SUN 교사

역삼
공과대학교

네트워크 인프라 구축 및 보안 프로젝트

이남혁
이정훈
강버들
백정이
장성주
전보라

목차

1. 프로젝트 개요

프로젝트 구축 목적

1

내부망 기반의 안정적 네트워크 인프라 구축

사무동·강의동·서버존 등 각 구역을 분리하여 통신
충돌 없이 안정적으로 연결되는 내부망 환경 설계

2

DNS·FTP·TFTP 등 주요 서비스 직접 운영

DNS·FTP·TFTP 등 주요 내부 사용자들이 외부망 없
이도 도메인 조회, 파일 전송, 시스템 관리가 가능한
자체 서비스 구축.서비스 직접 운영

3

권한 관리 체계 확립

사용자와 그룹별 접근 권한을 구분하여 불필요한
접근을 제한하고 관리 효율성을 향상

4

보안 정책 관리 및 강화

방화벽 설정과 포트 제어를 통해 내부망 침입을
차단하고 안전한 서비스 운영을 유지

1. 프로젝트 개요

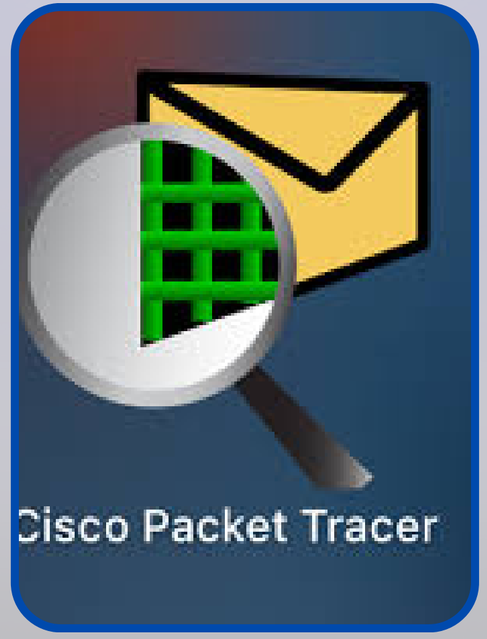
구축 목표

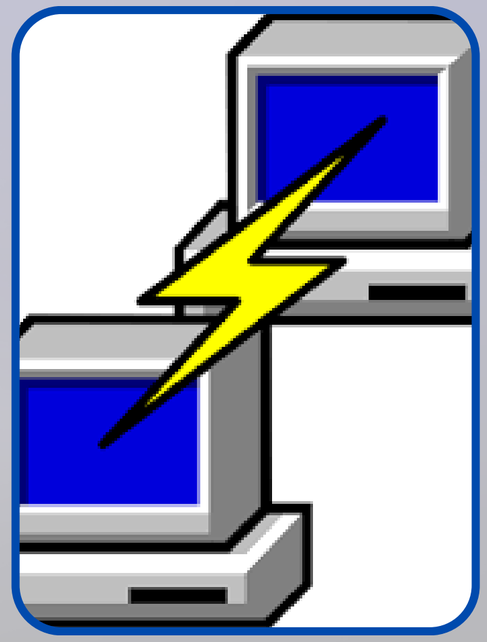
역삼공과대학교 내부망 보안
네트워크 설계 및 서비스 운영

1. 프로젝트 개요

수행 환경

VMWARE 17.X
ROCKY LINUX 8.10
KALI LINUX (DEBIAN 10.X - 64BIT)
PACKET TRACER 8.2.2
GNS3 1.5.3
PUTTY RELEASE 0.83





2. 팀원 및 파트 소개

시스템 구축

담당자

강버들
장성주

네트워크 설계

담당자

백정이
이남혁
장성주

보안 정책

담당자

이정훈
전보라

서비스 운영

담당자

백정이
이남혁

통합 관리

담당자

이정훈
전보라

3. 파트별 작업 소개 - 시스템 구축 (운영체제 설치)

설치 환경 & 사양

항목	내용
OS 버전	Rocky Linux 8.10
ISO 파일	Rocky-8.10-x86_64-dvd1.iso
디스크	20GB
메모리	4GB

- 안정성과 호환성이 뛰어난 록키리눅스 **8.10** 버전을 선택
- 기본 메모리 **4GB**와 디스크 **20GB**를 배정하여 실습과 서비스 구동에 충분한 환경을 구성

파티션

적재 지점	용량	파일시스템
/boot	1G	ext4
/home	1G	ext4
/var	4G	ext4
/usr	7G	ext4
swap	2G	swap
/	5G	ext4

- 사용자 정의 파티션을 설정하여 각 디렉터리의 역할에 따라 공간을 효율적으로 분배
- 파티션을 **/boot, /home, /var, /usr, /swap, /** 으로 세분화하여 관리 편의성과 장애 대응성 향상

설치 과정 설정

구분	설정값
설치 목적지	수동 파티션 구성
네트워크	ON / DHCP 자동 할당
소프트웨어 선택	서버 GUI + 레거시 UNIX 호환성
사용자 생성	admin + root 설정
SELinux 모드	disabled

- 최초 부팅 싱글 부팅 모드로 진입, **SELinux**를 **disabled**로 변경하여 실습 및 서비스 테스트 시 불필요한 접근 제한 최소화
- **GUI** 환경 및 사용자 설정을설치 중에 완료함으로써 부팅 직후 바로 운영이 가능한 환경을 구축

3. 파트별 작업 소개 - 시스템 구축 (운영체제 설치)

VMnet 구성

VMnet 번호	할당 PC	타입	DHCP	대역	서브넷 마스크
1	FTP 서버	Host-only	X	63.63.63.0	255.255.255.248
2	TFTP 서버	Host-only	X	63.63.63.8	255.255.255.248
3	DNS 서버	Host-only	X	63.63.63.16	255.255.255.248
8	외부 통신	NAT	O	192.168.10.0	255.255.255.0

- 각 서버를 독립된 네트워크 대역으로 분리하여 트래픽 간섭을 방지하고, 서비스별로 관리가 용이하도록 구성
- Host-only 모드를 사용해 외부 네트워크로부터 격리된 실습 환경을 구현했으며, NAT(VMnet8)는 인터넷 통신용으로만 제한
- DHCP를 비활성화하고 수동 IP를 설정함으로써 IP 충돌을 방지하고 일관된 주소 체계를 유지
- 설정 파일(/etc/sysconfig/network-scripts/ifcfg-ens33)을 직접 수정하여 불필요한 항목을 제거하고 최소 구성 유지

서비스 구성

서비스	FTP	TFTP	DNS
버전	vsftpd-3.0.3-36.el8.x86_64	ftp-server-5.2-27.el8.x86_64	bind-9.11.36-16.el8_10.4.x86_64
ens33 설정	DEVICE=ens33 ONBOOT=yes IPADDR=63.63.63.1 NETMASK=255.255.255.248 GATEWAY=63.63.63.6 DNS1=168.126.63.1	DEVICE=ens33 ONBOOT=yes IPADDR=63.63.63.9 NETMASK=255.255.255.248 GATEWAY=63.63.63.14 DNS1=168.126.63.1	DEVICE=ens33 ONBOOT=yes IPADDR=63.63.63.17 NETMASK=255.255.255.248 GATEWAY=63.63.63.22 DNS1=168.126.63.1

3. 파트별 작업 소개 - 시스템 구축 (권한 부여 및 생성)

FTP-계정

순번	계정	소속 그룹	보조 그룹	UID
1	admin	admin	-	1000
2	stud1	students	-	1001
3	stud2	students	-	1002
4	profe1	professors	-	1003
5	profe2	professors	-	1004
6	mana1	managers	-	1005
7	mana2	managers	-	1006
8	admis1	admissions	-	1007
0	admis2	admissions	-	1008

FTP-그룹

순번	그룹	GID
1	admin	1000
2	tftp	1001
3	netegineer	1002
4	managers	1003
5	admissions	1004

FTP 디렉터리 권한

디렉터리	경로	권한	소유자:그룹
college	/college	**755**	root:root
ftp	/college/ftp	**2775**	admin:ftp
professor	/college/ftp/professor	**2774**	admin:professors
student	/college/ftp/student	**774**	admin:students
manage	/college/ftp/manage	**2754**	admin:managers
admission	/college/ftp/admission	**2774**	admin:admissions

- 각 서버별로 역할 기반 계정과 그룹을 세분화해 관리 효율성과 보안을 강화
- FTP 서버는 학생, 교수, 관리자, 입학처 등 부서별 그룹을 구성하고, setgid를 적용해 그룹 단위 협업 환경 지원

3. 파트별 작업 소개 - 시스템 구축 (권한 부여 및 생성)

TFTP-계정

순번	계정	소속 그룹	보조 그룹	UID
1	admin	admin	-	1000
2	admin1	admin	tftp	1001
3	net1	neteginner	tftp	1002
4	net1	netegineer	tftp	1003

TFTP-그룹

순번	그룹	GID
1	admin	1000
2	tftp	1001
3	netegineer	1002

DNS-계정

순번	계정	소속 그룹	보조 그룹	UID
1	admin	admin	-	1000
2	admin1	admin	dns	1001
3	net1	neteginner	dns	1002
4	net1	netegineer	dns	1003

DNS-그룹

순번	그룹	GID
1	admin	1000
2	netengineer	1001
3	dns	1002

- TFTP와 DNS 서버는 네트워크 엔지니어용 계정을 별도로 구성하여 서비스 접근을 구분
- 모든 디렉터리의 소유자·그룹·권한을 명확히 설정해 잘못된 접근이나 파일 충돌을 방지

3. 파트별 작업 소개 - 네트워크 설계 (네트워크 대역 설정)

서버 존 (DMZ, Static NAT)

구분	내부 IP	공인 IP	비고
FTP 서버	63.63.63.1/29	3.3.3.10	DB 및 문서 파일 저장
TFTP 서버	63.63.63.9/29	3.3.3.20	장비 설정 파일 관리
DNS 서버	63.63.63.17/29	3.3.3.30	내부 DNS 서비스

강의동 (교수실 & 강의실) — PAT

구분	내부 네트워크 대역	NAT 공인 대역	게이트웨이	비고
3층 교수실	192.168.53.0/27	2.2.2.0/30	192.168.53.1	게임/보안/디자인/IT
2층 C·D 강의실	192.168.53.64/26	2.2.2.0/30	192.168.53.65	실습 강의실
1층 A·B 강의실	192.168.53.128/26	2.2.2.0/30	192.168.53.129	실습 강의실

사무동 (행정/입학 부서) — PAT

구분	내부 네트워크 대역	NAT 공인 대역	게이트웨이	비고
관리부	10.0.1.64/28	1.1.1.0/30	10.0.1.78	2층 관리부
입학센터	10.0.1.80/28	1.1.1.0/30	10.0.1.94	1층 입학처

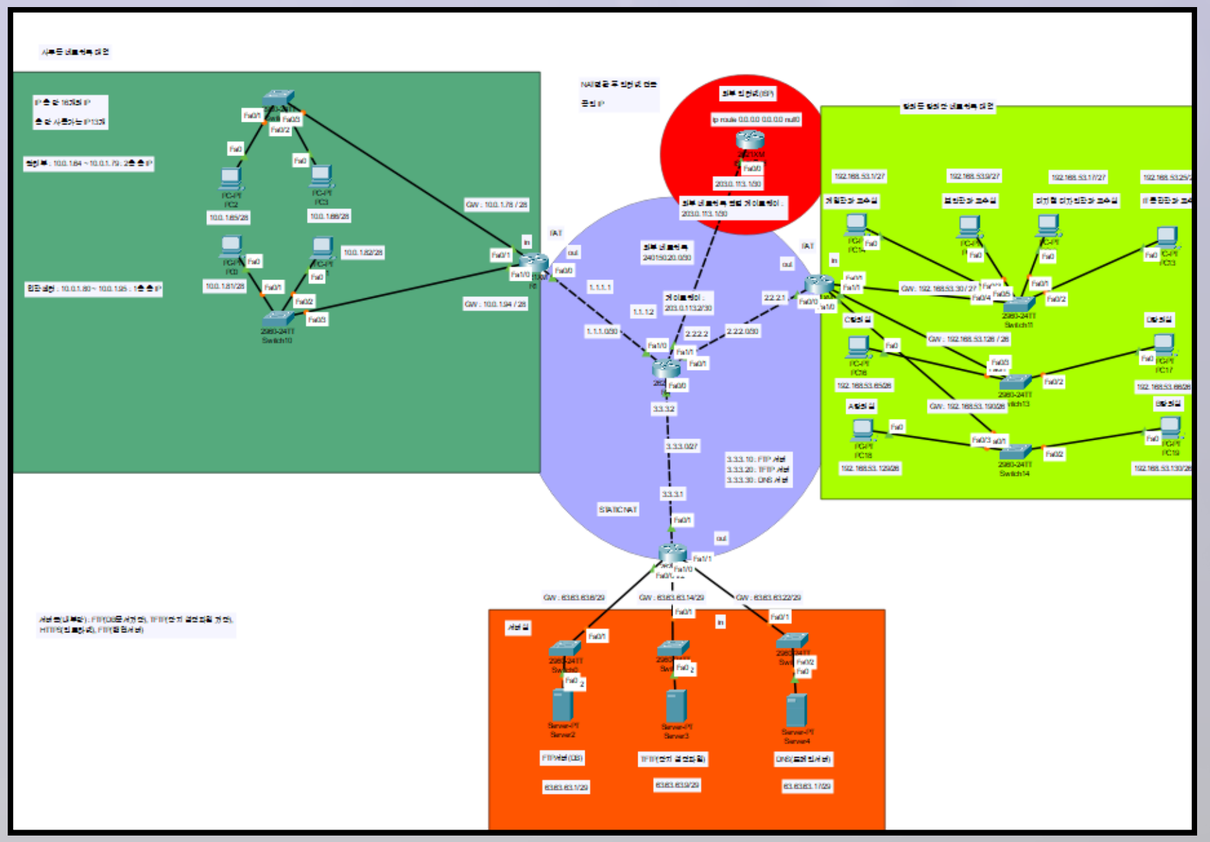
강의동 (교수실 & 강의실) — PAT

구분	네트워크 대역	장비	IP 주소	설명
외부 게이트웨이	203.0.113.0/30	R4 ↔ ISP Router	R4: 203.0.113.2ISP: 203.0.113.1	전체 트래픽 최종 출구

3. 파트별 작업 소개 - 네트워크 설계 (네트워크 대역 설정)

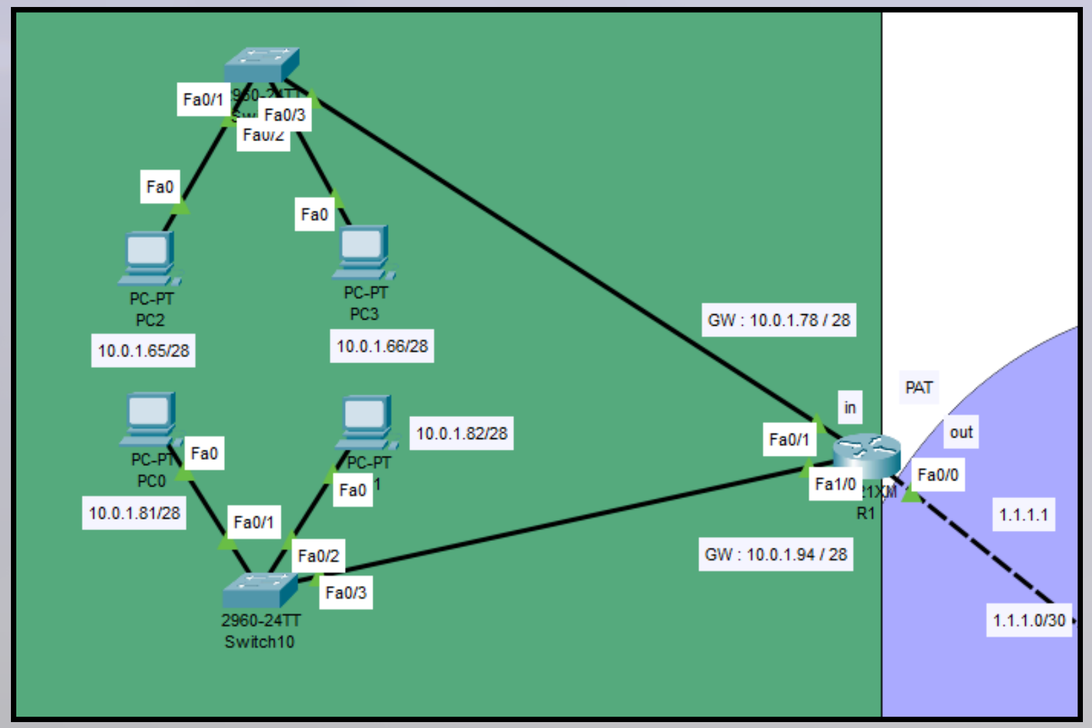
NAT 방식 요약

구분	NAT 방식	공인 IP 대역	대상 구역
FTP / TFTP / DNS	Static NAT	3.3.3.x	DMZ 서버존
사무동	PAT	1.1.1.0/30	행정 + 입학
강의동	PAT	2.2.2.0/30	교수실 + 강의실
외부 연결	-	203.0.113.0/30	ISP 연결



3. 파트별 작업 소개 - 네트워크 설계 (토폴로지 구성)

사무동 네트워크



네트워크 대역 할당 이유

필요한 만큼만 할당하고, 불필요한 낭비를 줄인 효율적 설계

NAT 방식 : PAT

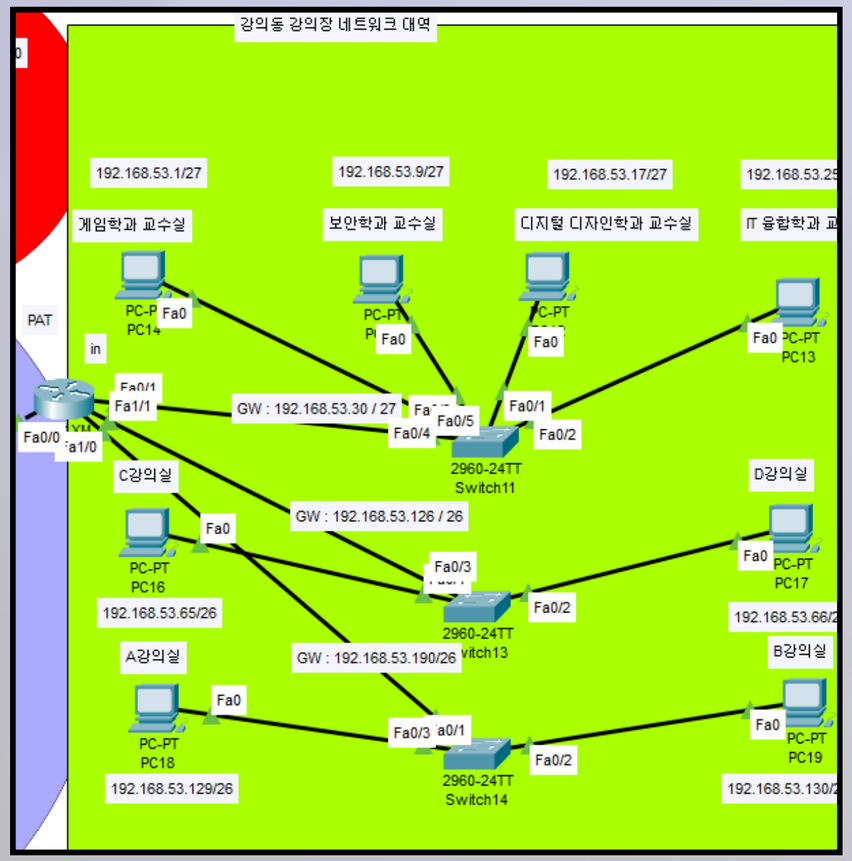
한정된 공인 IP 자원을 효율적으로 활용하면서도 관리 통제

보안 정책 고려

행정업무 중심의 안정성과 신뢰성을 확보한 네트워크 설계

3. 파트별 작업 소개 - 네트워크 설계 (토폴로지 구성)

강의동 네트워크



네트워크 대역 할당 이유

사용자 수가 많아 대역을 넓게 확보하여 IP 충돌 방지 및 관리 효율 향상

NAT 방식 : PAT

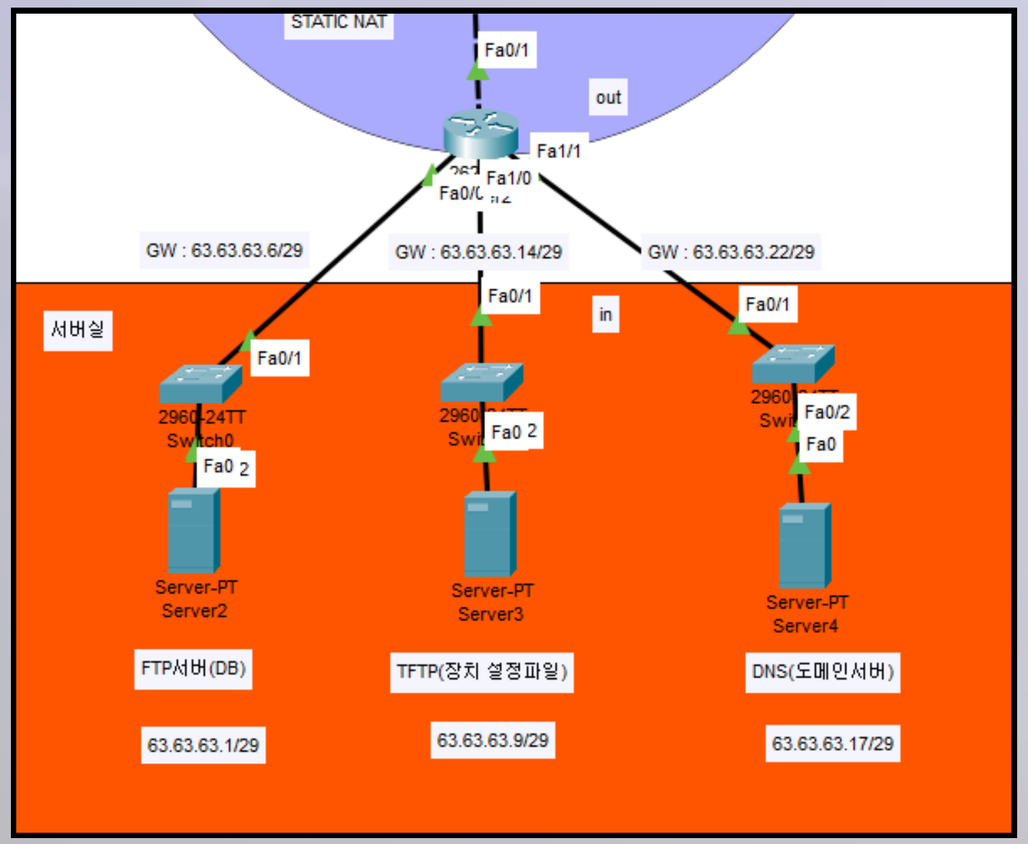
내부 사용자는 개별 IP 유지,
외부엔 단일 IP(2.2.2.2)로 표현되어 공인 IP 자원 절약

보안 정책 고려

실습 중 불필요한 접근을 차단하고 교육망의 안정성을 확보

3. 파트별 작업 소개 - 네트워크 설계 (토폴로지 구성)

서버존 네트워크



네트워크 대역 할당 이유

서버별로 독립된 스위치 포트를 구성해 확장성과 유지보수성 확보

NAT 방식 : STATIC NAT

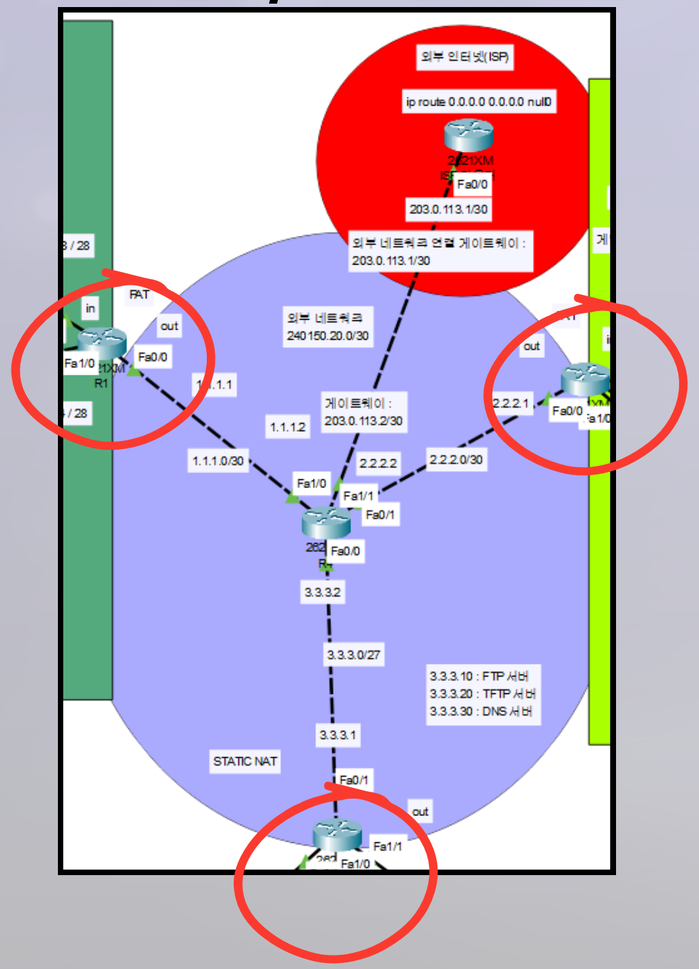
외부에서도 서버 접근이 가능해야 하므로
내부 IP와 공인 IP를 1:1로 고정 매핑

보안 정책 고려

서버 보호 및 침입 위험 최소화

3. 파트별 작업 소개 - 네트워크 설계 (토폴로지 구성)

NAT 설정 / 외부 인터넷 연결



NAT 라우터 설계 이유

학교 전체의 “인터넷 출구 게이트웨이

NAT 및 라우팅 구조

공인 IP를 단일화해 관리 효율과 보안성 확보

보안 정책 고려

외부에서 내부로 직접 접근 불가 — 모든 통신은 NAT를 거쳐야 함

3. 파트별 작업 소개 - 보안 정책 (보안 공격 유형과 대응 방안)

firewalld 설정

항목	명령어	설명
FTP 서버	firewall-cmd --permanent --add-port=21/tcp	FTP 포트 허용 추가
	firewall-cmd --permanent --add-service=ftp	FTP 서비스 허용 추가
TFTP 서버	firewall-cmd --permanent --add-port=69/udp	TFTP 포트 허용 추가
	firewall-cmd --permanent --add-service=tftp	TFTP 서비스 허용 추가
DNS 서버	firewall-cmd --permanent --add-service=dns	DNS 서비스 허용 추가
	firewall-cmd --permanent --add-port=53/udp firewall-cmd --permanent --add-port=53/tcp	DNS 포트 허용 추가
공통 적용 사항	firewall-cmd --permanent --add-port=22/tcp firewall-cmd --permanent --add-service=ssh	SSH 포트 및 서비스 허용 추가
	firewall-cmd --permanent --add-icmp-block={echo-request,echo-reply,timestamp-reply,timestamp-request}	ICMP 메세지 차단
	firewall-cmd --permanent --direct --add-rule ipv4 filter OUTPUT 0 -p icmp --icmp-type 3 -j DROP	ICMP Type 3 관련 규칙 추가

3. 파트별 작업 소개 - 보안 정책 (보안 공격 유형과 대응 방안)

설정 파일 적용

파일	설정 값	설명
/etc/ssh/sshd_config	AllowGroups admin	admin이라는 그룹에 속한 사용자들만 SSH를 통해 접속할 수 있도록 제한
	PermitRootLogin no	root사용자의 ssh 직접접근 차단 설정
	PasswordAuthentication yes	SSH 접속 시 사용자 인증을 위해 비밀번호 입력을 허용
/etc/vsftpd/vsftpd.conf	userlist_file=/etc/vsftpd/user_list	사용자 목록이 저장된 파일의 경로를 지정
	userlist_enable=YES	/etc/vsftpd/user_list 파일에 정의된 사용자 목록을 참조하여 FTP 접근을 제어
	userlist_deny=NO	userlist에 있는 사용자를 모두 허용
/etc/crontab	• 0 9 * * 1 root find / -xdev \(-nouser -o -nogroup \) -exec chown root:root {} \; >> /var/log/cron_fix.log 2>&1	소유자 또는 소유그룹이 없는 파일 소유자 및 소유권한 자동 변경 설정
/etc/login.defs	PASS_MAX_DAYS 90	최대 비밀번호 사용일을 90일로 지정(이후 변경해야함)
	PASS_MIN_DAYS 1	비밀번호를 변경한 후 최소 1일 이후 변경 가능
	PASS_MIN_LEN 10	최소 비밀번호 길이를 10으로 지정
	PASS_WARN_AGE 7	비밀번호 만료 7일 전에 경고 메시지 표시

3. 파트별 작업 소개 - 보안 정책 (보안 공격 유형과 대응 방안)

sysctl 설정

항목	설정 값	설명
#시스템의 커널 파라미터 설정 파일 /etc/sysctl.d/99-security.conf	net.ipv4.conf.all.accept_redirects = 0	라우터 리다이렉트 차단(ICMP Redirect 공격 대응)
	net.ipv4.conf.all.send_redirects = 0	송신 리다이렉트 차단(ICMP Redirect 공격 대응)
	net.ipv4.tcp_syncookies = 1	SYN Cookies 활성화 (TCP SYN Flooding 공격 대응)
	net.ipv4.conf.all.rp_filter = 1 net.ipv4.conf.default.rp_filter = 1	역방향 경로 필터링 활성화 (IP Spooing 공격 대응)

3. 파트별 작업 소개 - 서비스 운영 (FTP 서버 설정)

설치 & 서비스 관리 및 방화벽 설정

작업	명령어	설명
vsftpd 설치	sudo dnf install -y vsftpd	FTP 서버 설치
데몬 즉시 시작	sudo systemctl start vsftpd	서비스 시작
서비스 활성화(부팅 시 자동)	sudo systemctl enable vsftpd	자동 실행
데몬 재시작	sudo systemctl restart vsftpd	변경 적용
서비스 상태 확인	sudo systemctl status vsftpd	로그·상태 확인

작업	명령어	설명
FTP 서비스 허용	sudo firewall-cmd --permanent --add-	FTP 포트 자동 등록
패시브 포트 허용(선택)	sudo firewall-cmd --permanent --add-	Notion 설정 기준
규칙 적용	sudo firewall-cmd --reload	반드시 실행

3. 파트별 작업 소개 - 서비스 운영 (FTP 서버 설정)

vsftpd.conf 주요 옵션 설정

항목	설정 내용	설명
익명 로그인 제한	anonymous_enable=NO	보안
로컬 계정 허용	local_enable=YES	/etc/passwd 계정
쓰기 허용	write_enable=YES	업/삭제 허용
사용자 루트 제한	chroot_local_user=YES	탈출 방지
쓰기 가능 chroot 허용	allow_writeable_chroot=YES	보안 주의
로그인 홈 지정	local_root=/college/ftp	홈 디렉토리
패시브 모드 설정	pasv_enable=YES	패시브 on
SSL (선택)	ssl_enable=YES	TLS 암호화

3. 파트별 작업 소개 - 서비스 운영 (FTP 서버 설정)

ftp 서버 도메인명으로 접속 완료

```
C:\Users\qorwj>ftp 63.63.63.1
63.63.63.1에 연결되었습니다.
220 (vsFTPd 3.0.3)
200 Always in UTF8 mode.
사용자(63.63.63.1:(none)): stud1
331 Please specify the password.
암호:

230 Login successful.
ftp>
```

professor 디렉터리에 파일 업로드, 서버에서 확인

```
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
admssion
manage
professor
student
226 Directory send OK.
ftp: 0.00초 20.50KB/초
ftp> cd professor
250 Directory successfully changed.
ftp> put professor.txt
200 PORT command successful. Consider using PASV.
150 Ok to send data.
226 Transfer complete.
ftp>
```

```
[root@localhost ~]# ls -l /college/ftp/professor/
합계 0
-rw-r--r-- 1 profe1 professors 0 10월  27 05:09 professor.txt
[root@localhost ~]#
```

3. 파트별 작업 소개 - 서비스 운영 (FTP 서버 설정)

student 디렉터리에서 파일 삭제 작업 실패

```
ftp> cd student
250 Directory successfully changed.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
student.txt
226 Directory send OK.
ftp: 0.00초 16000.00KB/초
ftp> delete student.txt
550 Delete operation failed.
```

professor 디렉터리에서 파일 삭제 작업 성공

```
ftp> pwd
257 "/professor" is the current directory
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
professor.txt
226 Directory send OK.
ftp: 0.00초 18000.00KB/초
ftp> delete professor.txt
250 Delete operation successful.
```

3. 파트별 작업 소개 - 서비스 운영 (FTP 서버 설정)

루트 디렉터리에서 상위 경로로 이동 불가

```
ftp> pwd
257 "/" is the current directory
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
admssion
manage
professor
student
226 Directory send OK.
ftp: 0.00초 41.00KB/초
ftp> cd ..
250 Directory successfully changed.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
admssion
manage
professor
student
226 Directory send OK.
ftp: 0.00초 41.00KB/초
ftp> pwd
257 "/" is the current directory
```

/var/log/xferlog 에서 로그 기록 확인

```
-rw-r--r-- 1 profe1 professors 16 10월  28 01:14 professortest2.txt
[root@localhost professor]#
[root@localhost professor]#
[root@localhost professor]#
[root@localhost professor]#
[root@localhost professor]# cat /var/log/xferlog
Tue Oct 28 01:13:28 2025 1 ::ffff:2.2.2.1 16 /professor/professortest2.txt b _ i r profe1 ftp 0 * c
Tue Oct 28 01:14:59 2025 1 ::ffff:2.2.2.1 16 /professor/professortest2.txt b _ i r profe1 ftp 0 * c
[root@localhost professor]#
```

3. 파트별 작업 소개 - 서비스 운영 (TFTP 서버 설정)

설치 & 서비스 활성화 표

작업	명령어	설명
TFTP 패키지 설치	sudo dnf -y install tftp-server	TFTP 서버 설치
소켓 활성화	sudo systemctl enable tftp.socket	부팅 시 자동시작
소켓 시작	sudo systemctl start tftp.socket	즉시 실행
상태 확인	sudo systemctl status tftp.socket	동작 확인
로그 확인	sudo journalctl -u tftp.socket -f	실시간 로그

설정 수정 표

작업	파일/명령	설명
설정파일 수정	sudo vi /usr/lib/systemd/s	systemd 설정
실행 설정	-s /tftp	상위 디렉터리 접근 차단 (TFTP 루트)
쓰기 허용	-c	파일 업로드 허용
보안 옵션	ProtectHome=yesNoNewPrivileges=ye	홈 접근 차단 / 권한상승 방지
설정 반영	sudo systemctl daemon-reload	systemd 갱신
재시작	sudo systemctl restart tftp.socket	새 설정 적용

3. 파트별 작업 소개 - 서비스 운영 (TFTP 서버 설정)

디렉터리 생성 & 권한 설정 표

작업	명령어	설명
디렉터리 생성	sudo mkdir -p /tftp/router	라우터 설정 저장 용도
디렉터리 생성	sudo mkdir -p /tftp/firmware	펌웨어 저장 용도
디렉터리 생성	sudo mkdir -p /tftp/uploads	업로드 용도
상위 디렉 권한	sudo chmod g+w /tftp	그룹 쓰기 허용
setgid 적용	sudo chmod 2775 /tftp/routersudo	생성파일 소유 그룹 유지
허가권 변경	sudo chmod 1733 /tftp/uploads	업로드 가능하도록 쓰기 권한 부여
소유권 변경	sudo chown admin:netengineer	그룹 오탈자 주의 (netengineer)

방화벽 설정 표

작업	명령어	설명
TFTP 서비스 허용	sudo firewall-cmd --permanent --add-	UDP 69 허용
방화벽 적용	sudo firewall-cmd --reload	규칙 반영

3. 파트별 작업 소개 - 서비스 운영 (TFTP 서버 설정)

TFTP서버에 파일 업로드

```
[root@localhost tftp]# chmod 662 R4_sta
[root@localhost tftp]# chown admin:netegineer R4_sta
[root@localhost tftp]# ll
합계 8
-rw-rw--w- 1 admin netegineer    0 10월  27 20:32 R4_sta
drwxrwsr-x 2 admin admin      4096 10월  26 04:21 firmware
drwxrwsr-x 2 admin netegineer 4096 10월  26 04:21 router
R4#copy sta tftp:
Address or name of remote host []? tftp.yeoksam.ac.local
Destination filename [r4-confg]? R4_sta
!!
1519 bytes copied in 0.204 secs (7446 bytes/sec)
```

TFTP서버 파일 확인

```
[root@localhost tftp]# ll
합계 12
-rw-rw--w- 1 admin netegineer 1519 10월  27 20:36 R4_sta
drwxrwsr-x 2 admin admin      4096 10월  26 04:21 firmware
drwxrwsr-x 2 admin netegineer 4096 10월  26 04:21 router
[root@localhost tftp]# cat R4_sta

!
upgrade fpd auto
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R4
!
```

3. 파트별 작업 소개 - 서비스 운영 (DNS 서버 설정)

DNS 메인 설정 (/etc/named.conf)

설정 항목	파일	설명	예제
설정 파일 수정	/etc/named.conf	listen-on, allow-query, recursion 설	sudo vi /etc/named.conf
listen-on	named.conf	DNS 요청 수신할 인터페이스 지정	listen-on port 53 { any; };
IPv6 비활성화	named.conf	IPv6 사용 안함	listen-on-v6 port 53 { none; };
zone 파일 저장 경로 지정	named.conf	zone 파일 위치	directory "/var/named";
질의 허용 네트워크	named.conf	허용 IP 대역 지정	(아래 표 참고)
재귀 질의 허용	named.conf	내부 DNS 캐싱 기능	recursion yes;

BIND 설치 (DNS 서버 패키지)

작업	명령어	비고
BIND 설치	sudo dnf -y install bind	named 포함

질의 허용(allow-query) 네트워크

네트워크	의미
63.63.63.0/29	FTP 서버존
63.63.63.8/29	TFTP 서버존
63.63.63.16/29	DNS 서버존
1.1.1.0/30	사무동 NAT 라우터
2.2.2.0/30	강의동 NAT 라우터
3.3.3.0/27	공인(서버존)

3. 파트별 작업 소개 - 서비스 운영 (DNS 서버 설정)

zone 파일 연결 설정 (/etc/named.rfc1912.zones)

작업	명령어/파일	설명	비고
zone 등록	sudo vi /etc/named.rfc191	zone 파일 경로 지정	domain ↔ zone 파일 연결
정방향 Zone 선언	zone "yeoksam.ac.local"	.zone 파일 지정	/var/named/yeoksam.ac.local.zone

zone 파일 작성 (/var/named/*.zone)

작업	파일	설명	예시
정방향 zone 생성	/var/named/yeoksam.ac.local.zone	도메인 → IP(DB)	ftp/tftp/dns/www
TTL 설정	zone 파일 내부	캐시 유지시간 설정	1D 또는 86400
A 레코드 등록	ftp/tftp/dns → IP	내부 서버 주소 매핑	아래 표

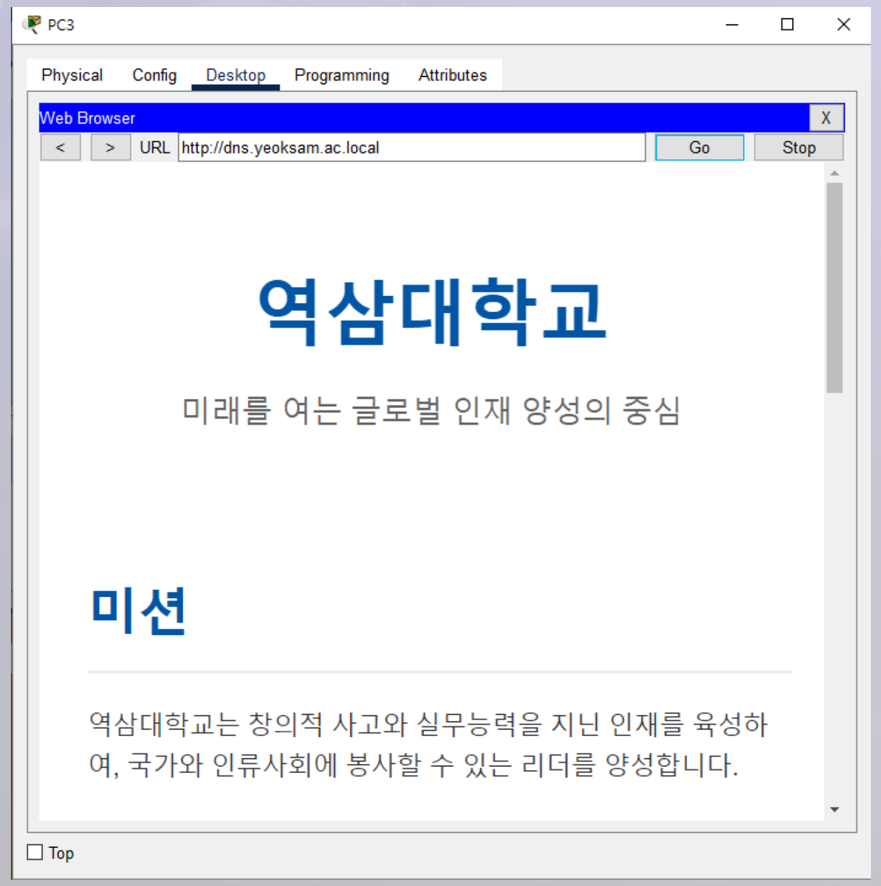
서비스 활성화 & 방화벽 설정

작업	명령어	설명
named 데몬 활성화	sudo systemctl enable named	자동 실행 등록
named 재시작	sudo systemctl restart named	설정 적용
named 상태 확인	sudo systemctl status named	오류 확인
방화벽 DNS 허용	sudo firewall-cmd --permanent --add-	TCP/UDP 53 허용
방화벽 반영	sudo firewall-cmd --reload	정책 적용

도메인 이름	서버 용도	매핑된 ip 주소
ftp.yeoksam.ac.local	내부 사용자용	3.3.3.10
tftp.yeoksam.ac.local	관리용	3.3.3.20
dns.yeoksam.ac.local	내부 전용 네임서버	3.3.3.30

3. 파트별 작업 소개 - 서비스 운영 (DNS 서버 설정)

사무동 → dns서버 접근



접근 가능한 외부망 공인 ip주소로 정상 반환

```
[root@localhost ~]# nslookup ftp.yeoksam.ac.local
Server:         3.3.3.30
Address:        3.3.3.30#53

Name:   ftp.yeoksam.ac.local
Address: 3.3.3.10

[root@localhost ~]# nslookup tftp.yeoksam.ac.local
Server:         3.3.3.30
Address:        3.3.3.30#53

Name:   tftp.yeoksam.ac.local
Address: 3.3.3.20

[root@localhost ~]# nslookup dns.yeoksam.ac.local
Server:         3.3.3.30
Address:        3.3.3.30#53

Name:   dns.yeoksam.ac.local
Address: 3.3.3.30
```

3. 파트별 작업 소개 - 통합 관리

GNS 설정

항목	명령어	설명
VPCS	ip IP주소/Prefix 게이트웨이주소	IP 주소, 서브넷 마스크, 게이트웨이 주소 설정
	ip dns DNS서버주소	DNS 주소 설정
	save	IP 정보 저장 적용
	show ip	IP 설정 정보 출력
Router	-	네트워크 설정의 라우터와 동일

5. 개선사항

1

시스템 구축 및 권한 :
계정·그룹별 접근 권한을 명확히 구분하고,
백업 및 로그 관리 체계 강화 필요

2

네트워크 설계 :
네트워크 이중화 및 2차 백업 서버 및 DMZ 구역 설계

3

서비스 운영 :
서버 접근 로그 및 자원 모니터링 시스템 도입으로
운영 효율성 강화 및 보조 DNS 서버 및 웹 서버 증설

4

보안 계획 :
정기적인 백업으로 재난 복구 계획 수립 및
로그 설정으로 모니터링 및 위협 탐지 능력 강화

6. 느낀 점

이남혁	네트워크 구성 이상으로 네트워크,보안,시스템,서비스가 유기적으로 맞물려야 진정한 내부망 환경이 완성된다는 것을 직접 느꼈다. 기술적 성취뿐만 아니라 팀워크, 리더십, 문제 해결력 면에서도 한 단계 성장할 수 있었던 경험이었다.
이정훈	보안 설정을 하며 보안을 강화할수록 안전해지지만 관리가 까다로워진다고 생각했고, 작은 실수 하나에 시스템 접속 자체가 멈출 수 있어 유의해서 작업을 진행해야한다고 생각했습니다.
강버들	인프라 구축에서는 문서 정리가 전부라는 걸 깨달았고, 매뉴얼이란 실제 업무 환경을 이루는 설계도로써 누구나 이해 가능하고 적용 가능하도록 작성하는 능력이 매우 중요하다는 걸 이해하였습니다.
백정이	네트워크 대역 설정 규칙(ex 필요호스트 당 설정 가능한 주소)을 명확히 알고있어야 함을 깨달았다. 서비스 운영 그리고 보안을 위해서 다양한 설정값, 그리고 서비스 기본 동작 원리를 알고있어야 함을 알게 되었다.
장성주	디렉토리 또는 파일마다 권한을 부여하는 방법이 쉽지 않다는 느낌을 받았고, 또한 네트워크 대역을 설정한는 방법을 정확히 알고 있어야 한다는 것을 느낄 수 있었다. 또한 네트워크에서 설정이 하나라도 겹치면 안되는 것을 느꼈다.
전보라	전체적인 네트워크 구성을 확인하고, 각 서비스를 테스트하며 기본적인 네트워크 관련 지식 및 이해도의 중요성을 느꼈습니다. 보안 공격의 유형을 알고, 해당 공격에 대한 대응 방안을 탐색한 후 리눅스 명령어를 정리하여 체계화하는 작업을 진행하며 네트워크 계층과 프로토콜에 대한 이해도를 높일 수 있었습니다.

THANK YOU

SUN교사