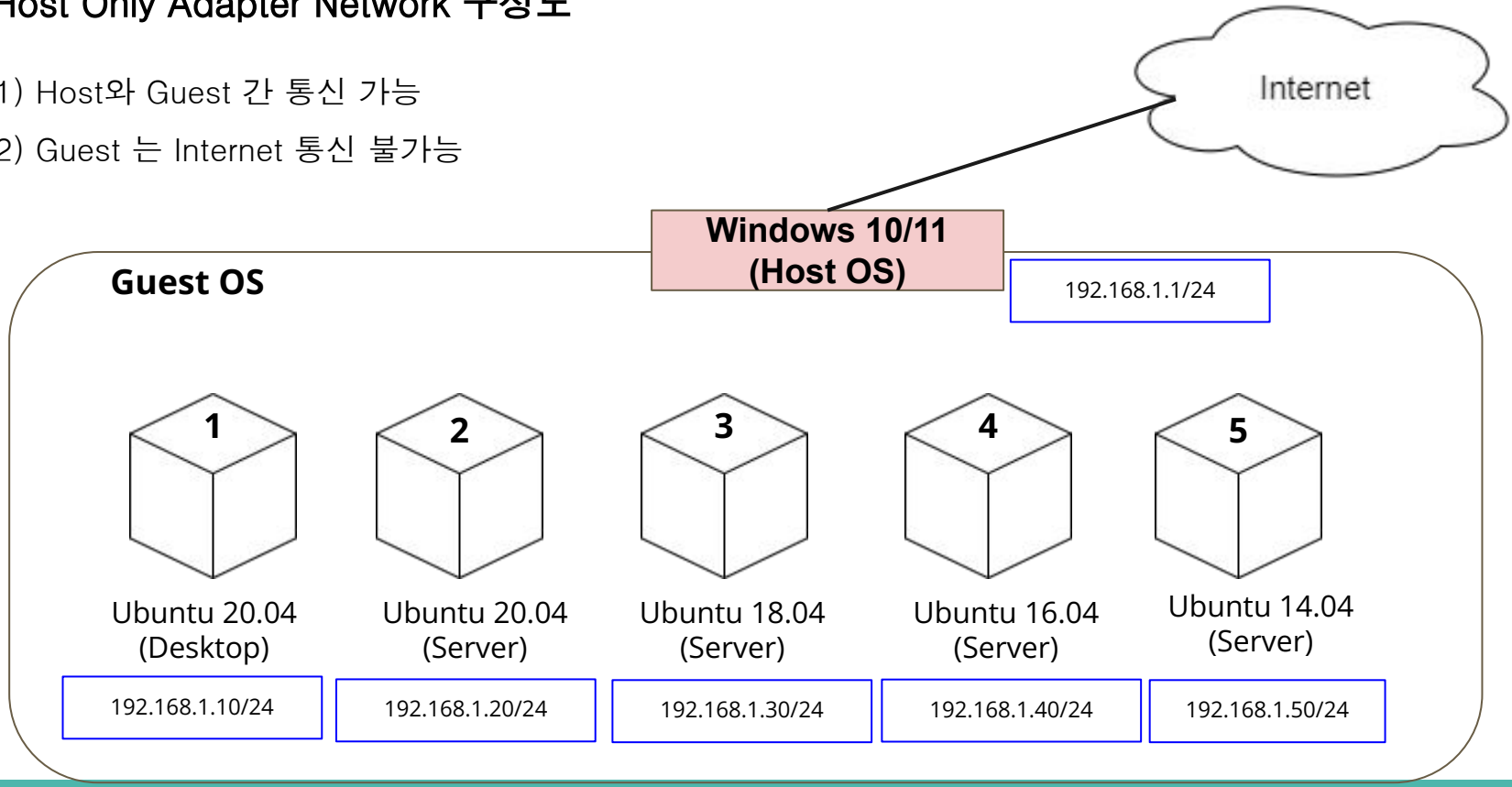
< 4 – 3번 안되는 경우 IP 설정 적용 명령어 >

Ubuntu Network 설정

3. Host Only Adapter Network 구성도

1) Host와 Guest 간 통신 가능

2) Guest 는 Internet 통신 불가능



원격접속 (Telnet, SSH)

xinetd

- Network 관련 서비스 데몬을 관리하는 **슈퍼데몬**
- 기본적으로 다른 네트워크 서비스들을 위해 요청을 받고 실행하는 역할
  - telnetd 관리 (옛날 버전은 FTP 또한 관리했었음)
- 요즘은 systemd 에서 관련 기능의 역할을 대체하고 있어서 잘 사용하지 않음

환경구성

1. 텔넷(Telnet), SSH(Secure Shell), XRDP
2. 프로토콜 / 포트번호
   a. 텔넷 : TCP / 23 Port
   b. SSH : TCP /22 Port
   c. XRDP : TCP / 3389 Port

텔넷과 SSH 보안성 차이점

a. 텔넷 : 취약 (Cleartext - 평문)
b. SSH : 강함 (Encryption - 암호화)

원격접속 (Telnet, SSH)

텔넷과 SSH 비교

구분	텔넷 서버	SSH 서버
속도	빠르다.	빠르다.
그래픽 지원	지원 안 한다.	지원 안 한다.
보안	취약하다.	강하다.
사용 가능 명령어	텍스트 모드의 명령어만 사용할 수 있다.	텍스트 모드의 명령어만 사용할 수 있다.
클라이언트 프로그램	대개의 운영체제가 기본적으로 있다.	리눅스는 기본적으로 있다. Windows는 별도 설치해야 한다.

원격접속 (Telnet, SSH)

Telnet 설정 Ubuntu 18.04 / 20.04 / 22.04 기준

```
apt-get install xinetd telnetd -y
```

< 1 – telnet 관련 패키지 설치 >

```
service telnet
{
        disable         = no
        flags           = REUSE
        socket_type     = stream
        wait            = no
        user            = root
        server          = /usr/sbin/in.telnetd
        log_on_failure  += USERID
}
```

< 2 – /etc/xinetd.d/telnet >

```
service telnet
{
        disable         = no
        flags           = REUSE
        socket_type     = stream
        wait            = no
        user            = root
        server          = /usr/sbin/in.telnetd
        log_on_failure  += USERID
}
```

< 설정 포맷 >

```
/etc/init.d/xinetd restart
```

< 3 – xinetd 서비스 재시작 명령어 >

tcpdump 를 통한 패킷 스니핑

tcpdump 란?

설명 :

- TCPDump는 네트워크 패킷을 캡처하고 분석하는 데 사용되는 명령 줄 기반의 도구
- 네트워크 문제 해결, 보안 감시, 실시간 네트워크 트래픽 분석 및 저장 등 다양한 용도로 활용
- 명령줄 기반의 도구로 Terminal 에서 사용됨
  (GUI 인터페이스를 제공하는 Wireshark와 달리 시각적 표현 기능 등은 저하)

주요기능 :

- 패킷 캡처: TCPDump는 네트워크 인터페이스에서 패킷을 캡처하여 출력합니다. 이를 통해 네트워크 트래픽을 실시간으로 모니터 가능
- 필터링: TCPDump는 BPF(Berkeley Packet Filter) 필터를 사용하여 특정 프로토콜, 송수신 주소, 포트 등을 기반으로 패킷을 필터링 가능
- 디스플레이 포맷: 캡처된 패킷은 다양한 형식으로 출력될 수 있습니다. 기본적으로 텍스트 형식으로 출력되지만, `-w` 옵션을 사용하여 캡처 파일을 저장 가능 (Wireshark 도구와 연동 가능)
- 스냅숏 출력: `-c` 옵션을 사용하여 지정된 패킷 수나 시간 동안의 패킷만 캡처하여 출력 가능

tcpdump 를 통한 패킷 스니핑

Telnet과 SSH를 tcpdump 해보기 (Wireshark 포함)

명령어 :

기본 사용법: sudo tcpdump
- 모든 인터페이스에서 수신되는 패킷을 실시간으로 출력

특정 인터페이스 지정: sudo tcpdump -i eth0
- eth0 인터페이스에서 수신되는 패킷을 출력

필터링: sudo tcpdump -i eth0 tcp port 23
- eth0 인터페이스에서 TCP 포트 23 포트로 들어오는 패킷만 출력

패킷 저장: sudo tcpdump -i eth0 -w capture.pcap
- eth0 인터페이스에서 캡처된 패킷을 capture.pcap 파일에 저장