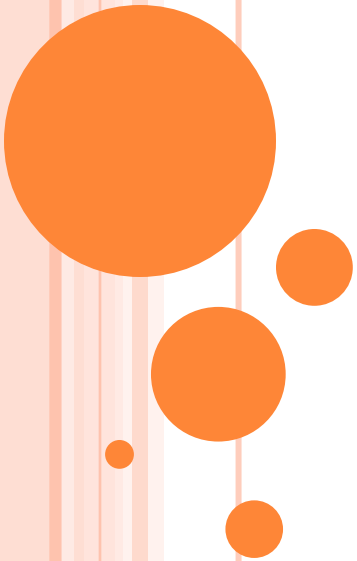
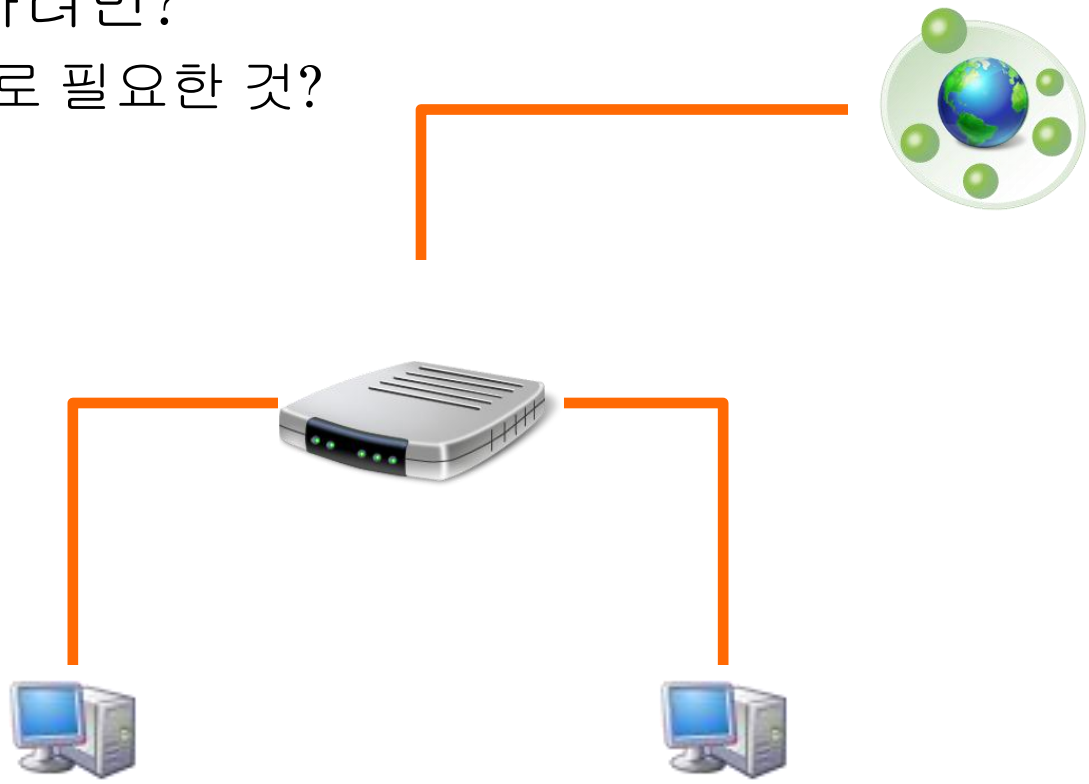


Linux Admin 2nd Course

Created by - Jang Dong Hyun

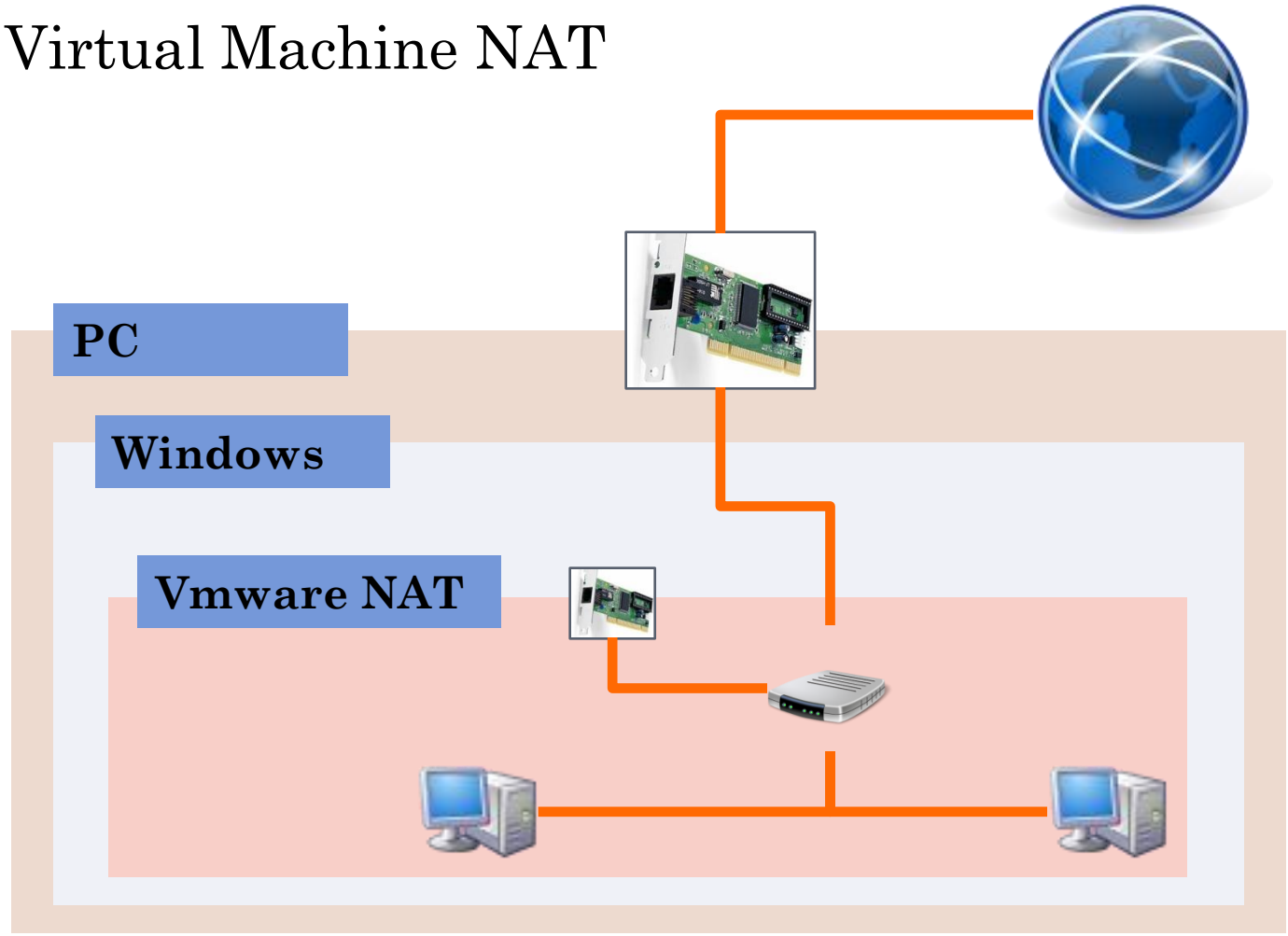
NET WORK

- 인터넷을 하려면?
  - 기본적으로 필요한 것?



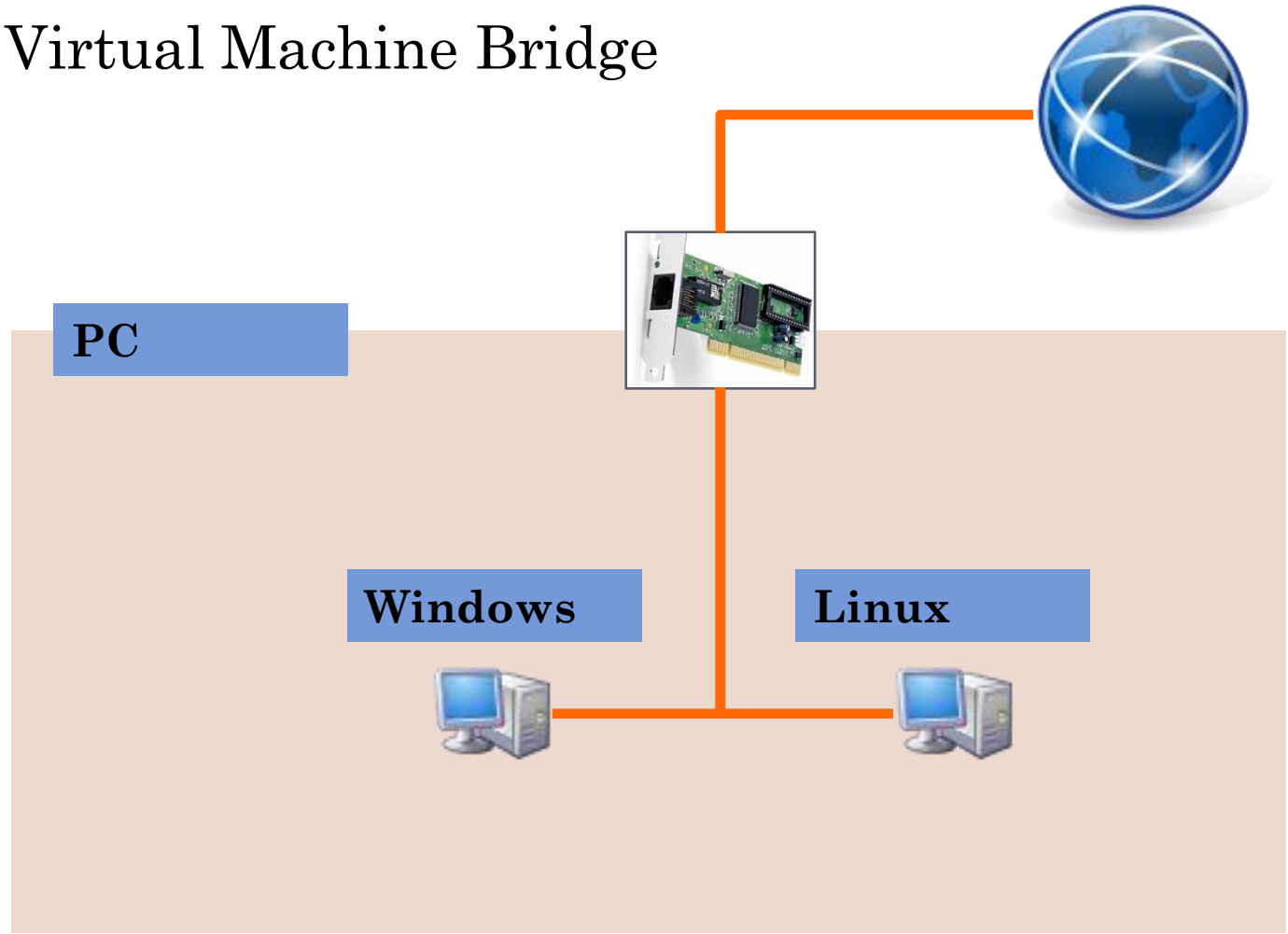
Net Work

- Virtual Machine NAT



Net Work

- Virtual Machine Bridge



Net Work

- Net Work needs
  - IP Address
  - Subnet Mask & IP Band
  - Broadcast
  - Gate Way

Net Work

- /etc/modprobe.conf
  - Ethernet Device Check conf file

```
alias eth0 pcnet32
alias scsi_hostadapter ata_piix
alias snd-card-0 snd-intel8x0
options snd-card-0 index=0
options snd-intel8x0 index=0
remove snd-intel8x0 { /usr/sbin/alsactl stor
bin/modprobe -r --ignore-remove snd-intel8x0
```

NET WORK

- /etc/sysconfig/network
  - Network 사용 선택
  - Hostname 지정

```
NETWORKING=yes
NETWORKING_IPV6=no
HOSTNAME=makjjang.com
```

NET WORK

- /etc/hosts
  - host 주소에 이름 부여

```
# Do not remove the following line,
# that require network functionali
127.0.0.1                   localhost.
::1                 localhost6.localdor
210.16.199.249                 makjjang
```

```
[root@makjjang.com ~]
[18:04:25]# ping makjjang
PING makjjang (210.16.199.249) 56(84) bytes
64 bytes from makjjang (210.16.199.249): ic
64 bytes from makjjang (210.16.199.249): ic
64 bytes from makjjang (210.16.199.249): ic
```

NET WORK

- ifconfig
  - 네트워크 interface에 설정을 적용하거나, 내용 출력
  - ifconfig [interface] [IP] ... [up|down]

```
[root@makjjang.com ~]
[18:05:18]# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:FC:7D:4E
          inet addr:10.0.2.15  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fefc:7d4e/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:954 errors:0 dropped:0 overruns:0 frame:0
          TX packets:685 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:79190 (77.3 KiB)  TX bytes:86800 (84.7 KiB)
          Interrupt:11 Base address:0xd020
```

NET WORK

- /etc/sysconfig/network-scripts/ifcfg-eth0
  - Network 구성 설정 file

```
DEVICE=eth0
BOOTPROTO=dhcp
HWADDR=08:00:27:FC:7D:4E
ONBOOT=yes
```

  - 수동 설정 시
    - BOOTPROTO=static
    - IPADDR=[IP]
    - NETMASK=[Netmask number]
    - GATEWAY=[Gateway address]

NET WORK

- dhclient
  - DHCP Server가 있으면, IP를 할당 받아 적용
  - dhclient [interface]

```
[root@makjjang.com ~]
[18:47:40]# dhclient eth0
Internet Systems Consortium DHCP Client V3.0.5-RedHat
Copyright 2004-2006 Internet Systems Consortium.
All rights reserved.
For info, please visit http://www.isc.org/sw/dhcp/

Listening on LPF/eth0/08:00:27:fc:7d:4e
Sending on   LPF/eth0/08:00:27:fc:7d:4e
Sending on   Socket/fallback
DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interval 7
DHCPOFFER from 10.0.2.2
DHCPREQUEST on eth0 to 255.255.255.255 port 67
DHCPACK from 10.0.2.2
bound to 10.0.2.15 -- renewal in 34861 seconds.
```

NET WORK

- route
  - Linux의 Router 정보 출력 및 설정 명령

```
[root@makjjang.com ~]
[02:20:19]# route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
10.0.2.0        *               255.255.255.0   U     0      0        0 eth0
169.254.0.0     *               255.255.0.0     U     0      0        0 eth0
default         10.0.2.2        0.0.0.0         UG    0      0        0 eth0
```

  - Gate Way 설정
    - route add default gw [Gateway address] dev [interface]
  - Gate Way 설정 해제
    - route del default gw [Gateway address]

NET WORK

- DNS Setting
  - /etc/resolv.conf
  - DNS server IP를 정의하여, Linux에 적용

```
nameserver 211.63.64.11
nameserver 168.126.63.1
```

  - 최대 3개 까지 지정가능

NET WORK

- netstat
  - Network 상태를 좀 더 자세히 확인

```
[root@makjjang.com ~]
[02:31:08]# netstat -ant
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address               Foreign Address             State
tcp        0      0 127.0.0.1:2208              0.0.0.0:*                   LISTEN
tcp        0      0 0.0.0.0:614                 0.0.0.0:*                   LISTEN
tcp        0      0 0.0.0.0:111                 0.0.0.0:*                   LISTEN
tcp        0      0 127.0.0.1:631               0.0.0.0:*                   LISTEN
tcp        0      0 127.0.0.1:25                0.0.0.0:*                   LISTEN
tcp        0      0 127.0.0.1:6010              0.0.0.0:*                   LISTEN
tcp        0      0 127.0.0.1:2207              0.0.0.0:*                   LISTEN
tcp        0      0 :::22                       :::*                        LISTEN
tcp        0      0 ::1:6010                    :::*                        LISTEN
tcp        0    132 ::ffff:10.0.2.15:22         ::ffff:210.16.199.249:4229  ESTABLISHED
```

NET WORK

- nslookup
  - DNS를 이용한 Domain search
  - IP의 정보 확인

```
[root@makjjang.com ~]
[02:42:27]# nslookup
> www.yahoo.com
Server:         168.126.63.1
Address:        168.126.63.1#53

Non-authoritative answer:
www.yahoo.com   canonical name = www.wa1.b.yahoo.com.
www.wa1.b.yahoo.com     canonical name = www-real.wa1.b.yahoo.com.
Name:   www-real.wa1.b.yahoo.com
Address: 87.248.113.14
```

NET WORK

- Sun Virtual Box **Port Forwarding**
  - Virtual Box는 Host OS 의 통신이 이뤄지지 않기 때문에 Port Forwarding 을 지정해야 함
  - 지정하기 위해서는 설치 위치로 가서 명령 수행

- VBoxManage setextradata “[Guest OS Name]" "VBoxInternal/Devices/pcnet/0/LUN#0/Config/[Service]/Protocol" [TCP|UDP]
- VBoxManage setextradata "[Guest OS Name]" "VBoxInternal/Devices/pcnet/0/LUN#0/Config/[Service]/GuestPort" [Port Number]
- VBoxManage setextradata "[Guest OS Name]" "VBoxInternal/Devices/pcnet/0/LUN#0/Config/[Service]/HostPort" [Port Number]

NET WORK

- iptables
  - Linux에서 사용하는 자체 방화벽
  - IP와 port등을 이용하여 접근 제어

- /etc/sysconfig/iptables
  - 방화벽 설정 file

```
[root@makjjang.com ~]
[03:01:49]# cat /etc/sysconfig/iptables
# Firewall configuration written by system-config-securitylevel
# Manual customization of this file is not recommended.
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
:RH-Firewall-1-INPUT - [0:0]
-A INPUT -j RH-Firewall-1-INPUT
-A FORWARD -j RH-Firewall-1-INPUT
-A RH-Firewall-1-INPUT -i lo -j ACCEPT
-A RH-Firewall-1-INPUT -p icmp --icmp-type any -j ACCEPT
-A RH-Firewall-1-INPUT -p 50 -j ACCEPT
-A RH-Firewall-1-INPUT -p 51 -j ACCEPT
-A RH-Firewall-1-INPUT -p udp --dport 5353 -d 224.0.0.251 -j ACCEPT
```

NET WORK

- iptables에 port 예외 적용
  - -A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 80 -j ACCEPT

- iptables 재 적용
  - service iptables restart

ROUTING

- MASQUERADE Server
  - Router 장비가 없어도, routing 기능 활용
  - 중,소규모 크기의 Network 분할, 인트라넷 등 많은 부분에서 저렴한 비용으로 사용 가능

ROUTING

- 1st : 네트워크 카드 두 개 설정
  - eth 0 : Router 간 네트워크 대역
  - eth1 : Router 아래 소규모 네트워크 대역

ROUTING

- 2nd : IP forwarding 지정
  - /etc/sysctl.conf 의 설정 변경
  - 변경 완료 시 Re booting

```
# Controls IP packet forwarding
net.ipv4.ip_forward = 1
```

  - 확인 법
    - **#cat /proc/sys/net/ipv4/ip_forward**

ROUTING

- 3rd : IPtable에 보안 설정 및 모듈 적용
  - iptables에 Musquerade 설정
  - *filter 바로 위

***nat**
:POSTROUTING ACCEPT
-A POSTROUTING -o eth1 -j MASQUERADE
COMMIT

  - 방화벽 설정

-A RH-Firewall-1-INPUT -m state --state NEW -o eth1 -j ACCEPT

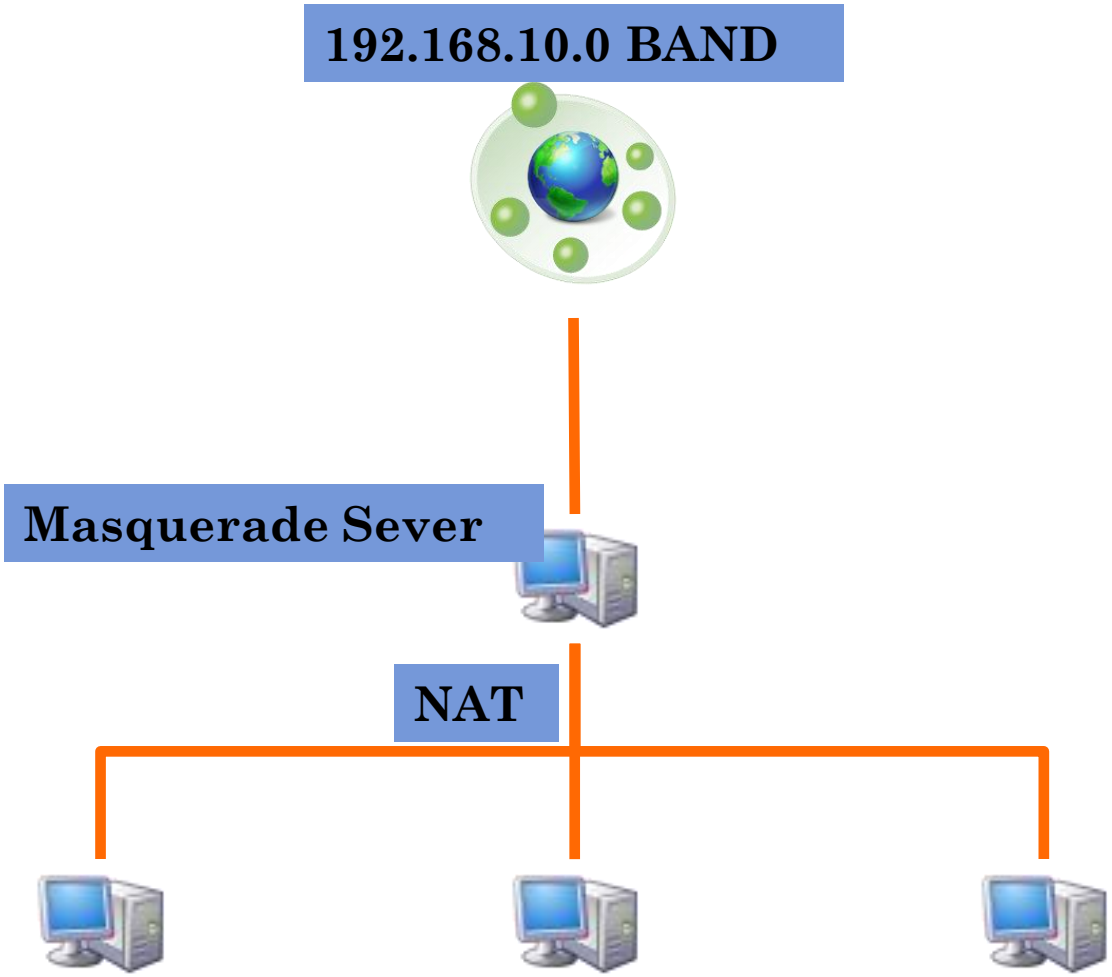
ROUTING

- 4th : 방화벽 설정 완료 시, 재 적용 후 확인

```
[root@makjjang.com ~]
[18:21:44]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
RH-Firewall-1-INPUT  all  --  anywhere             anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
RH-Firewall-1-INPUT  all  --  anywhere             anywhere
```

```
[root@makjjang.com ~]
[18:24:07]# iptables -L -t nat
Chain PREROUTING (policy ACCEPT)
target     prot opt source               destination

Chain POSTROUTING (policy ACCEPT)
target     prot opt source               destination
MASQUERADE  all  --  anywhere             anywhere
```

RAB



DHCP

- Dynamic Host Configuration Protocol
  - 정해진 IP 대역 대 내에서 IP 대여하려는 Client의 요청에 의거해 대여 할당하는 Server Protocol

  - Client에 IP 할당 시 4가지 단계
    - **DHCPDISCOVER**
    - **DHCPOFFER**
    - **DHCPREQUEST**
    - **DHCPACK**

DHCP

- dhcpd 가 없습니까?
  - yum install -y dhcp 로 설치!

DHCP

- /etc/dhcpd.conf
  - DHCP Server Configuration File

- Configuring
  - option routers [IP]
    - Client 에 부여할 Gate Way IP

  - option subnet-mask [subnet-mask number]
    - 적용할 subnet-mask

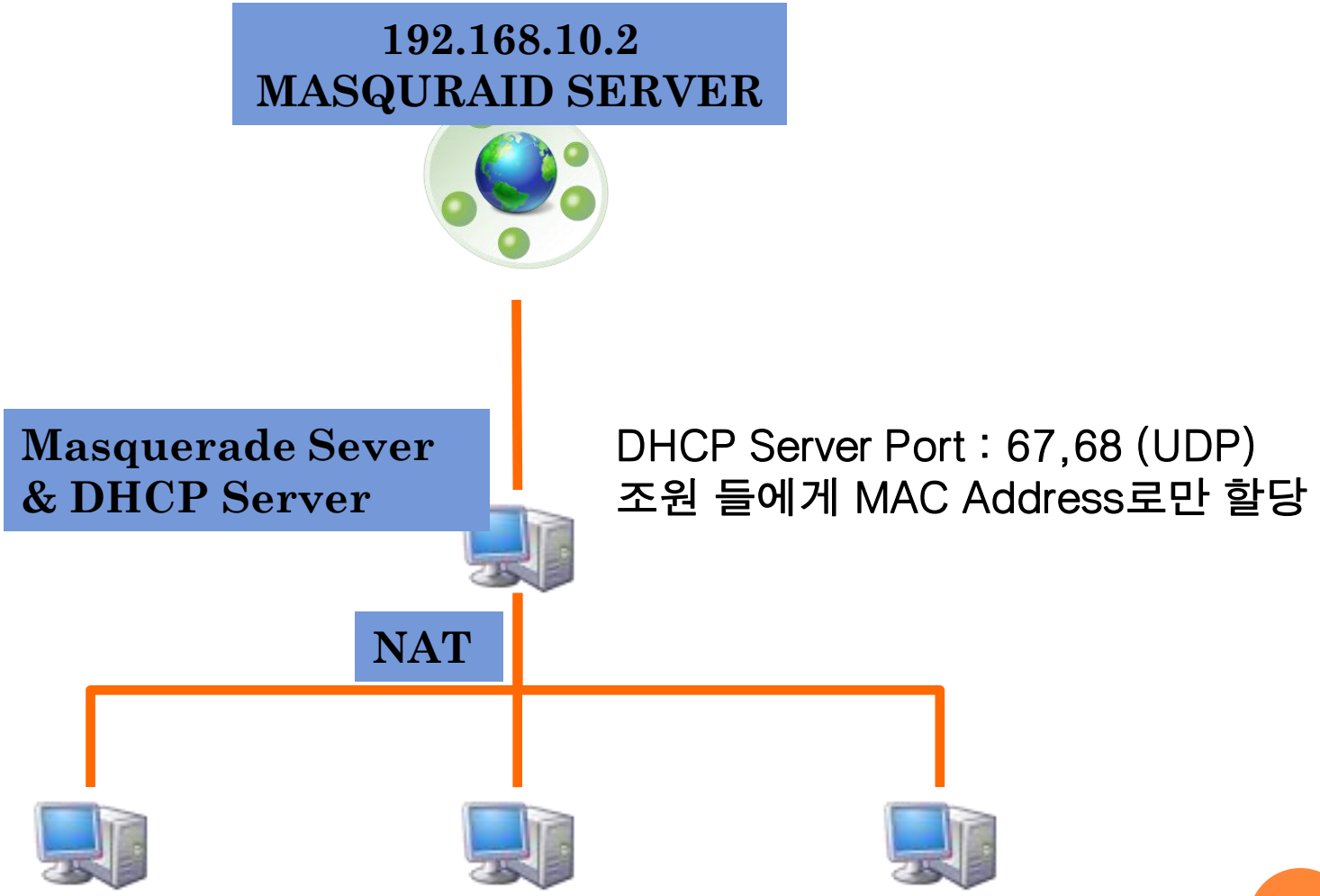
DHCP

- Configuring
  - option domain-name-servers [IP] [IP] ...
    - 적용할 DNS
  - range dynamic-bootp [Start IP] [End IP]
    - Client에 부여할 IP 대역 대
  - host [name]{ ... }
    - MAC Address로 static IP 설정 시에 사용

DHCP

- Configuring
  - host
    - hardware ethernet [MAC Address]
      - 적용되는 MAC Address
    - fixed-address [IP]
      - MAC Address를 가진 Client에 부여할 IP

RAB


192.168.10.2
MASQURAID SERVER
Masquerade Sever
& DHCP Server
DHCP Server Port : 67,68 (UDP)
조원 들에게 MAC Address로만 할당
NAT

Proxy Server

- Proxy Server
  - 인터넷 공유를 위한 서버
  - cache를 지원하여 누군가가 한번 들어간 곳은 다시 들어갈 때 더 빠르게 들어 갈 수 있음
  - 내부 네트워크 보안에 좋음
- Squid
  - Proxy Server 중에 가장 많이 사용
  - 자세한 내용 : www.squid-cache.org

Proxy Server

- /etc/squid/squid.conf
  - Squid Configuration File

  - acl 부분 설정
    - acl [적용 그룹] src [적용 그룹 IP 대역 대] / [Subnet-Mask]
    - ex>

```
acl firestrike src 192.168.100.0/255.255.255.0
```

  - Access 설정
    - http_access [allow | deny] [적용 그룹]
    - ex>

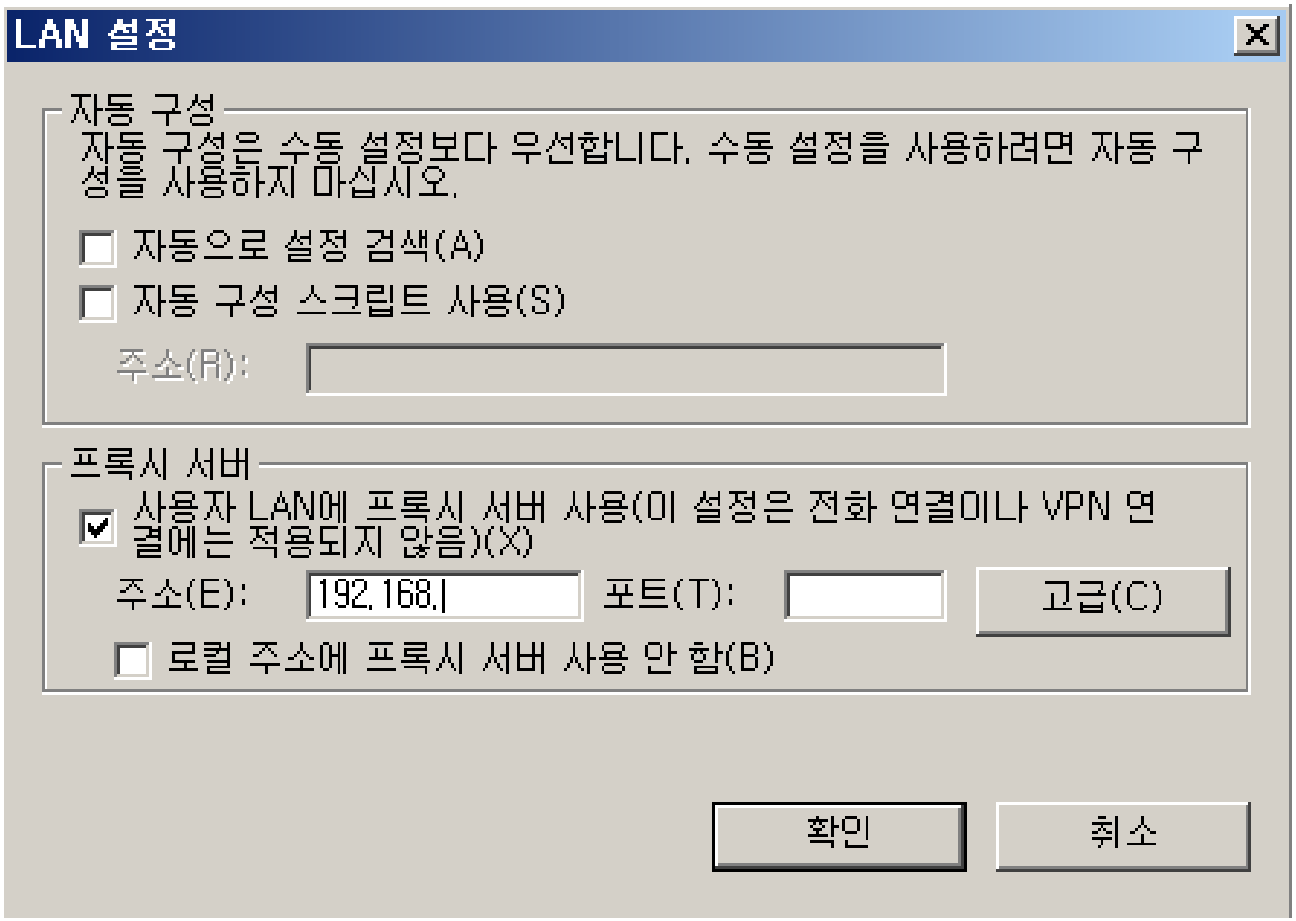
```
http_access allow firestrike
```

Proxy Server

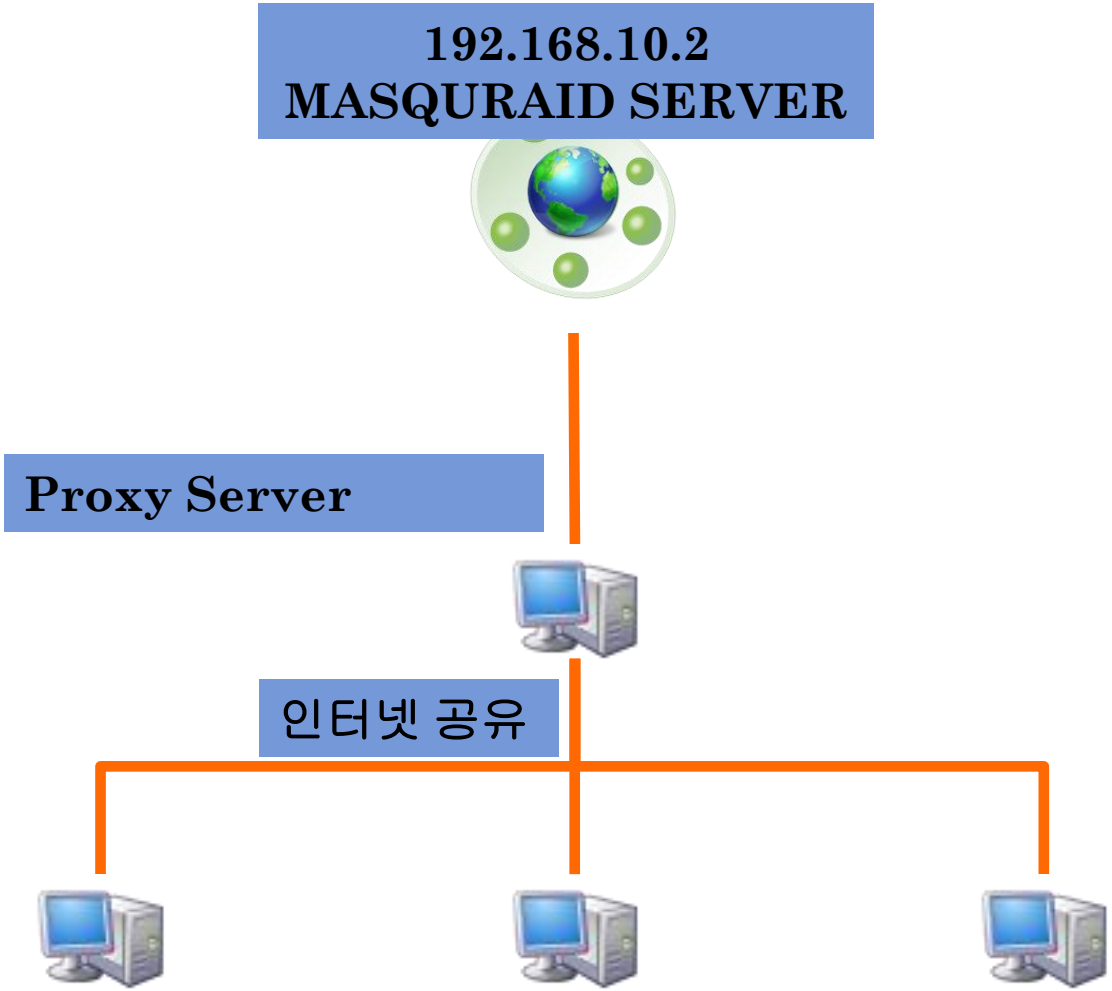
- Trouble shooting
  - log file Check
    - /var/log/squid Directory
  - Conf File Check
    - visible_hostname [group]

Proxy Server

- Client Proxy Server 설정



RAB



NFS

- NFS란?
  - Server의 특정 Directory를 Client에서 Mount 하는 일종의 공유
  - Server와 Client 간 RPC 통신을 사용하며, RPC 통신을 위한 정해진 Service Port가 없어 portmapper를 이용하여 가능하게 함
- 관련 Service
  - nfs
  - portmap

NFS

- 1st
  - /etc/exports File Configuration
  - 공유할 Directory와 옵션 지정
  - 기본 (ro), writable 시 (rw)로 지정
  - Directory [IP or Hosts]([Options])

```
/tmp/pubNfs *(ro)
/tmp/t1 192.168.10.100
/tmp/t2 makjjang1(ro)
```

NFS

- 2nd
  - nfs와 portmap Service Start
  - #exportfs -v
    - 공유 Directory 확인

NFS

- 3rd
  - #rpcinfo -p 127.0.0.1
  - 자신의 Server RPC port open Information Check
  - 열려 있는 port에 따라 방화벽 설정 (udp,tcp)

NFS

- 정해진 port
  - portmapper : 111
  - nfs : 2049

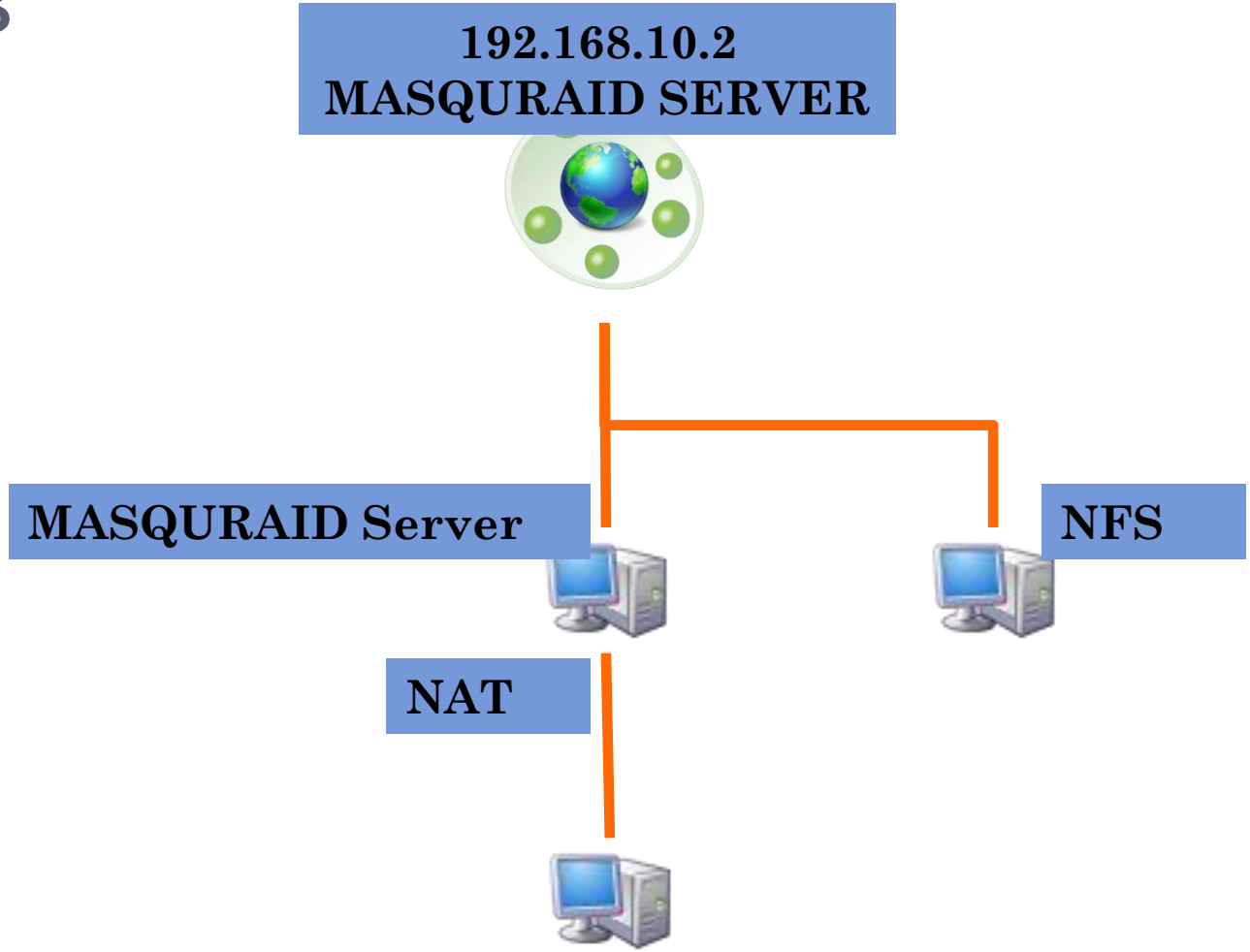
- 가변 port
  - rquotad
  - nlockmgr
  - mountd

NFS

- /etc/sysconfig/nfs
  - 가변 port를 사용하지 않고, 원하는 port 사용가능

- no_root_squash
  - rw 가 되지 않을 때 부여할 옵션
  - 누구나 nobody 계정으로 들어오지만, 모두 root 권한으로 사용 가능

RAB



SAMBA

- Samba?
  - Linux와 Windows 공유 Directory 설정
  - 백업, 공유 등 많은 부분에서 전반적인 사용
- Service Name
  - smb

SAMBA

- 1st : /etc/samba/smb.conf Configuration
  - workgroup = [group name]
    - 공유할 그룹 설정
    - Windows와 동일하게 설정해야함
  - host allow = [allow ip]
    - 허용할 ip 적용
  - netbios name = [server name]
    - 네트워크 상 표시될 서버 이름
  - security = [user | share]
    - 사용 수준 지정

SAMBA

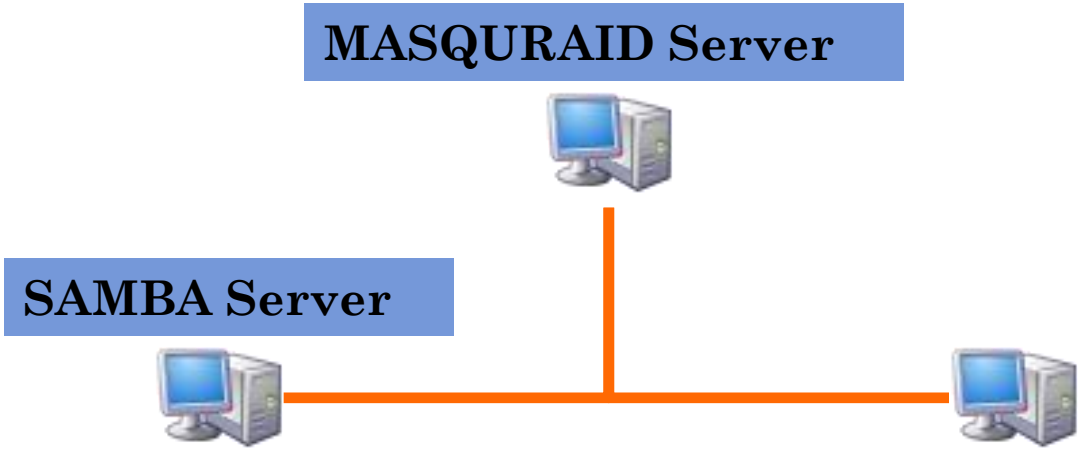
- 2nd : 사용 계정 생성
  - #mkdir /tmp/smbdata
    - 공유 Directory 생성
  - #useradd -d /dev/null -s /sbin/nologin samba
    - 공유를 이용할 대표 ID 생성
  - #chown samba:samba /tmp/sambdata
    - samba 계정이 사용할 수 있게 설정

SAMBA

- 3rd : /etc/samba/smb.conf Add Configuration

```
[public_data]
 comment = Linux Samba
 path = /tmp/smbdata
 force user = samba
 force group = samba
 read only = no
 writable = yes
 public = yes
 browseable = yes
 printable = no
 create mode = 0665
```

RAB



SMB Server Port : 137~139 (TCP,UDP)
445(TCP)

SAMBA

- SWAT
  - 복잡한 samba 설정은 손쉽게 가능
  - 설치
    - yum install -y samba-swat
  - 설정 변경
    - /etc/xinetd.d/swat

```
service swat
{
        port            = 901
        socket_type     = stream
        wait            = no
        only_from       = 210.16.199.249
        user            = root
        server          = /usr/sbin/swat
        log_on_failure  += USERID
        disable         = no
}
```

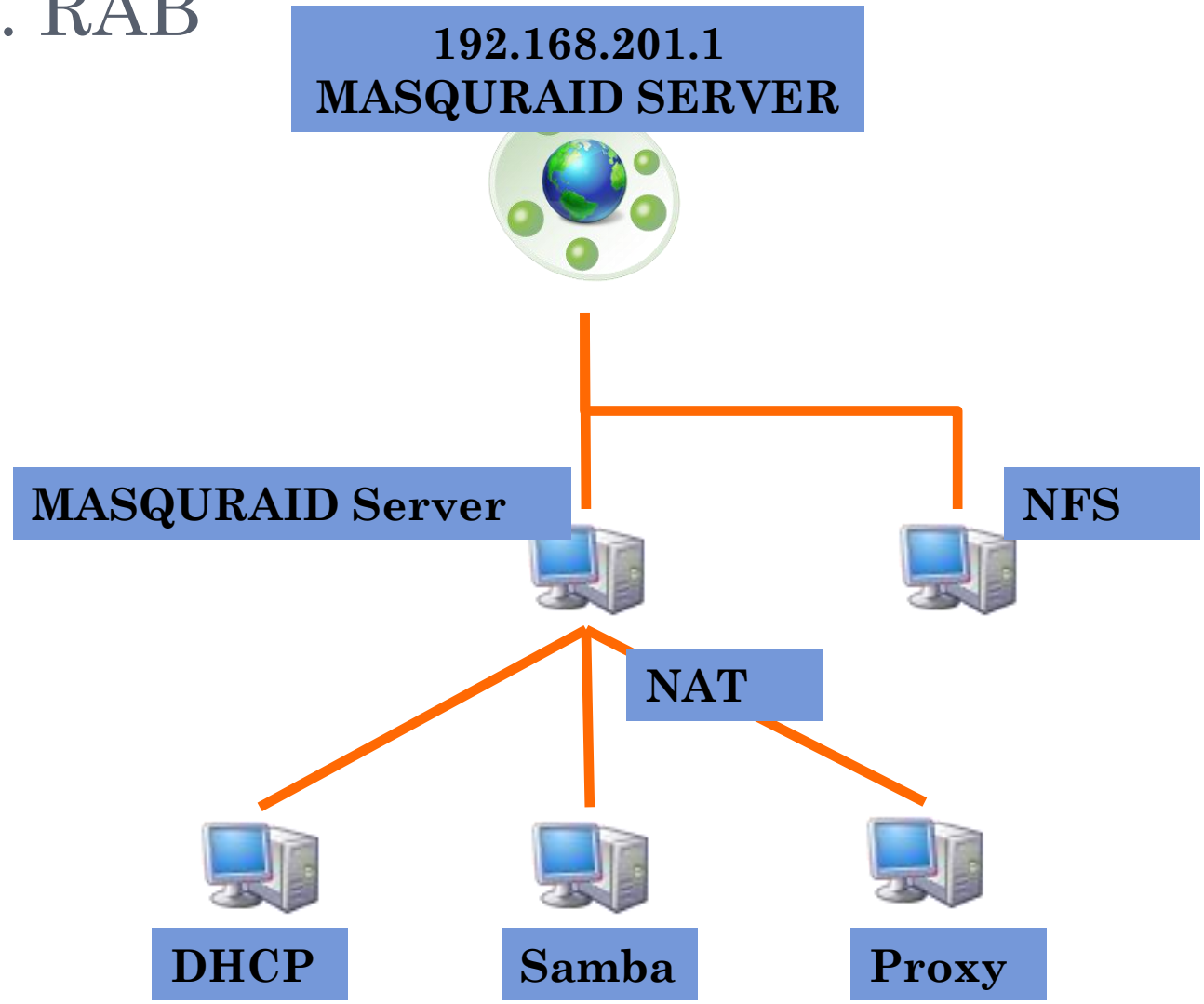
SAMBA

- 중요!
  - SWAT 적용하기 위해서는 samba 가 접근 허용한 ip로 지정하여야 가능함.

SAMBA

- SWAT 실행
  - port 사용
    - 901
  - 설정 적용
    - /etc/init.d/xinetd restart
  - Web page에서 http://[ip]:[swat port]

Adv. RAB


192.168.201.1
MASQURAID SERVER
MASQURAID Server
NFS
NAT
DHCP
Samba
Proxy

DNS

- DNS 란?
  - 인터넷을 접속하기 위해 IP로 사용
  - IP는 숫자, 외우기 힘듦
  - 문자열로 쓰면 그것을 IP로 바꿔서 사용하게 함
  - 그게 DNS 임
- 보안을 위한 Fake Directory
  - /var/named/chroot

DNS

- 1st : named.conf Configuration
  - 위치 : /var/named/chroot/etc/
  - 설정

```
options {
        directory "/var/named";
        dump-file "/var/named/data/cache_dump.db";
        statistics-file "/var/named/data/named_stats.txt";
};

zone "intoc.kr" IN {
        type master;
        file "intoc.zone";
        allow-update { none; };
};

zone "201.168.192.in-addr.arpa" IN {
        type master;
        file "intoc.rev";
        allow-update{ none; };
};
```

DNS

- 2nd : Forward Zone file setting
  - 위치 : /var/named/chroot/var/named/

```
$TTL 0
@       IN      SOA     intoc.net.      root.intoc.net. (
                        1               ;serial
                        43200           ;refresh
                        3600            ;retry
                        43200           ;expire
                        0               ;TTL
                        )

        IN      NS      intoc.net.

@       IN      A       192.168.201.1
www     IN      A       192.168.201.1
```

DNS

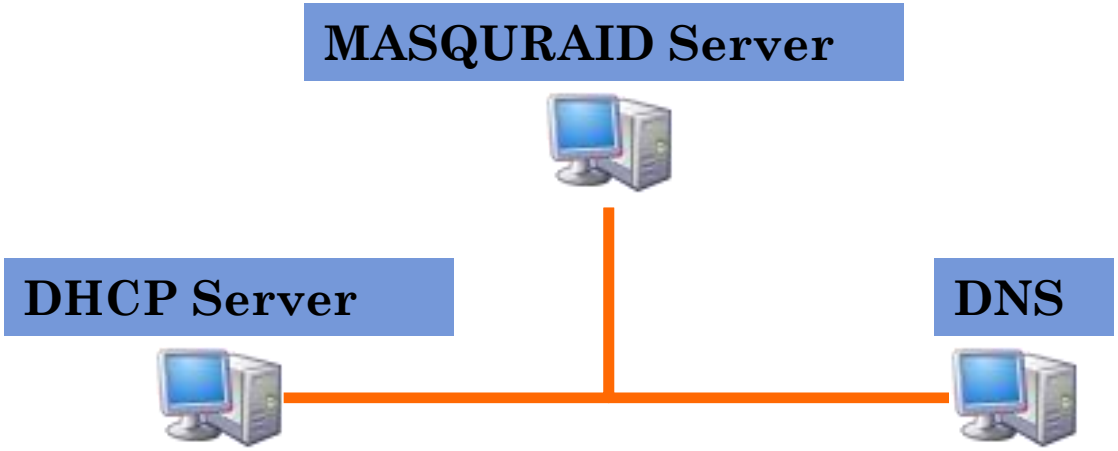
- 3rd : Reverse Zone file setting
  - 위치 : /var/named/chroot/var/named/

```
$TTL 0
@       IN      SOA     intoc.net.      root.intoc.net. (
                1       ;serial
                43200   ;refresh
                3600    ;retry
                43200   ;expire
                0       ;TTL
                )

        IN      NS      intoc.net.

1       IN      PTR     intoc.net.
```

DNS

- Time info
  - TTL (Time to Live)
    - 정보를 가져와 얼마나 오래 가지고 있는가?
    - 0으로 셋팅이 가장 속편 함
  - serial
    - 데이터 버전, 업데이트시 확인
  - Refresh
    - 업데이트 갱신 시간
  - Retry
    - 연결 안될 때 재 연결 시까지의 시간
  - Expire
    - 정보를 받아오는 서버에 접속 하지 못할 경우, 가지고 있는 정보를 얼마나 오랫동안 가지고 있는가?

RAB



DNS Port : 53 (TCP,UDP)

FTP

- vsftpd
  - Very Secure FTP Daemon
  - Cris Evans에 의해 개발된, GPL 기반의 매우 안전하고, 빠르고, 강력한 프로그램
  - 많은 nix OS에서 사용하고 있음
  - xinetd 로 동작

FTP

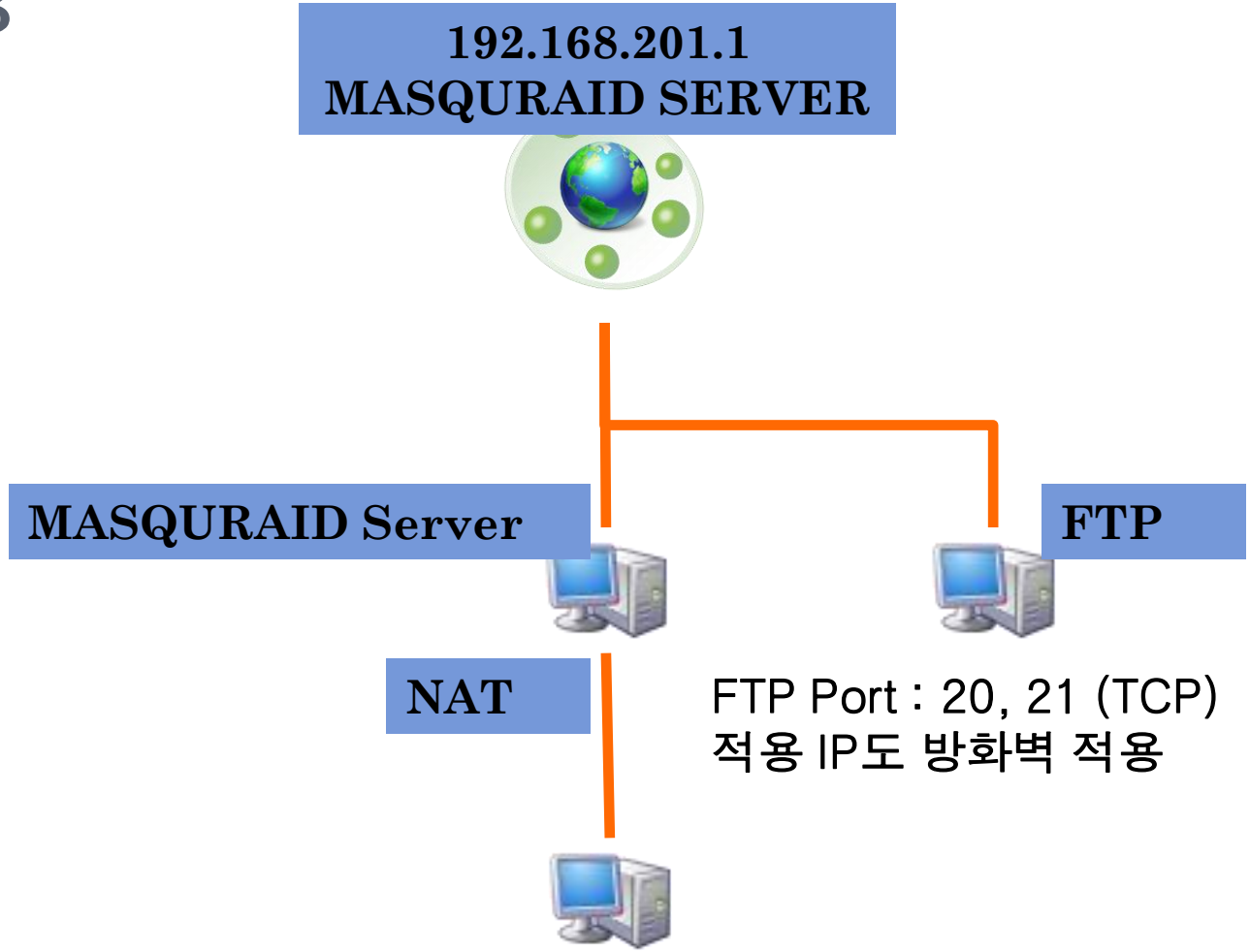
- **/etc/vsftpd/vsftpd.conf**
  - FTP 접근 및 권한 등에 대한 설정 파일
  - 설정 필드

- **/etc/vsftpd/user_list, /etc/vsftpd/ftpusers**
  - 접근 제어 파일, 계정에 대한 접근 제어 설정 가능

FTP

- Service vsftpd restart
  - 서비스 재 시작
- child died Error
  - #setsebool -P ftp_home_dir=1

RAB


192.168.201.1
MASQURAID SERVER
MASQURAID Server
FTP
NAT
FTP Port : 20, 21 (TCP)
적용 IP도 방화벽 적용