|  |
| --- |
| * Ch\_1 \_ DHCP 서버 구축 * Ch\_2 \_ 프록시 서버 구축 * Ch\_3 \_ 방화벽 컴퓨터 개요와 실습 환경 * Ch\_4 \_ 방화벽 컴퓨터 구축 * Ch\_5 \_ PXE 서버 구축 * Ch\_6 \_ 도커 개념정리 및 실습 구축 * DHCP 개념 * DHCP(Dynamic Host Configuration Protocol) 서버가 하는 역할은 자신의 네트워크 안에 있는 클라이언트 컴퓨터가 부팅될 때 자동으로 IP주소, 서브넷 마스크, 게이트웨이 주소, DNS 서버 주소를 할당해 주는 것임 * 일반 사용자는 IP에 관련된 어려운 정보를 알지 못해도, 인터넷을 사용하는 데는 더 이상 아무런 문제가 없어짐 * DHCP서버의 가장 큰 장점은 관리하기 편하고 이용자가 편하다는 것 * 또한 한정된 IP주소를 가지고 더 많은 IP주소가 있는 것처럼 활용할 수 있음. 즉, 적은 개수의 IP주소로 여러 명의 사용자가 사용할 수 있다는 의미 * DHCP서버의 작동원리      * DHCP 클라이언트로 설정 방법      * 우분투를 텍스트 모드에서 DHCP 클라이언트로 설정하려먼 /etc/netplan/\*.yaml 파일의 ‘dhcp4:no’부분을 파일의 ‘dhcp4:true’로 수정하면 된다 * VMware 내부에서 구현할 DHCP 서버 구성도      * VMware가 제공하는 DHCP서버의 기능은 중지시켜야 한다 * DHCP 서버 구축 * Vmware pro에서 서버4대 초기화 (스냅샷) * server > Edit > Virtual Network Editor… > 우측 하단 Change Settings      * DHCP Setttings와 NAT Settings 확인 가능      * 항목 체크를 풀고 Apply > ok // 더 이상 DHCP 서버를 사용하지 않음 * server와 server(b)는 ip를 직접 할당하였기 때문에 지장이 없지만   client와 Winclient는 자동 ip 이였기 때문에 인터넷 사용 불가     * Client를 ifconfig로 확인해 본 결과 // 인터넷 비활성화      * server(b) ping 8.8.8.8 정상 작동 확인      * /etc/netplan/00-installer-config.yaml 파일 수정 * dhcp4:no를 true 로 변경하고 하단 addresses 등 ip내용 삭제      * /etc/systemd/system/network-onlien.target.wants/systemd-networkd-wait-onlien.servie 파일 수정 * 재부팅 후 확인하려는데 이 재부팅이 오래걸린다 (계속해서 ip를 찾기 때문) 따라서 이 재부팅 시 ip찾는 시간을 제한하는 내용을 추가한다 (10sec)      * ip없음 확인 가능      * server dhcp-server 패키지 설치 (apt install)      * /etc/dhcp/dhcpd.conf 파일 내용 추가 * 맨 하단 subnet, netmask 주소, 라우터와 서브넷마스크, ip범위 등을 추가한다 * dhcp서버는 빌려준 내역을 기록하는데 그 파일 내용은 /var/lib/dhcp/dhcpd.leases 서 확인 가능하다      * server(b), client ifconfig로 ip할당 확인 * 프록시 서버 개념 * 프록시(Proxy)란 단어가 뜻하듯 ‘대리인’의 역할을 하는 서버 * 웹 환경에서 프록시 서버는 웹 클라이언트와 웹 서버 사이에서 요청한 데이터를 전달하는 역할 * 한번 전송한 데이터를 캐시에 저장한 후, 같은 데이터를 또 요청할 경우에 캐시에 저장된 것을 보내줌        * squid 패키지 설치 (프록시 서버)      * /etc/squid/squid.conf 파일 내용 추가 (맨 상단) * 이후 방화역 비활성화/ systemctl stop squid      * 웹 브라우저 > 메뉴 > 네트워크설정 > 연결설정에서 프록시,포트 설정      * 연결 거부 확인 (squid를 정지시켰기 때문에 정상 반응임)        * server squid 시스템 재시작 후 client 인터넷 연결 확인      * 시작 > 설정 > 네트워크 및 인터넷 > 프록시 * 자동으로 설정 검색 off / 프록시 서버 사용 on 내용추가      * winclient 연결 성공 확인 * 보안을 위한 네트워크 설계 * 방화벽이란 * 외부의 공개된 네트워크와 내부의 사설 네트워크 사이에 자리잡고, 외부와 내부에 전달되는 트래픽을 ‘정책(Policy)’에 의해서 허용/거부하는 역할을 하는 컴퓨터나 장치를 말함 * 내부의 사용자는 외부의 인터넷을 이용하면서, 외부에서는 내부로 침입할 수 없게 하는 방법 중 가장 보편적으로 많이 사용하는 방법이 사설IP(Private IP)라고 흔히 불리는 nonroutable IP 주소를 이용함 * 사설IP의 주소 범위는 * 10.0.0.0 ~ 10.255.255.255, 172.16.0.0 ~ 172.31.255.255, 192.168.0.0~192.168.255.255 세 범위가 있음 * 사설IP주소의 컴퓨터가 외부의 인터넷으로 접속할 수 있도록 해주는 방법을 IP마스커레잉딩(Masquerading)이라고 함      * 보편적인 회사 네트워크 구성      * 실습에서 구현할 네트워크 구성 * 방화벽 컴퓨터 구축 실습      * server(b) 네트워크어뎁터 > 기존 NET 에서 변경 후 확인      * 현재 고정된 ip(192.168.111.100)의 변경을 위해 /etc/netplan/00-installer-config.yaml 파일 수정 * addresses, gateway, namesevers 수정      * ip addr 명령어로 주소 확인      * ping 명령어로 인터넷 연결 확인 (접속 불가) // 게이트웨이를 아직 생성하지 않음        * Client 네트워크 어뎁터 설정 변경 후 인터넷 > 연결 - 시스템 설정 모듈 > ipv4 방법 수동 / 주소 추가      * 재부팅 후 client 주소 확인 가능 (정상적으로 적용) * ping 명령어로 연결 확인 (연결 x)      * server에 랜카드(네트워크 어뎁터) 추가 생성 * 기존에 사용하던 192.168.111.100, 추가할 10.1.1.1 총 2개의 어뎁터      * ens37 ipv4 설정 * 게이트웨이는 ens 33이 실행하기 때문에 필요가 없음 (ens37 자신이 게이트웨이)      * ens33의 설정 (유지) 외부 인터넷과 연결상태 양호      * 재부팅 후 ifconfig로 주소 확인      * /etc/sysctl.conf 파일 28행 주석 제거      * 설정한 ip가 포워딩될 수 있도록 파일 생성 후 확인      * iptable 초기화      * 사설네트워크가 server를 통해서 외부에 접촉 가능을 위한 명령어 추가      * 위 명령어로 외부 접촉을 허용      * 변경 내용 저장        * ping, 웹 브라우저 등 연결 확인 * 외부 컴퓨터는 Client가 아닌 방화벽 컴퓨터인server가 접속했다고 인지 * server(b) 웹서버를 만들어 외부에서 허용가능하게 만드는 실습 * apt install apapche2 * allow http * cd /var/www/html > 기존에 index.html 삭제 후 다시 생성 * 작성할 내용 추가한 뒤 시스템 재시작 (systemctl restart apache2) * server(b)웹서버 생성 완료      * 정책 추가 * ens33 으로 80port 요청이 오면 10.1.1.20 (serverb webserver) 로 연결해 줌      * 저장 후 방화벽 비활성화      * 외부 사용자인 Winclient에서 192.168.111.100 접속하니 serverB로 접속시킨 모습 |