

여삼  
공과대학교

- 네트워크 인프라 구축 및 보안 프로젝트 -

SUN 교사

이남혁  
이정훈  
강버들  
백정이  
장성주  
전보라

# 목차

## 1 프로젝트 개요

→ 구축 목적, 구축 목표, 수행 환경

## 2 팀원 및 파트 소개

→ 역할 분담, 담당 서비스

## 3 파트 별 작업 소개

→ 시스템 구축, 네트워크 설계,  
보안 정책, 서비스 운영, 통합 관리

## 4 개선사항

→ 구축 과정에서 발생한 문제, 개선 방향 제시

## 5 느낀 점

→ 팀원 별 소감

## 6 인사

→ 마무리



# 1. 프로젝트 개요

# 1.프로젝트 개요

## 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 서비스 서버 직접 운영

DNS·FTP·TFTP 서비스를 사용자들이 내부망 내에서 도메인 조회, 파일 전송, 네트워크 장비 백업 관리가 가능한 자체 서비스 구축 및 운영

3

### 권한 관리 체계 확립

사용자와 그룹 별 접근 권한을 구분하여 불필요한 접근을 제한 및 관리 효율성을 향상

4

### 보안 정책 관리 및 강화

방화벽 설정과 설정 파일 값을 통해 공격자의 침입을 차단하고 안전한 서비스 운영을 유지

# 1.프로젝트 개요

## 구축 목표

역삼공과대학교 내부망 보안

네트워크 설계 및 서비스 운영



역삼  
공과대학교

# 1.프로젝트 개요

## 수행 환경

VMWARE 17.X

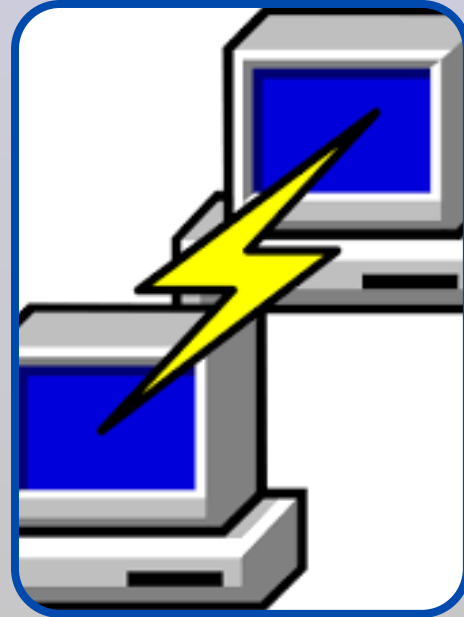
ROCKY LINUX 8.10

KALI LINUX (DEBIAN 10.X)

PACKET TRACER 8.2.2

GNS3 1.5.3

PUTTY RELEASE 0.83



## 2. 팀원 및 파트 소개

## 2. 팀원 및 파트 소개

### 시스템 구축

강버들  
장성주

### 네트워크 설계

백정이  
이남혁  
장성주

### 보안 정책

이정훈  
전보라

### 서비스 운영

백정이  
이남혁

### 통합 관리

이정훈  
전보라



### 3. 파트 별 작업 소개



# 시스템 구축 파트



# 네트워크 설계 파트

# 3. 파트 별 작업 소개 - 네트워크 설계

## 외부 인터넷

구분	네트워크 대역	장비	IP 주소	설명
외부 게이트 웨이	203.0.113.0/30	R4-ISP Router	<b>R4</b> 203.0. 113.2  <b>ISP</b> 203.0. 113.1	전체 트래픽 최종 출구

## 사무동(관리부 & 입학 센터) - PAT

구분	내부 네트워크 대 역	NAT 공인 대역	게이트웨이	비고
관리부	10.0.1.64/28	1.1.1.0/30	10.0.1.78	2층 관리부
입학 센터	10.0.1.80/28	1.1.1.0/30	10.0.1.94	1층 입학 센터

# 3. 파트 별 작업 소개 - 네트워크 설계

## 서버 존 (Static NAT)

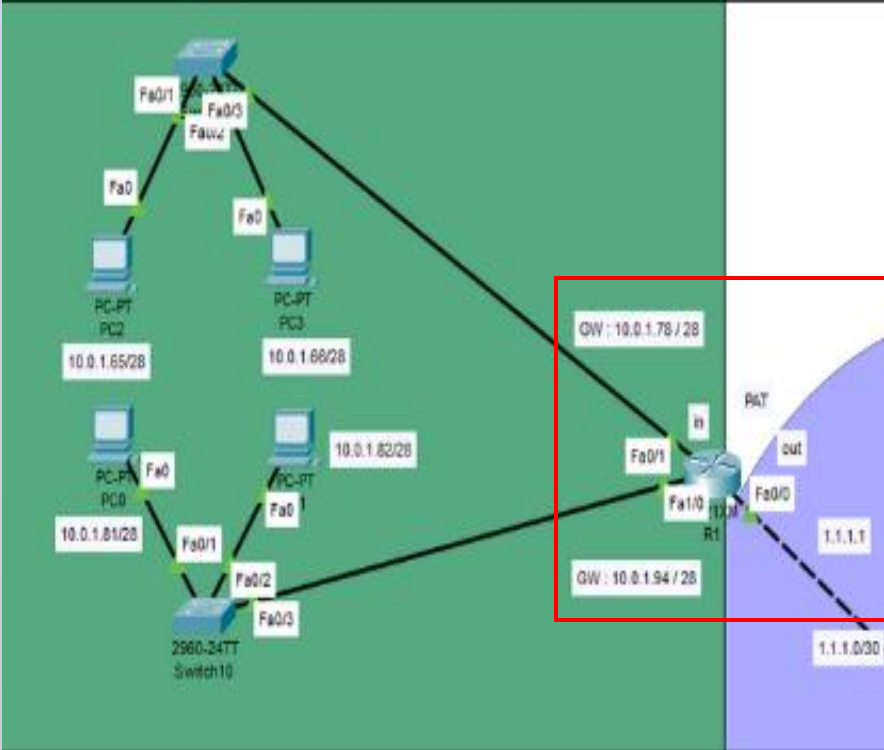
구분	내부 IP	공인 IP	비고
FTP 서버	63.63.63.1/29	3.3.3.10	DB 및 문서 파일 저장
TFTP 서버	63.63.63.9/29	3.3.3.20	장비 설정 파일 관리
DNS 서버	63.63.63.17/29	3.3.3.30	내부 DNS 서비스

## 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

## 3. 파트 별 작업 소개 - 네트워크 설계

# 사무동 네트워크



## 네트워크 대역 할당 이유

## 필요한 만큼만 할당하고, 불필요한 낭비를 줄인 효율적 설계

## NAT 방식 : PAT

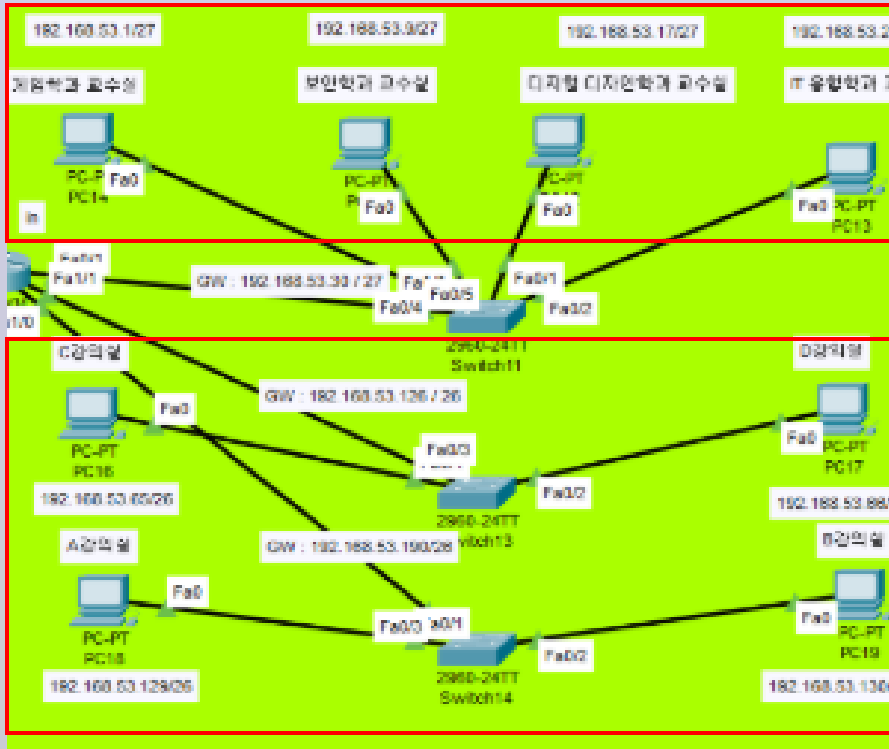
## 한정된 공인 IP 자원을 효율적으로 활용하면서도 관리 통제

# 보안 정책 고려

## 행정업무 중심의 안정성과 신뢰성을 확보한 네트워크 설계

# 3. 파트 별 작업 소개 - 네트워크 설계

## 강의동 네트워크



## 네트워크 대역 할당 이유

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

## NAT 방식 : PAT

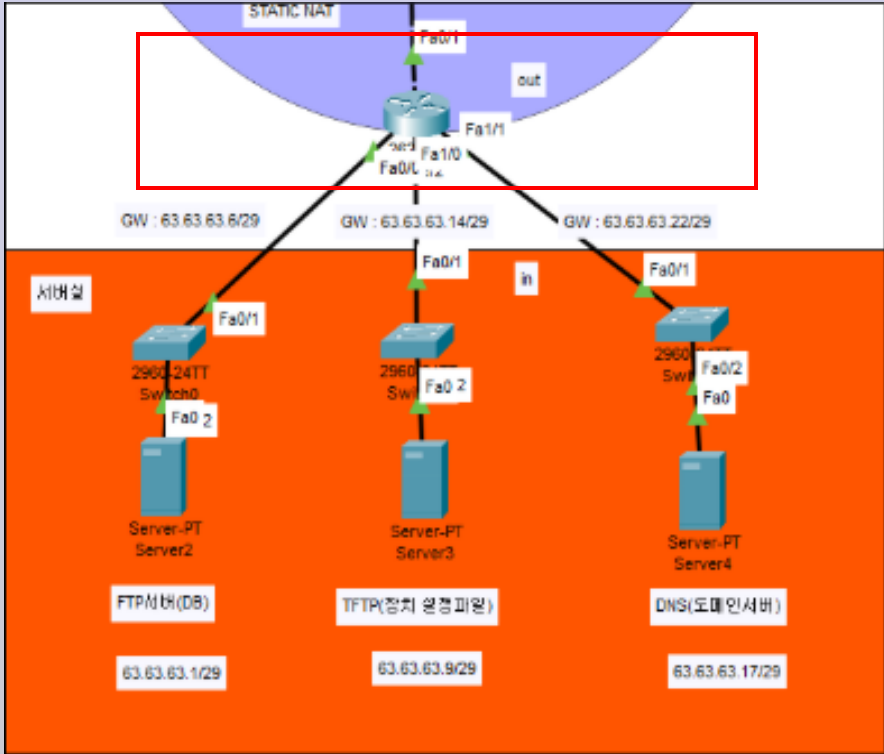
내부 사용자는 개별 IP 유지,  
외부엔 단일 IP(2.2.2.2)로 표현되어 공인 IP 자원 절약

## 보안 정책 고려

실습 중 불필요한 접근을 차단하고 교육망의 안정성 확보

## 3. 파트 별 작업 소개 - 네트워크 설계

# 서버존 네트워크



## 네트워크 대역 할당 이유

## 서버 별로 독립된 스위치 포트를 구성해 확장성과 유지보수성 확보

## NAT 방식 : STATIC NAT

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

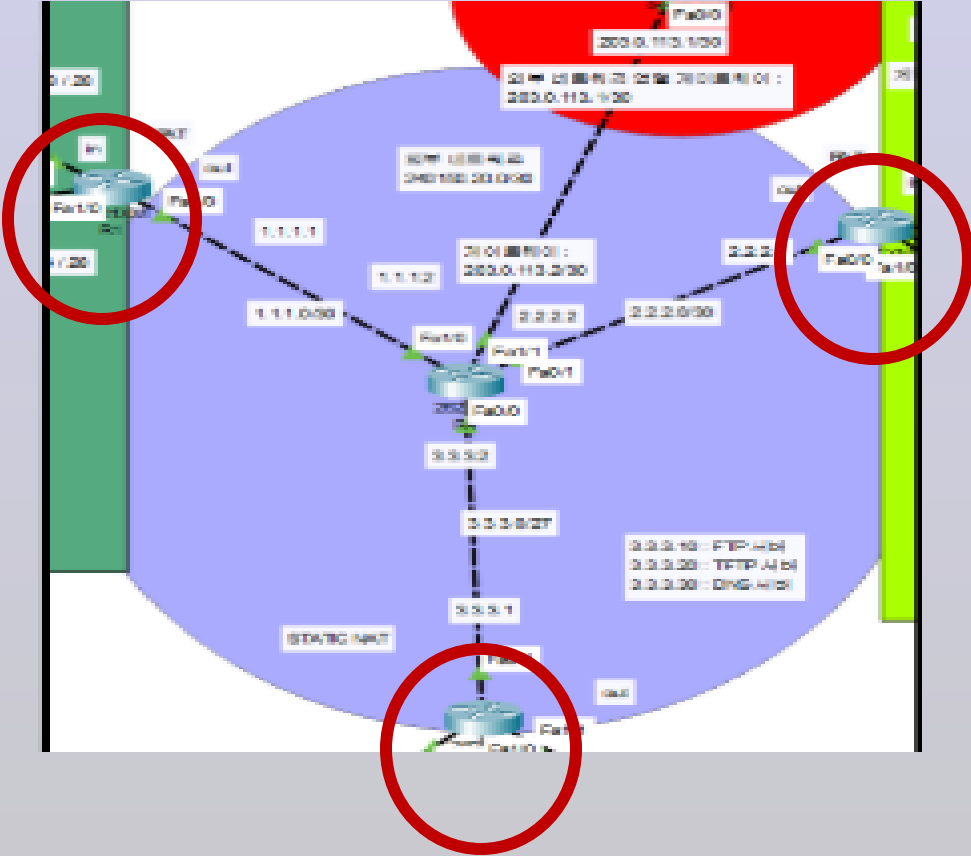
# 보안 정책 고려

## 서버 보호 및 침입 위험 최소화



## 3. 파트 별 작업 소개 - 네트워크 설계

## 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**



# 서비스 운영 파트

# 3. 파트 별 작업 소개 - 서비스 운영

## firewalld 설정

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

## 방화벽 설정

작업	명령어	설명
FTP 서비스 허용	<code>firewall-cmd --permanent --add-service=ftp</code>	FTP 서비스 자동 등록
패시브 포트 허용(선택)	<code>firewall-cmd --permanent --add-port=50000-50005/tcp</code>	자동 추적 없을 경우 허용
방화벽 적용	<code>firewall-cmd --reload</code>	규칙 반영

# 3. 파트 별 작업 소개 - 서비스 운영

## vsftpd.conf 주요 옵션 설정

항목	설정 내용	설명
익명 로그인 제한	anonymous_enable=NO	보안 강화
로컬 계정 허용	local_enable=YES	/etc/passwd 등록 계정
쓰기 허용	write_enable=YES	업로드/삭제 허용
사용자 루트 제한	chroot_local_user=YES	탈출 방지
쓰기 가능 루트 디렉터리 접근 허용	allow_writeable_chroot=YES	보안 주의
로그인 홈 지정	local_root=/college/ftp	로그인 시 위치
패시브 모드 설정	pasv_enable=YES pasv_min_port=50000(선택) pasv_max_port=50005(선택)	패시브 on 기준
SSL (선택)	ssl_enable=YES	TLS 암호화, 키/인증서 필요

# 3. 파트 별 작업 소개 - 서비스 운영

## ftp 서버 도메인 접속

```
[root@localhost ~]# ftp ftp.yeoksam.ac.local
Connected to ftp.yeoksam.ac.local (3.3.3.10).
220 (vsFTPd 3.0.3)
Name (ftp.yeoksam.ac.local:root): profel
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> _
```

```
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.
```

## 디렉터리 파일 업로드 성공

```
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
admission
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.
```

professor

# 3. 파트 별 작업 소개 - 서비스 운영

## 디렉터리 파일 삭제 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.
```

student

```
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
admission
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> |
```

## 디렉터리 파일 삭제 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.
```

professor

### 3. 파트 별 작업 소개 - 서비스 운영

루트 → 상위 경로 이동 불가

```
ftp> pwd
257 "/" is the current directory
/college/ftp
ftp> ls
227 Entering Passive Mode (3,3,3,10,82,167).
150 Here comes the directory listing.
drwxrwsr-x  2 1000    1004    4096 Oct 25 01:54 admssion
drwxrwsr-x  2 1000    1003    4096 Oct 25 01:53 manage
drwxrwsrwx  2 1000    1002    4096 Oct 27 16:23 professor
drwxrwsr-x  2 1000    1001    4096 Oct 27 15:45 student
226 Directory send OK.
ftp> cd ..
250 Directory successfully changed.
ftp> ls
227 Entering Passive Mode (3,3,3,10,73,151).
150 Here comes the directory listing.
drwxrwsr-x  2 1000    1004    4096 Oct 25 01:54 admssion
drwxrwsr-x  2 1000    1003    4096 Oct 25 01:53 manage
drwxrwsrwx  2 1000    1002    4096 Oct 27 16:23 professor
drwxrwsr-x  2 1000    1001    4096 Oct 27 15:45 student
226 Directory send OK.
ftp>
```

/var/log/xferlog 에서 로그 기록 확인

```
-rw-r--r-- 1 profel 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 profel ftp 0 * c
Tue Oct 28 01:14:59 2025 1 ::ffff:2.2.2.1 16 /professor/professortest2.txt b _ i r profel ftp 0 * c
[root@localhost professor]#
```

# 3. 파트 별 작업 소개 - 서비스 운영

## 설치 & 서비스 활성화 표

작업	명령어	설명
TFTP 패키지 설치	<code>dnf -y install tftp-server</code>	TFTP 서버 설치
소켓 활성화	<code>systemctl enable tftp.socket</code>	부팅 시 자동 시작
소켓 시작	<code>systemctl start tftp.socket</code>	즉시 실행
상태 확인	<code>systemctl status tftp.socket</code>	동작 확인

## 설정 수정 표

작업	파일/명령	설명
설정파일 수정	<code>vi /usr/lib/systemd/system/tftp.service</code>	systemd 기준 설정
실행 설정	<code>-s /tftp</code>	상위 디렉터리 접근 차단 / TFTP 루트 디렉터리 지정
쓰기 허용	<code>-c</code>	파일 업로드 허용
보안 옵션	<code>ProtectHome=yesNoNewPrivileges=yes</code>	/home 접근 차단 / 권한상승 방지
설정 반영	<code>systemctl daemon-reload</code>	서비스 설정 갱신
재시작	<code>systemctl restart tftp.socket</code>	소켓 재시작



### 3. 파트 별 작업 소개 - 서비스 운영

#### 방화벽 설정 표

작업	명령어	설명
TFTP 서비스 허용	firewall-cmd --permanent --add-service=tftp	TFTP 서비스 허용
방화벽 적용	firewall-cmd --reload	규칙 반영

#### 디렉터리 생성 & 권한 설정 표

작업	명령어	설명
디렉터리 생성	mkdir -p /tftp/router mkdir -p /tftp/firmware	라우터 설정 저장 용도, 펌웨어 저장 용도
백업용 파일 생성	touch /tftp/R4_sta	R4 설정 업로드용 파일
루트디렉터리 권한	chmod g+w /tftp	그룹 쓰기 허용
setgid 적용	chmod 2775 /tftp/router chmod 2775 /tftp/firmware	생성파일 소유 그룹 유지
허가권 변경	chmod 662 /tftp/R4_sta	업로드 가능하도록 쓰기 권한 부여
소유권 변경	chown admin:netengineer /tftp/router chown admin:admin /tftp/firmware chown admin:netengineer /tftp/R4_sta	admin 그룹 접근 가능, netengineer 그룹 설정 파일 조회 가능, 폴더 접근 가능

# 3. 파트 별 작업 소개 - 서비스 운영

## TFTP서버에 파일 업로드

```
[root@localhost tftp]# chmod 662 R4_sta
[root@localhost tftp]# chown admin:netengineer R4_sta
[root@localhost tftp]# ll
합계 8
-rw-rw--w- 1 admin netengineer 0 10월 27 20:32 R4_sta
drwxrwsr-x 2 admin admin 4096 10월 26 04:21 firmware
drwxrwsr-x 2 admin netengineer 4096 10월 26 04:21 router
R4#copy sta tftp:
Address or name of remote host []? tftp.yeoksam.ac.local
Destination filename [r4-config]? 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 netengineer 1519 10월 27 20:36 R4_sta
drwxrwsr-x 2 admin admin 4096 10월 26 04:21 firmware
drwxrwsr-x 2 admin netengineer 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. 파트 별 작업 소개 - 서비스 운영

## BIND 설치

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

## ZONE 파일 연결 설정

작업	명령어/파일	설명	비고
zone 등록	vi /etc/named.rfc1912.zones	zone 파일 경로 지정	domain ↔ zone 파일 연결
정방향 Zone 선언	zone "yeoksam.ac.local"	.zone 파일 지정	/var/named/yeoksam.ac.local.zone

# 3. 파트 별 작업 소개 - 서비스 운영

## ZONE 파일 작성

작업	파일	설명	예시
정방향 zone 생성	/var/named/yeok sam.ac.local.zone	도메인 → IP(DB)	ftp/tftp/dns
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	systemctl enable named	자동 실행 등록
named 재시작	systemctl restart named	설정 적용
named 상태 확인	systemctl status named	오류 확인
방화벽 DNS 허용	firewall-cmd --permanent --add-service=named	DNS 서비스 허용
방화벽 적용	firewall-cmd --reload	규칙 반영

# 3. 파트 별 작업 소개 - 서비스 운영

## 질의 허용 네트워크

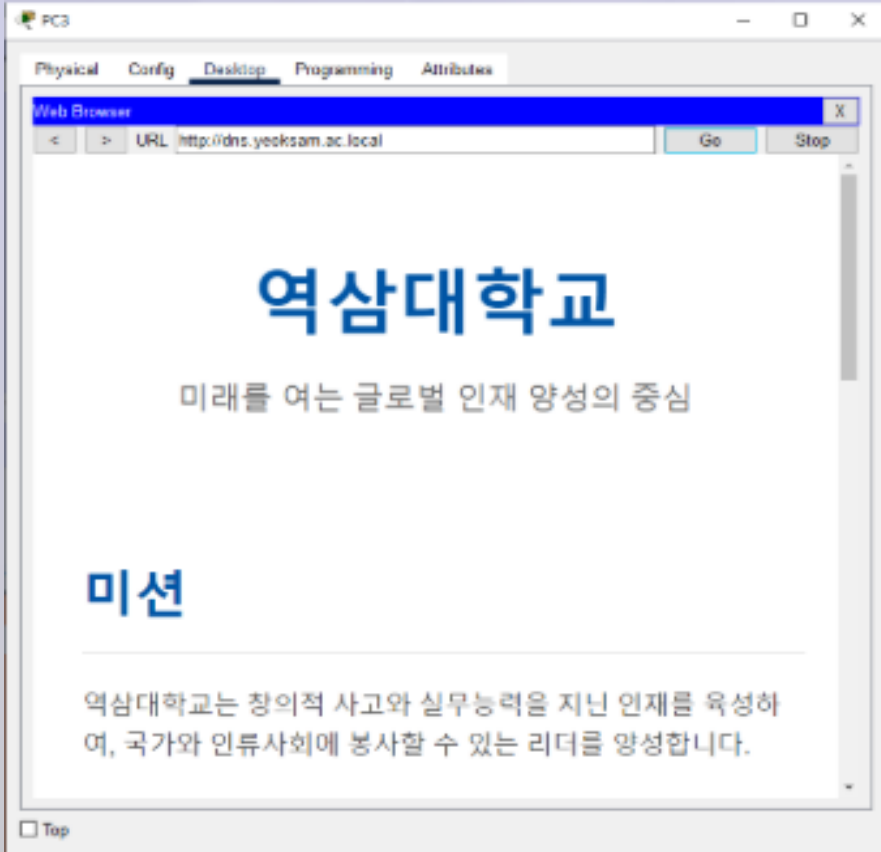
네트워크	의미
63.63.63.0/29	FTP 서버존
63.63.63.8/29	TFTP 서버존
63.63.63.16/29	DNS 서버존
1.1.1.0/30	사무동 NAT 라우터
2.2.2.0/30	강의동 NAT 라우터
3.3.3.0/27	공인(서버존)

## DNS 메인 설정

설정 항목	파일	설명	예제
설정 파일 수정	/etc/named.conf	listen-on, allow-query, recursion 설정	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	(왼쪽 표의 대역 허용)
재귀 질의 허용	named.conf	내부 DNS 캐싱 기능	recursion yes;

# 3. 파트 별 작업 소개 - 서비스 운영

사무동 → DNS 서버 접근



접근 가능한 외부 공인 IP주소 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
```

## 4. 개선사항

# 4. 개선사항

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

**2 네트워크 설계**  
네트워크 이중화 와 2차 백업 서버 및  
DMZ 구역 설계



**3 서비스 운영**  
서버 접근 로그와 자원 모니터링 시스템  
도입으로 운영 효율성 강화,  
보조 DNS 서버 및 웹 서버 증설

**4 보안 계획**  
정기적인 백업과 로그 설정으로  
재난 복구 계획 수립과 모니터링 및  
위협 탐지 능력 강화



**역삼  
공과대학교**





## 5. 느낀 점

## 5. 느낀 점

이남혁  
(총장)

네트워크 구성 이상으로 네트워크, 보안, 시스템, 서비스가 유기적으로 맞물려야 진정한 내부망 환경이 완성된다는 것을 직접 느꼈습니다. 기술적 성취뿐만 아니라 팀워크, 리더십, 문제 해결력 면에서도 한 단계 성장할 수 있었던 경험이었습니다.

이정훈  
(학장)

보안 설정을 하며 보안을 강화할수록 안전해지지만 관리가 까다로워진다고 생각했고, 작은 실수 하나에 시스템 접속 자체가 멈출 수 있어 유의해서 작업을 진행해야 한다고 생각했습니다.

강버들

인프라 구축에서는 문서 정리가 전부라는 것을 깨달았고, 매뉴얼이란 실제 업무 환경을 이루는 설계도로써 누구나 이해 가능하고 적용 가능하도록 작성하는 능력이 매우 중요하다는 것을 이해하였습니다.

## 5. 느낀 점

백정이

네트워크 대역 설정 규칙을 명확히 알고 있어야 함을 깨달았습니다.  
서비스 운영 그리고 보안을 위해서 다양한 설정 값  
그리고 서비스 기본 동작 원리를 알고 있어야 함을 알게 되었습니다.

장성주

디렉토리 또는 파일마다 권한을 부여하는 방법이 쉽지 않다는 것을 느꼈고,  
또한 네트워크 대역을 설정하는 방법을 정확히 알고 있어야 한다는 것을 느낄 수 있었습니다.  
네트워크에서 설정이 하나라도 겹치면 안되는 것을 느꼈습니다.

전보라

전체적인 네트워크 구성하고 서비스를 테스트하며 기본 지식 및 이해도의 중요성을 느꼈습니다.  
보안 공격의 유형을 알고 대응 방안을 탐색한 후 체계화하는 작업을 진행하며,  
네트워크 계층과 프로토콜에 대한 이해도를 높일 수 있었습니다.

중간 프로젝트 링크 : [https://www.notion.so/1-SafeDugout\\_-2807b112410a8118a0cad8754224c885?source=copy\\_link](https://www.notion.so/1-SafeDugout_-2807b112410a8118a0cad8754224c885?source=copy_link)

중간 프로젝트 : [https://github.com/Team1-SafeDugout/SafeDugout\\_backend.git](https://github.com/Team1-SafeDugout/SafeDugout_backend.git)

세미 프로젝트 링크 : [https://www.notion.so/2a87b112410a81809573ff810dedc291?source=copy\\_link](https://www.notion.so/2a87b112410a81809573ff810dedc291?source=copy_link)

세미 프로젝트 서버 드라이브 링크 : <https://drive.google.com/drive/folders/19FKuGD6QTXyn2zzSwXZEZDse-zZ7YOZQ?usp=sharing>



# THANK YOU



SUN교사