**Network**

목차

[**1. Network** 5](#_Toc111133372)

[**1.1. Network 장비** 5](#_Toc111133373)

[**1.2. Network 보안** 6](#_Toc111133374)

[**1.3. Network 전송방식** 7](#_Toc111133375)

[**1.4. Network 유형** 7](#_Toc111133376)

[**1.5. OSI 7계층** 8](#_Toc111133377)

[**1.6. TCP/UDP 포트** 9](#_Toc111133378)

[**1.7. Network 주소** 10](#_Toc111133379)

[**2. Subnet** 12](#_Toc111133380)

[**2.1. Subnet(서브넷)** 12](#_Toc111133381)

[**2.2. Subnet Mask** 12](#_Toc111133382)

[**2.3. Subnet 문제** 13](#_Toc111133383)

[**3. Router 설정** 17](#_Toc111133384)

[**3.1. Routing Protocol** 17](#_Toc111133385)

[**3.2. Router 설정 방법 (Packet Tracer)** 17](#_Toc111133386)

[**3.3. Subnet 문제** 21](#_Toc111133387)

[**4. 네트워크 연습문제** 28](#_Toc111133388)

[**5. Hub & Switch** 33](#_Toc111133389)

[**5.1. Hub** 33](#_Toc111133390)

[**5.2. Switch** 33](#_Toc111133391)

[**6. ARP** 34](#_Toc111133392)

[**6.1. ARP** 34](#_Toc111133393)

[**7. VLAN** 34](#_Toc111133394)

[**7.1. VLAN** 34](#_Toc111133395)

[**7.2. VLAN 설정** 35](#_Toc111133396)

[**7.3. Trunk Mode** 38](#_Toc111133397)

[**7.4. Inter VLAN** 41](#_Toc111133398)

[**7.4.1. Inter VLAN이란?** 41](#_Toc111133399)

[**7.4.2. Router를 이용한 방법** 41](#_Toc111133400)

[**7.4.3. L3 Switch를 이용한 방법(Routed Port)** 47](#_Toc111133401)

[**8. STP** 49](#_Toc111133402)

[**8.1. STP** 49](#_Toc111133403)

[**8.2. STP 동작 과정** 52](#_Toc111133404)

[**8.3. STP 확인** 54](#_Toc111133405)

[**8.4. STP 수동 설정** 55](#_Toc111133406)

[**8.5. PVST** 58](#_Toc111133407)

[**9. VTP** 63](#_Toc111133408)

[**9.1. VTP** 63](#_Toc111133409)

[**9.2. VTP 설정** 64](#_Toc111133410)

[**9.3. VTP Pruning** 68](#_Toc111133411)

[**9.4. VTP 실습** 68](#_Toc111133412)

[**10. Cisco 장비 복구** 72](#_Toc111133413)

[**10.1. 장비 동작에 필요한 파일 및 메모리** 72](#_Toc111133414)

[**10.2. 패스워드 초기화** 73](#_Toc111133415)

[**10.3. IOS 및 Config 파일 Backup/Restore** 75](#_Toc111133416)

[**11. RIP** 79](#_Toc111133417)

[**11.1. RIP** 79](#_Toc111133418)

[**11.2. RIPv2 설정** 80](#_Toc111133419)

# **1. Network**

## **1.1. Network 장비**

**1.1.1. Router**

OSI 7 Layer 중 3계층 장비

서로 다른 Network의 통신을 가능하게 한다.

Routing Table에 의하여 Packet을 최적의 경로로 전송한다.

**1.1.2. Switch**

OSI 7 Layer 중 2계층 장비

동일한 Network에서 Node를 확장

Mac Address Table에 의하여 Frame을 최적의 경로로 전송한다.

**1.1.3. Load Balancer**

트래픽을 여러 경로로 분산시킨다. (부하 분산)

**Layer4**

IP와 Port 기반

**Layer7**

상위 계층의 구분에 따라서 로드 밸런싱

예) 기본 웹페이지를 담당하는 웹서버와 특정 서비스에 대한 API 웹서버를 따로 운용하고 트래픽 요청에

따라서 로드 밸런싱

**Fault Tolerant**

결함 감내, 결함을 허용한다는 의미로 장애 시 다른 장비가 그 역할을 즉각적으로 수행하여 장애 대비

**1.1.4. Broadband Router 공유기**

간단한 Routing + NAT + DHCP 기능 갖춘 Home Network

\*NAT (Network Address Translation) : Network 주소 변환 기능

\*DHCP (Dynamic Host Configuration Protocol) : 동적 Host 구성 (대부분 IP 자동 구성 기능)

**1.1.5. 케이블(전송 매체)**

OSI 7 Layer 중 1계층 장비

**동축 케이블(Coxial Cable)**

10Base5의 굵은 케이블과 10Base2의 얇은 케이블이 있다.

10Base2 : 주로 컴퓨터애 사용, 10Mbps의 전송 속도 / 10Base5 : 주로 백본에 사용, 10Mbps의 전송 속도

**UTP(Unshielded Twist Pair)**

가장 많이 사용되는 전송 매체

100m, 100Mbps ~ 1Gbpm의 전송 속도

**광케이블(Fiber Cable)**

전기가 아닌 빛으로 데이터 전송

Single Cable -> 50km

Multi Cable -> 다양한 데이터 전달 가능, 700m

## **1.2. Network 보안**

**1.2.1. Firewall(방화벽)**

3계층과 4계층 기반, 즉 IP와 Port 정보 기반으로 방어

**1.2.2. IDS (Intrusion Detection System)**

침입 탐지 시스템, 소극적, Packet 문자열

**1.2.3. IPS (Intrusion Prevention System)**

침입 장지 시스템, 적극적

**1.2.4. Web Firewall**

동일 Site 내의 특정 페이지 필터링

예) Naver 접속은 가능하지만 Naver의 웹 메일 페이지는 접속 불가, 암호화된 패킷은 하위 계층에서

복호화 후 필터링

**1.2.5. NAC (Network Access Control)**

단말이 네트워크에 접근하기 전 보안정책 준수 여부 검사, 네트워크 사용을 제어

1) 네트워크 사용 사전 동의 후 네트워크 접속 허용

2) 미인증 사용자 네트워크 접속 제한

3) 필수 소프트웨어 미설치 단말에 경고창 팝업 또는 특정 네트워크 접속 제한

## **1.3. Network 전송방식**

**1.3.1. 유니캐스트(Unicast)**

1:1 전송방식, LAN 통신에서 송신자와 수신자의 MAC 주소를 모두 알 때 사용

**1.3.2. 브로드캐스트(Broadcast)**

네트워크에 있는 모든 사용자에게 데이터를 전달하는 방식

**1.3.3. 멀티캐스트(Multicast)**

1:N 전송 방식, 네트워크 상에 있는 사용자 중 지정된 다수의 사용자에게만 데이터를 전달하는 방식

쉽게 생각하면 Unicast + Broadcast 방식

## **1.4. Network 유형**

**1.4.1. LAN(Local Area Network)**

소규모 지역에 위치한 호스트로 구성된 네트워크

브로드캐스트 방식을 사용해 데이터 전송, 빠른 속도

**1.4.2. MAN(Metropolitan Area Network)**

도시 규모에 위치한 호스트로 구성된 네트워크

**1.4.3. WAN(Wide Area Network)**

국가 규모 이상의 넓은 지역에 위치한 호스트로 구성된 네트워크

비용이 많이 든다.

## **1.5. OSI 7계층**

OSI (Open System Interconnections Reference Model)

컴퓨터 네트워크 프로토콜 디자인과 통신을 계층별로 나누어 설명한 것

**1.5.1. 장점**

1) 데이터의 흐름을 알 수 있다. 2) Trouble Shooting - 문제 해결이 쉽다. 3) Standard – 표준화

**1.5.2. 특징**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 계층 | 데이터 단위 | 장비 | 특징 |
| 상위계층 | Layer 7 Application  응용 계층 | Data |  | **App 처리**  1) 데이터 생성을 목적으로 사용자에게 인터페이스와 네트워크 서비스 제공  2) HTTP, FTP, Telnet 등 |
| Layer 6 Presentation  표현 계층 |  | **데이터 표현 방법**  1) 7계층에서 만든 데이터에 컴퓨터가 인식할 수 있도록 데이터 표현 방식 할당  2) JPEG, mp3, 압축 등 |
| Layer 5 Session  세션 계층 |  | **통신 시작과 종료**  1) 응용 프로그램 또는 네트워크 간에 연결을 맺거나 끊기, 연결을 유지하는 기능 |
| 하위계층 | Layer 4 Transport  전송 계층 | Segment | L4 Switch  Gateway | **네트워크 통신 관리**  1) 테이터 전송 방식(TCP, UDP) 결정 및 서비스 포트번호 구별 |
| Layer 3 Network  네트워크 계층 | Packet | Router | **네트워크 통신 경로 선택**  1) IP 주소를 기반으로 출발지에서 목적지까지 가는 데이터 경로 설정  2) 최적 경로 설정 -> Routing Protocol  3) IP, ICMP, IGMP, ARP, RARP |
| Layer 2 DataLink  데이터 링크 계층 | Frame | Switch | **기기간 처리**  1) MAC 주소를 기반으로 노드대 노드로 데이터 전송 형태를 결정  2) Ethernet, HDLC, PPP |
| Layer 1 Physical  물리 계층 | Bit | Cable  Hub | **전기적인 접속** |

## **1.6. TCP/UDP 포트**

0번 ~ 1023번 : 잘 알려진 포트 (well-known port)

1024번 ~ 49151번 : 등록된 포트 (registered port)

49152번 ~ 65535번 : 동적 포트 (dynamic port)

(리눅스 /etc/services 파일)

**주요 Well-known Port**

|  |  |  |
| --- | --- | --- |
| 번호 | TCP/UDP | 설명 |
| 7 | TCP/UDP | ECHO 프로토콜 |
| 20 | TCP | 파일 전송 프로토콜 (FTP, File Transfer Protocol) – 데이터 포트 |
| 21 | TCP | 파일 전송 프로토콜 (FTP, File Transfer Protocol) – 제어 포트 |
| 22 | TCP | 시큐어 셀 (SSH, Secure SHell) – 암호화되지 않은 텍스트 통신 |
| 25 | TCP | SMTP (Simple Mail Transfer Protocol) – 이메일 전송에 사용 |
| 53 | TCP/UDP | 도메인 네임 시스템 (DNS, Domain Name System)  평소에는 UDP 사용  전송하는 데이터가 512byte를 넘어가거나 영역 전송할 때 TCP 사용 |
| 67 | UDP | BOOTP (부비스트랩 프로토콜) 서버  DHCP로도 사용 |
| 68 | UDP | BOOTP (부비스트랩 프로토콜) 클라이언트  DHCP로도 사용 |
| 80 | TCP/UDP | HTTP (HyperText Transfer Protocol) – 웹 페이지 전송 |
| 110 | TCP | POP3 (Post Office Protocol version 3) – 전자우편 가져오기에 사용 |
| 143 | TCP | 인터넷 메시지 접속 프로토콜 4 (IMAP4, Internet Message Access Protocol 4) |
| 443 | TCP | HTTPS – 보안 소켓 레이어 (SSL, Secure Socket Layer) 위의 HTTP (암호화 전송) |
| 445 | TCP | Microsoft-DS (액티브 디렉터리, 윈도우 공유, Sasser-worm, Agobot, Zobotworm) |
| UDP | Microsoft-DS SMB 파일 공유 |
| 465 | TCP | SSL 위의 SMTP - Cisco 프로토콜과 충동 |
| 990 | TCP | SSL 위의 FTP (암호화 전송) |
| 993 | TCP | SSL 위의 IMAP4 (암호화 전송) |
| 995 | TCP | SSL 위의 POP3 (암호화 전송) |

## **1.7. Network 주소**

네트워크상에서 고유한 식별번호, IP 주소와 MAC 주소가 있다.

**1.7.1. MAC Address (Media Access Controller Address)**

텍스트이(가) 표시된 사진

자동 생성된 설명

물리적 주소, OSI 2계층(데이터 링크 계층)에서 사용된다.

16진수 12자리로 표현되어 있다. (한자리에 4bit씩 총 48bit)

앞쪽 6자리는 제조회사 고유번호 (OUI), 뒤쪽 6자리는 제조회사에서 부여한 일련번호

주소 부족 문제를 해결하기 위해 UUID 도입

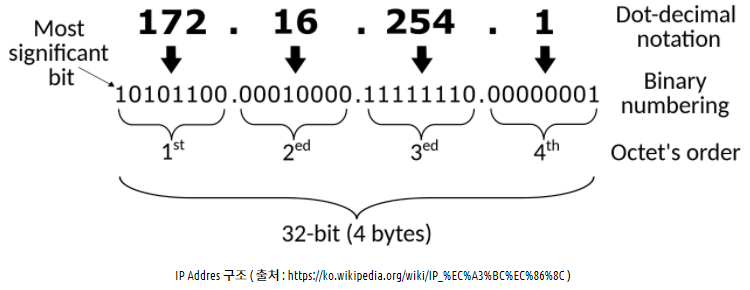
Windows는 cmd 창에 ipconfig /all 명령어를 입력해서 확인 가능

**1.7.2. IP Address (Internet Protocol Address)**

논리적 주소, OSI 3계층(네트워크 계층)에서 사용된다.

version 4와 version 6가 있다.

**IP Address version 4**



1) 2진수 32개, 총 32bit

2) 2진수 8개를 묶어서 하나의 Octet으로 구별한다.

3) 4개의 Octet으로 구성된다. 각 Octet 별로 10진수로 변환해서 표현한다.

**1.7.3. Class**

초창기에는 Class별로 IP를 사용하였다. (현재는 IP 주소 부족으로 Subnet Mask 도입)

테이블이(가) 표시된 사진

자동 생성된 설명

**1.7.4. 사이더 (CIDR, Classless Inter Domain Routing)**

Class별 IP 사용으로 인한 IP의 낭비를 줄이고자 도입되었다.

Class별 크기가 아니라 Subnet Mask에 의해서 Network 크기를 제한한다.

테이블이(가) 표시된 사진

자동 생성된 설명

# **2. Subnet**

## **2.1. Subnet(서브넷)**

하나의 네트워크가 분할되어 나눠진 작은 네트워크

네트워크를 분할하는 것을 서브네팅이라고 하고 서브네팅은 서브넷 마스크를 통하여 수행된다.

네트워크를 규모에 맞게 분할하여 낭비되는 IP주소를 최소화하려는 것이 주된 목적

## **2.2. Subnet Mask**

**2.2.1. 특징**

IP Address와 동일한 규칙을 가진다.

2진수 0이 나오면 끝까지 0이어야 한다.

테이블이(가) 표시된 사진

자동 생성된 설명

**2.2.2. Prefix**

Subnet Mask의 표현법으로 이진수 ‘1’의 개수를 십진수로 표현

ex) 255.255.255.0 -> 11111111.11111111.11111111.00000000 -> /24

255.255.224.0 -> 11111111.11111111.11100000.00000000 -> /19

255.255.0.0 -> 11111111.11111111.00000000.00000000 -> /16

## **2.3. Subnet 문제**

**2.3.1. 100.100.0.0/24**

다음 IP 주소를 나누고 서브넷 마스크와 가용IP를 구하시오.

서브넷 마스크 : 255.255.255.0

100.100.0.0~100.100.0.255 (100.100.0.0 - 네트워크 ID / 10.0.0.255 - 브로드캐스트 주소)

가용IP : 10.0.0.1~10.0.0.254

**2.3.2. 100.100.0.0/26**

다음 IP 주소를 나누고 서브넷 마스크와 가용IP를 구하시오.

서브넷 마스크 : 255.255.255.192

100.100.0.0~100.100.0.63 / 가용IP : 100.100.0.1~100.100.0.62

100.100.0.64~100.100.0.127 / 가용IP : 100.1000.0.65~100.100.0.126

100.100.0.128~100.100.0.191 / 가용IP : 100.100.0.129~100.100.0.190

100.100.0.192~100.100.0.255 / 가용IP : 100.100.0.193~100.100.0.254

**2.3.3. 100.100.0.0/19**

다음 IP 주소를 나누고 서브넷 마스크와 가용IP를 구하시오.

서브넷 마스크 : 255.255.224.0

100.100.0.0~100.100.31.255 / 가용IP : 100.100.0.1~100.100.31.254

100.100.32.0~100.100.63.255 / 가용IP : 100.100.32.1~100.100.63.254

100.100.64.0~100.100.95.255 / 가용IP : 100.100.64.1~100.100.95.254

100.100.96.0~100.100.127.255 / 가용IP : 100.100.96.1~100.100.127.254

100.100.128.0~100.100.159.255 / 가용IP : 100.100.128.1~100.100.159.254

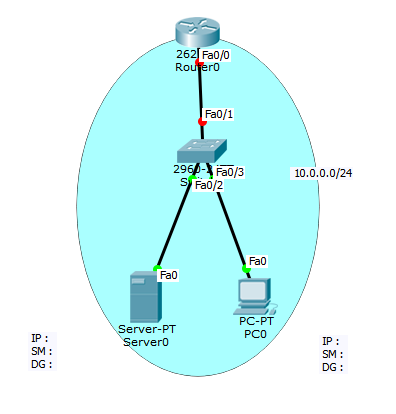
100.100.160.0~100.100.191.255 / 가용IP : 100.100.160.1~100.100.191.254

100.100.192.0~100.100.223.255 / 가용IP : 100.100.192.1~100.100.223.254

100.100.224.0~100.100.255.255 / 가용IP : 100.100.224.1~100.100.255.254

**2.3.4. 10.0.0.0/24 Packet Tracer를 이용**

다음 이미지와 조건대로 서브네팅 후 Server와 PC 통신 확인하기



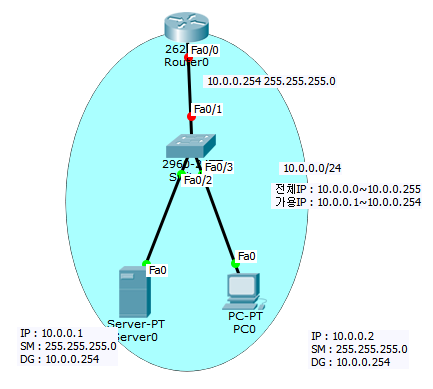
1) 서버는 네트워크의 첫 번째 IP를 할당

2) PC는 네트워크의 두 번째 IP를 할당

3) Default Gateway는 마지막 IP로 설정

**풀이**

다음 이미지와 같이 설정



Server에 IP 할당

텍스트이(가) 표시된 사진

자동 생성된 설명

PC에 IP 할당

텍스트이(가) 표시된 사진

자동 생성된 설명

프롬프트에서 ping 명령어를 사용하여 통신 상태 확인

텍스트이(가) 표시된 사진

자동 생성된 설명

# **3. Router 설정**

## **3.1. Routing Protocol**

목적지 네트워크로 가는 경로를 알아내기 위해 사용하는 프로토콜

라우터는 라우팅 프로토콜에 따라 라우터 테이블을 보고 packet을 전송한다.

## **3.2. Router 설정 방법 (Packet Tracer)**

Router를 클릭 후 CLI에 들어가서 설정 (실제로는 다른 기기에 콘솔 연결해서 설정)

**3.2.1. 명령어**

텍스트이(가) 표시된 사진

자동 생성된 설명

Continue with configuration dialog? [yes/no] -> 초기 설정을 대화 형식으로 진행할 것인지 묻는 것



사용자 모드 (ping test, trace 같은 간단한 확인 정도만 가능)



1) enable // 사용자 모드에서 관리자 모드로 진입하는 명령어

2) 관리자 모드 프롬프트



write // 설정 사항을 모두 저장하는 명령어



재부팅 명령어 (저장하지 않고 재부팅을 하면 변경사항이 적용되지 않는다.)

텍스트이(가) 표시된 사진

자동 생성된 설명

show running-config // 라우터의 설정 내용 확인 (Enter 로 내려가고 Ctrl + c 로 빠져나옴)



1) configure terminal // 글로벌 모드로 진입하는 명령어

2) 글로벌 모드 프롬프트



1) 유저 모드에서 관리자 모드로 진입 시 암호 설정 (평문, 보안성이 취약)

2) 유저 모드에서 관리자 모드로 진입 시 암호 설정 (암호화, 보안성이 우수)

평문 암호와 secret 암호가 중복되면 secret 암호가 우선순위를 갖는다.

3) 모든 평문 암호를 암호화하는 명령어



명령어 삭제 -> 기존 명령어 앞에 no를 붙인다.



명령어 잘못 입력 시 dns 서버를 찾는 과정 생략



do write // 관리자 모드가 아닌 곳에서 설정을 저장하는 명령어

텍스트, 테이블이(가) 표시된 사진

자동 생성된 설명

1) line console 0 // 콘솔 설정 모드로 진입하는 명령어

2) 콘솔 설정 모드 (어떤 line인지 정확하게 구분되지는 않음)

3) 콘솔 접속 시 패스워드 설정

4) login // 콘솔로 접속 시 패스워드를 물어보도록 설정 (패스워드 설정이 되어있어야 함)

5) exec-timeout 0 0 // 자동 로그아웃 방지 (앞의 숫자는 분, 뒤의 숫자는 초 / 기본 15분 00초)

6) logging synchronous // 타이핑 중 인터페이스가 활성화되어 명령어가 밀리는 것을 방지



exit // 이전 모드로 돌아가는 명령어





1) 인터페이스 접근 (fastEthernet의 0번 슬롯의 0번 포트)

2) 패스트 이더넷 인터페이스 프롬프트 (다른 인터페이스와 구분되지 않음)

3) 인터페이스 접근 (serial의 0번 슬롯의 0번 포트)

텍스트이(가) 표시된 사진

자동 생성된 설명

1) ip address IP주소 서브넷마스크 // IP와 서브넷 마스크 추가

2) no shutdown // port 활성화

shutdown // port 비활성화

텍스트이(가) 표시된 사진

자동 생성된 설명

copy running-config startup-config // 설정 내용을 저장 (파일 이름 지정)

텍스트이(가) 표시된 사진

자동 생성된 설명

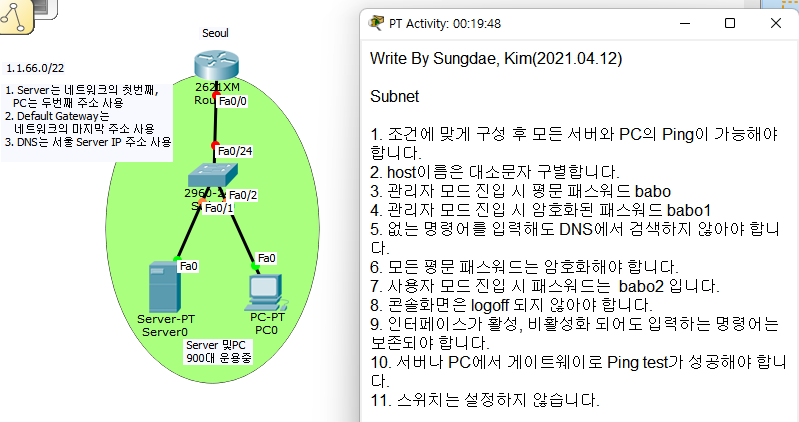
라우팅 명령어

\*\*\* Ctrl + z : 한번에 관리자 모드로 진입

## **3.3. Subnet 문제**

**3.3.1. 라우터 1개**

**문제**



**풀이**

서브넷 마스크가 255.255.252.0이므로 네트워크 개수는 64개이다.

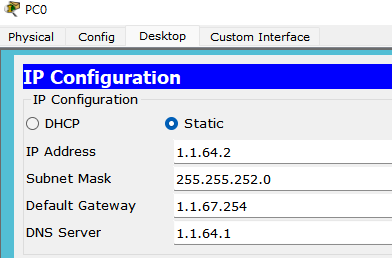
1.1.0.0~1.1.3.255

1.1.4.0~1.1.7.255

(생략)

1.1.64.0~1.1.67.255 -> 할당된 IP주소 / 가용IP : 1.1.64.1~1.1.67.254

텍스트이(가) 표시된 사진

자동 생성된 설명 

가용IP 내에서 조건에 맞게 Server와 PC에 IP 설정

텍스트이(가) 표시된 사진

자동 생성된 설명



조건에 맞게 기본 라우터 설정

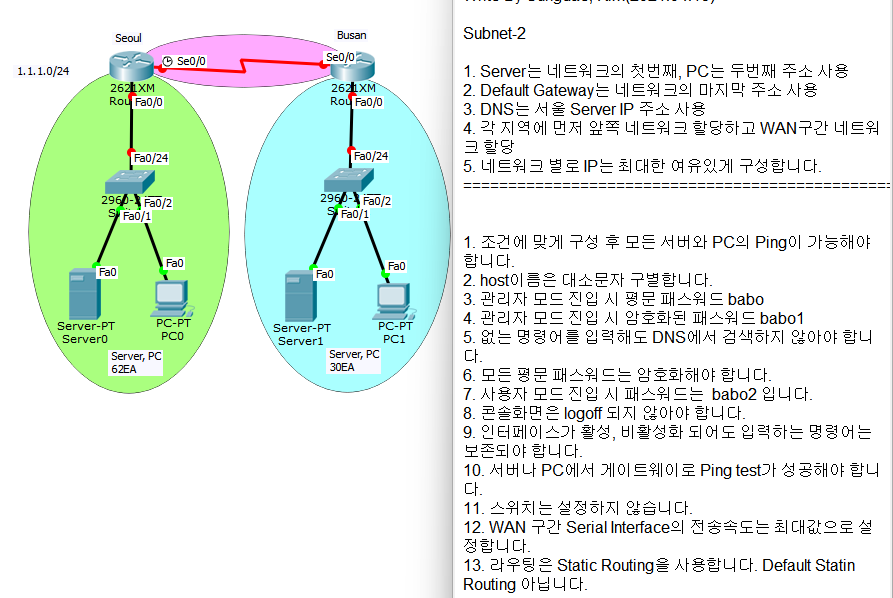
텍스트이(가) 표시된 사진

자동 생성된 설명

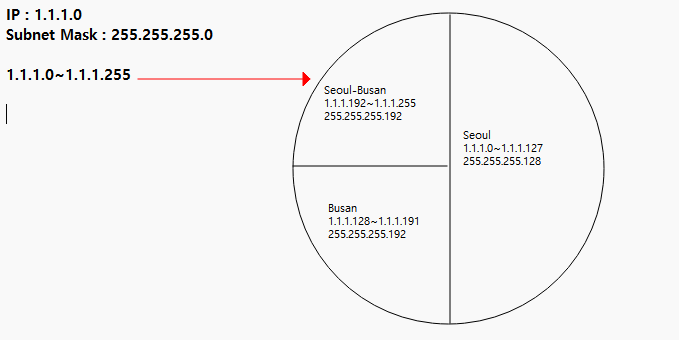
fasterEthernet 0/0 설정 및 활성화 후 저장

**3.3.2. 라우터 2개**

**문제**



**풀이**



네트워크가 3개 필요하다. (Seoul, Busan, Seoul과 Busan을 연결하는 네트워크)

Seoul은 62개의 서버와 PC를 운용하고 있고 Network ID, Broadcast 주소, Default Gateway를 포함하여 65개의 IP가 필요하여 128개의 IP를 할당한다. (1.1.1.0~1.1.1.127 255.255.255.128)

Busan은 30개의 62개의 서버와 PC를 운용하고 있고 Network ID, Broadcast 주소, Default Gateway를 포함하여 33개의 IP가 필요하여 64개의 IP를 할당한다. (1.1.1.128~1.1.1.191 255.255.255.192)

Seoul과 Busan을 연결하는 네트워크는 남은 IP를 할당한다. (1.1.1.192~1.1.1.255 255.255.255.192)

텍스트이(가) 표시된 사진

자동 생성된 설명 텍스트이(가) 표시된 사진

자동 생성된 설명

Seoul\_R1 가용IP 내에서 조건에 맞게 Server와 PC에 IP 설정

텍스트이(가) 표시된 사진

자동 생성된 설명 텍스트이(가) 표시된 사진

자동 생성된 설명

Busan\_R1 가용IP 내에서 조건에 맞게 Server와 PC에 IP 설정

텍스트이(가) 표시된 사진

자동 생성된 설명

Seoul\_R1 기본 라우터 설정

텍스트이(가) 표시된 사진

자동 생성된 설명

Seoul\_R1 fastEthernet 0/0 설정 및 활성화

텍스트이(가) 표시된 사진

자동 생성된 설명

Seoul\_R1 serial 0/0 설정 및 활성화



Seoul\_R1 라우팅 설정 후 저장

텍스트이(가) 표시된 사진

자동 생성된 설명

Busan\_R1 기본 라우터 설정

텍스트이(가) 표시된 사진

자동 생성된 설명

Busan\_R1 fastEthernet 0/0 설정 및 활성화

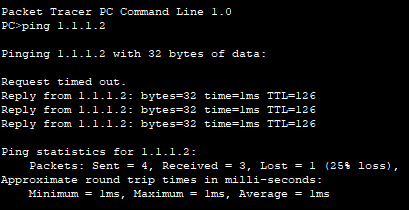
텍스트이(가) 표시된 사진

자동 생성된 설명

Busan\_R1 serial 0/0 설정 및 활성화



Busan\_R1 라우팅 설정 후 저장



Busan PC에서 Seoul Server로 ping 테스트

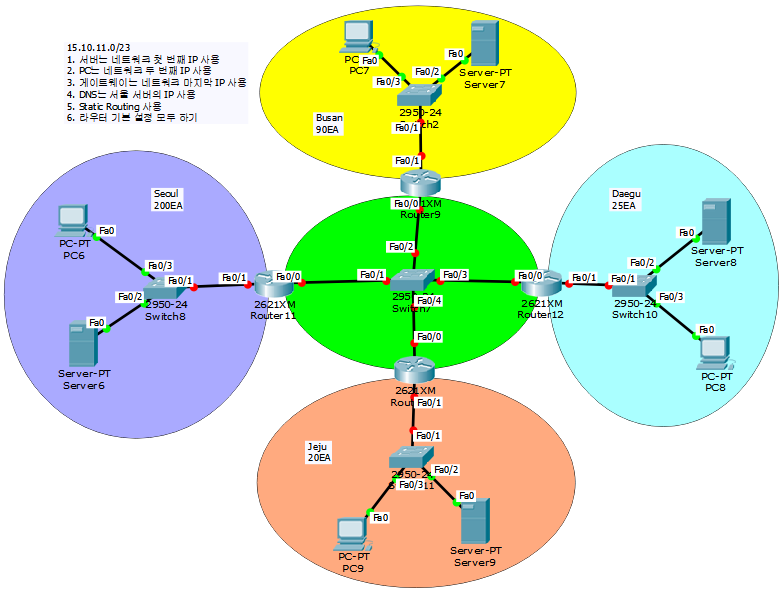
텍스트, 실내이(가) 표시된 사진

자동 생성된 설명

Seoul PC에서 Busan PC로 ping 테스트

# **4. 네트워크 연습문제**

**4.1. 설계**



**4.2. 서브네팅**

**Seoul (200EA)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| IP 범위 | | | 서브넷 마스크 | |
| 15.10.10.1 ~ 15.10.10.255 | | | 255.255.255.0 | |
| Device | IP Address | Subnet Mask | Gateway | DNS |
| Server | 15.10.10.1 | 255.255.255.0 | 15.10.10.254 | 15.10.10.1 |
| PC | 15.10.10.2 |

텍스트이(가) 표시된 사진

자동 생성된 설명텍스트이(가) 표시된 사진

자동 생성된 설명

**Busan (90EA)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| IP 범위 | | | 서브넷 마스크 | |
| 15.10.11.0 ~ 15.10.11.127 | | | 255.255.255.128 | |
| Device | IP Address | Subnet Mask | Gateway | DNS |
| Server | 15.10.11.1 | 255.255.255.128 | 15.10.11.126 | 15.10.10.1 |
| PC | 15.10.11.2 |

텍스트이(가) 표시된 사진

자동 생성된 설명텍스트이(가) 표시된 사진

자동 생성된 설명

**Daegu (25EA)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| IP 범위 | | | 서브넷 마스크 | |
| 15.10.11.128 ~ 15.10.11.159 | | | 255.255.255.224 | |
| Device | IP Address | Subnet Mask | Gateway | DNS |
| Server | 15.10.11.129 | 255.255.255.224 | 15.10.11.126 | 15.10.10.1 |
| PC | 15.10.11.130 |

텍스트이(가) 표시된 사진

자동 생성된 설명텍스트이(가) 표시된 사진

자동 생성된 설명

**Jeju (20EA)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| IP 범위 | | | 서브넷 마스크 | |
| 15.10.11.160 ~ 15.10.11.191 | | | 255.255.255.224 | |
| Device | IP Address | Subnet Mask | Gateway | DNS |
| Server | 15.10.11.161 | 255.255.255.224 | 15.10.11.190 | 15.10.10.1 |
| PC | 15.10.11.162 |

텍스트이(가) 표시된 사진

자동 생성된 설명텍스트이(가) 표시된 사진

자동 생성된 설명

**라우팅**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IP 범위 | | | 서브넷 마스크 | | |
| 15.10.11.192 ~ 15.10.11.199 | | | 255.255.255.248 | | |
| Device | IP Address | Subnet Mask | Device | IP Address | Subnet Mask |
| Router\_Seoul | 15.10.11.193 | 255.255.255.248 | Router\_Busan | 15.10.11.194 | 255.255.255.248 |
| Router\_Daegu | 15.10.11.195 | Router\_Jeju | 15.10.11.196 |

**4.3. 라우팅 설정**

텍스트이(가) 표시된 사진

자동 생성된 설명텍스트이(가) 표시된 사진

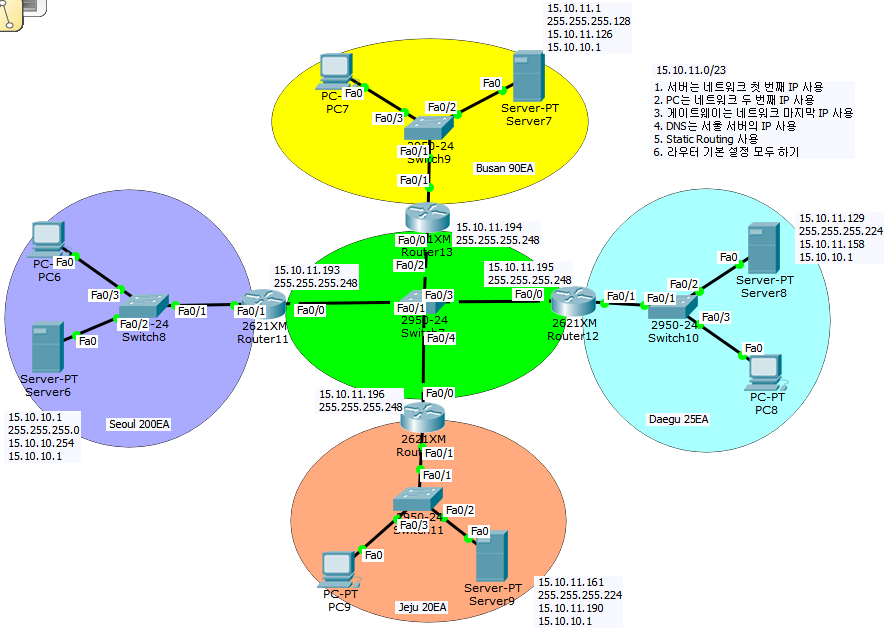
자동 생성된 설명

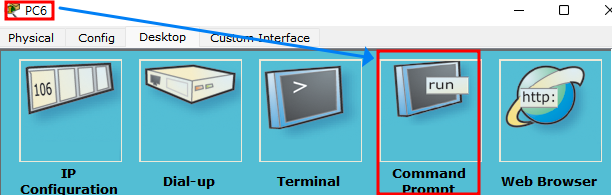
텍스트이(가) 표시된 사진

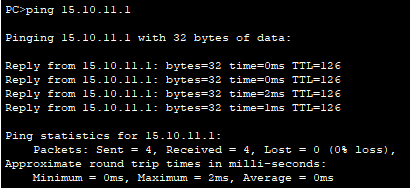
자동 생성된 설명텍스트이(가) 표시된 사진

자동 생성된 설명

**4.4. 테스트**







텍스트, 실내이(가) 표시된 사진

자동 생성된 설명

텍스트이(가) 표시된 사진

자동 생성된 설명

# **5. Hub & Switch**

## **5.1. Hub**

이더넷 허브(Ethernet Hub)는 이더넷 네트워크에서 여러 대의 컴퓨터, 네트워크 장비를 물리적 포트를 통해 연결하는 장치이다. 같은 허브에 연결된 컴퓨터와 네트워크 장비는 모두 상호 간에 통신할 수 있게 된다. 연결된 기기에서 전송된 패킷을 받아 다시 다른 기기로 내보내다.

패킷의 출발지와 목적에 대한 정보를 갖지 않아 모든 신호를 Broadcast한다. 그러다 보니 연결된 장치가 많아질수록 많은 충돌이 발생하고 속도가 느려지는 단점이 있다.

## **5.2. Switch**

스위치는 허브의 단점을 보안하는 네트워크 장비이다. 여러 대의 네트워크 장치를 하나의 네트워크로 연결해 주는 것은 동일하지만 스위치는 자신의 포트에 연결된 MAC Address를 통해 패킷의 출발지와 목적지 정보에 대해 파악할 수 있어 신호를 모든 컴퓨터에 뿌리지 않고도 목적지 포트에만 전송할 수 있다.

# **6. ARP**

## **6.1. ARP**

ARP(Address Resolution Protocol)은 네트워크 상에서 IP 주소를 물리적 네트워크 주소로 대응시키기 위해 사용되는 프로토콜 -> IP 주소를 MAC 주소와 매칭

텍스트이(가) 표시된 사진

자동 생성된 설명

Mac Address 확인

텍스트, 화면, 스크린샷이(가) 표시된 사진

자동 생성된 설명

처음 ARP을 조회하면 아무런 경로가 나오지 않지만 ping 테스트로 특정 IP로부터 Request를 받고 ARP를 조회하면 Request 받은 주소가 나온다. (일정 시간 유지되다 사라진다.)

# **7. VLAN**

## **7.1. VLAN**

**7.1.1. LAN이란?**

LAN(Local Area Network)란 집이나 사무실, 회사 같은 중소규모의 네트워크. 동일한 IP 대역과 동일한 Subnet Mask를 사용하며 ARP가 닿는 모든 범위를 말한다.

**7.1.2. VLAN이란?**

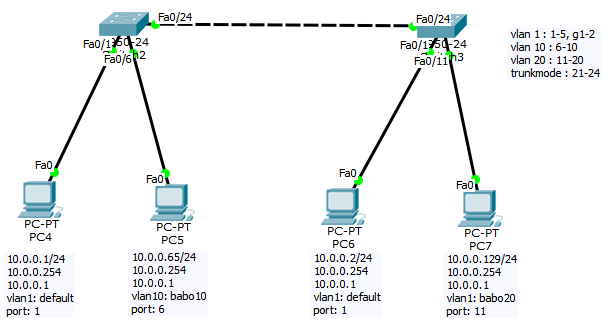
네트워크에서 여러 개의 구별되는 브로드캐스트 도메인을 만들기 위해 단일 2계층 네트워크를 분할할 수 있는데, 이렇게 분리되면 패킷들은 하나 이상의 라우터들 사이에서만 이동할 수 있다. 이러한 도메인을 VLAN(Virtual LAN)이라고 한다.

**7.1.2. 사용 이유**

1) 보안성 향상 2) Broadcast Domain 분리 (CD, BD)

## **7.2. VLAN 설정**

**7.2.1. 구조**



**7.2.2. 서브네팅**

텍스트이(가) 표시된 사진

자동 생성된 설명 텍스트이(가) 표시된 사진

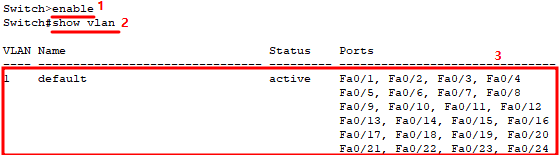
자동 생성된 설명 텍스트이(가) 표시된 사진

자동 생성된 설명 텍스트이(가) 표시된 사진

자동 생성된 설명

PC -> IP Configuration (동일 IP 대역, 동일 Subnet Mask)

**7.2.3. VLAN 정보 확인**



관리자 모드에서 VLAN 정보를 확인할 수 있다.

1) 관리자 모드로 전환 2) VLAN 정보 확인 3) 모든 포트가 VLAN 1(Default)로 지정되어 있다.

**7.2.4. VLAN 생성**

**Switch2 (왼쪽 스위치)**

텍스트이(가) 표시된 사진

자동 생성된 설명

전역 설정 모드에서 VLAN을 생성할 수 있다.

1) 전역 설정 모드로 전환 2) VLAN 10 생성 3) VLAN 이름 설정

테이블이(가) 표시된 사진

자동 생성된 설명

다시 VLAN 정보를 보면 VLAN이 생성되고 이름이 변경된 것을 확인 가능

**Switch3 (오른쪽 스위치)**

테이블이(가) 표시된 사진

자동 생성된 설명

동일하게 VLAN 생성

**7.2.5. VLAN 포트 추가**

.텍스트이(가) 표시된 사진

자동 생성된 설명

Switch2에 Ethernet 6-10번 포트를 VLAN 10에 추가하고 확인 (range 옵션으로 한 번에 설정 가능)

텍스트, 테이블이(가) 표시된 사진

자동 생성된 설명

Switch3에 Ethernet 11-20번 포트를 VLAN 20에 추가하고 확인

**7.2.6. 테스트**

텍스트이(가) 표시된 사진

자동 생성된 설명

같은 VLAN(VLAN 1)으로 묶여 있는 PC끼리만 통신이 된다.

## **7.3. Trunk Mode**

**7.3.1. Trunk Mode란?**

하나의 포트에 다수의 VLAN이 지나갈 수 있도록 기능하는 것을 Trunk Mode라고 한다. (하나의 VLAN만 할당하는 것은 Access Mode) -> 포트를 절약할 수 있다.

**7.3.2. VLAN 식별 방법**

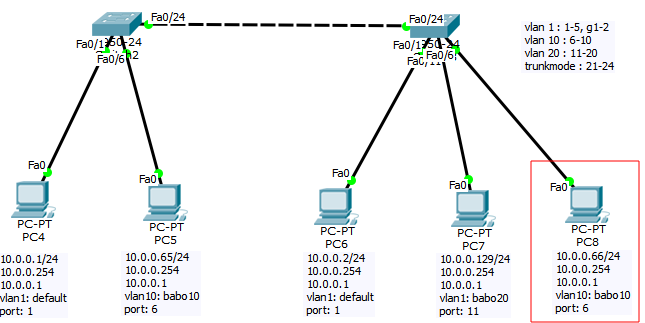
**ISL (Inter-Switch Link)**

Cisco 전용 프로토콜. 프레임 전체에 식별코드 부여 (암호화) -> 보안성 우수, 전송속도가 느려짐

**IEEE 802.1Q**

IEEE 표준. 트렁크에서 전송 및 수신된 다른 모든 프레임에 태그(이름표)를 지정

**7.3.3. Trunk Mode 설정**

 텍스트이(가) 표시된 사진

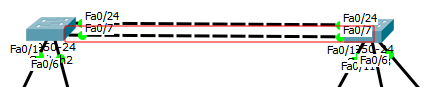
자동 생성된 설명

‘3.2. VLAN 설정’의 구성도에 VLAN 10을 사용할 PC를 추가해 준다.

테이블이(가) 표시된 사진

자동 생성된 설명

Switch3에 VLAN 10 생성 및 포트 추가

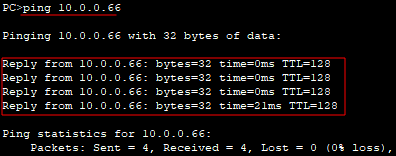


24 Port는 VLAN 1에 묶여 있기 때문에 VLAN 10에 묶여 있는 Port를 추가해 주어야 VLAN 10끼리 통신이 가능해진다. 하지만 이렇게 구성하게 되면 포트 낭비가 발생한다. 이때 Trunk Port를 추가해 주면 하나의 포트로 다수의 VLAN이 지나갈 수 있게 된다.

텍스트이(가) 표시된 사진

자동 생성된 설명

Switch2에 트렁크 설정해준다. (24 Port) -> Switch2에 설정하면 Swtich3도 저절로 설정된다.



VLAN 10으로 묶인 PC끼리 통신이 되는 것을 확인

**7.3.4. L3 Switch Trunk 설정**

텍스트이(가) 표시된 사진

자동 생성된 설명

L2 스위치와 동일하게 trunk 설정을 해주면 오류가 발생한다.

텍스트이(가) 표시된 사진

자동 생성된 설명

L3 스위치는 수동으로 Encapsulation을 지정해 주어야 Trunk Mode를 사용할 수 있다. (dot1q 방식)

**7.3.5. 특정 VLAN만 허용 설정**

Interface 프롬프트에서 ‘switchport trunk allowed vlan 1, 2, 3’ 명령어를 입력하면 Trunk Port를 VLAN 1, 2, 3만 지나갈 수 있게 된다.

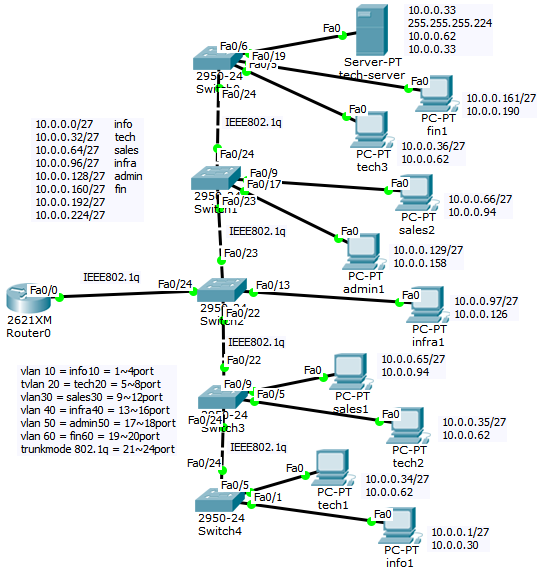
## **7.4. Inter VLAN**

### **7.4.1. Inter VLAN이란?**

서로 다른 VLAN의 통신이 가능하게 하는 기능으로 3계층 이상의 장비인 라우터나 L3 스위치를 통해야 한다.

### **7.4.2. Router를 이용한 방법**

**구성**



**Switch4 설정**

텍스트이(가) 표시된 사진

자동 생성된 설명 텍스트이(가) 표시된 사진

자동 생성된 설명

VLAN 추가 및 이름 변경 포트 추가

테이블이(가) 표시된 사진

자동 생성된 설명

확인

텍스트이(가) 표시된 사진

자동 생성된 설명

Trunk 설정

**Switch3 설정**

텍스트, 화면이(가) 표시된 사진

자동 생성된 설명 텍스트이(가) 표시된 사진

자동 생성된 설명

VLAN 추가 및 이름 변경 포트 추가

테이블이(가) 표시된 사진

자동 생성된 설명

확인

Trunk 설정은 Switch4의 설정으로 자동으로 설정되었다.

**Switch2 설정**

텍스트이(가) 표시된 사진

자동 생성된 설명 

테이블이(가) 표시된 사진

자동 생성된 설명

VLAN 설정 및 확인

텍스트이(가) 표시된 사진

자동 생성된 설명

Trunk 설정

**Switch1 설정**

텍스트, 실내이(가) 표시된 사진

자동 생성된 설명 텍스트이(가) 표시된 사진

자동 생성된 설명

테이블이(가) 표시된 사진

자동 생성된 설명

VLAN 설정 및 확인

**Switch0 설정**

텍스트이(가) 표시된 사진

자동 생성된 설명 텍스트이(가) 표시된 사진

자동 생성된 설명

테이블이(가) 표시된 사진

자동 생성된 설명

VLAN 설정 및 확인

텍스트이(가) 표시된 사진

자동 생성된 설명

Trunk 설정

**Router 설정**

Router를 가운데 Switch에 연결하는 것이 가장 좋다. (트래픽을 줄여준다.)

텍스트이(가) 표시된 사진

자동 생성된 설명

인터페이스 fastEthernet 0/0을 작동시킨다.

텍스트이(가) 표시된 사진

자동 생성된 설명

서브 인터페이스를 만들고 IP 할당

1) 서브 인터페이스를 만든다. (fastEthernet 0/0.10) 2) 서브 인터페이스 프롬프트

3) Encapsulation 지정 (dot1q, VLAN 10) 4) IP 할당 (info의 게이트웨이, 서브넷 마스크)

텍스트이(가) 표시된 사진

자동 생성된 설명

텍스트이(가) 표시된 사진

자동 생성된 설명

텍스트이(가) 표시된 사진

자동 생성된 설명

텍스트이(가) 표시된 사진

자동 생성된 설명

텍스트이(가) 표시된 사진

자동 생성된 설명

서브 인터페이스(fa0/0.20~fa0/0.60)를 만들고 IP 할당

**테스트**

텍스트이(가) 표시된 사진

자동 생성된 설명

텍스트이(가) 표시된 사진

자동 생성된 설명

텍스트이(가) 표시된 사진

자동 생성된 설명

텍스트이(가) 표시된 사진

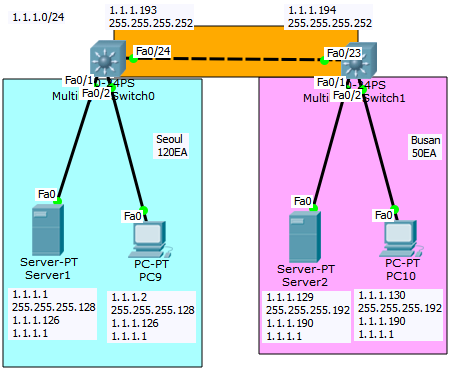
자동 생성된 설명

**모든 PC가 통신이 되는 것을 확인**

### **7.4.3. L3 Switch를 이용한 방법(Routed Port)**

L3 Switch의 각 포트 혹은 VLAN에 IP를 할당한다.

**구성**



**Switch0**

텍스트이(가) 표시된 사진

자동 생성된 설명

Default VLAN(VLAN 1)에 Gateway 주소를 추가해준다.

텍스트이(가) 표시된 사진

자동 생성된 설명

24 Port를 Routed Port로 사용하기 위해서 Switch Port를 사용하지 않도록 설정하고 IP를 입력한다.

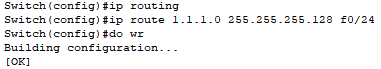


라우팅을 하도록 설정하고 Routing Table을 추가해 준다.

**Switch1**

텍스트이(가) 표시된 사진

자동 생성된 설명



Switch0과 동일하게 설정

**테스트**

텍스트, 실내이(가) 표시된 사진

자동 생성된 설명

통신 확인

# **8. STP**

## **8.1. STP**

**8.1.1. STP란?**

STP(Spanning Tree Protocol): 이중화 구조에서 Bridging Loop를 방지하기 위해 IEEE에서 정의한 프로토콜

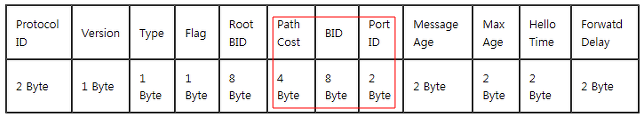
스위치 간에 BPDU Frame을 멀티캐스트로 교환하여 스위치 간에 물리적인 연결 상태와 내부 토폴로지 변경 사항 및 루프의 위치를 결정하여 최종적으로 포트를 차단

**8.1.2. BPDU**

BPDU(Bridge Protocol Data Unit): 스위치 간에 송수신 되는 STP의 정보 데이터이다. 설정 BPDU(Configuration BPDU)와 TNC BPDU(Topology Change Notification BPDU)가 있다.

**Configuration BPDU**

스위치는 Configuration BPDU를 2초마다 주기적으로 교환한다. 스위치는 수신한 설정 BPDU의 필드 값(Bridge ID, Path Cost, Port ID)을 기준으로 스위치의 역할과 포트의 역할을 결정한다.



**Bridge ID**

브리지나 Switch가 통신할 때 서로를 확인인하기 위해 가지고 있는 64bit 체계의 식별자

Bridge ID가 가장 낮은 Switch가 Root Bridge로 선출된다.

테이블이(가) 표시된 사진

자동 생성된 설명

Priority 16bit (Default 372768, VLAN 환경에서는 + ‘VLAN ID’) + MAC Address 48bit

**Path Cost**

특정 Switch 포트에서 Root Bridge까지 Link의 속도를 특정 값으로 변환시킨 것. BPDU에서는 경로의 합

테이블이(가) 표시된 사진

자동 생성된 설명

**Port ID**

Switch 포트마다 부여된 고유한 ID. 기본적으로 ‘128.포트번호’의 모양으로 사용되며 번호가 낮을수록 우선순위가 높다. (f0/1 -> 128.1, f0/24 -> 128.24)

**8.1.3. 관련 용어**

**이중화 구조**

이중화 구조는 서버를 구성할 때 서비스 장애가 발생되어도 다른 서버를 통해 서비스가 다운되지 않고 지속 가능하도록 해준다. 서비스를 보다 안정적으로 지원해준다.

**Bridging Loop**

Switch는 브로드캐스트를 수신하면 모든 트렁크 포트로 플러딩하기 때문에 지중화 링크를 구현한 환경에서는 브리징 루프가 발생한다. 크게 3개지 원인이 있다.

1) 브로드캐스트 스톰(Broadcast Storm)

Host가 전송하는 브로드캐스트 트레픽을 switch가 이중화 링크를 통하여 지속적으로 플러딩하여 네트워크 기능을 악화시키는 현상

2) MAC 주소 테이블 불안정(MAC Flapping)

Switch는 수신한 Frame의 출발지 MAC 주소가 자신의 MAC Address Table에 학습되지 않았다면 출발지 MAC 주소와 프레임을 수신한 포트 번호를 MAC Address Table에 등록. 만일 특정 포트로 MAC 주소가 학습되어 에이징 타이머가 동작 중일 때 출발지 주소가 동일한 MAC 주소를 다른 포트로 학습이 된다면 MAC 주소가 충돌하는 MAC Flapping 현상 발생

3) 유니캐스트 프레임 복제(Copy Unicast Frame)

Switch는 Unicast Frame을 수신하면 자신의 MAC Address Table을 참조하여 목적지 해당 포트로 Frame을 전송. 그러나 Unknown Unicast Frame을 수신하면 모든 Switch 포트로 프레임을 플러딩해야 함으로 스위치 개수만큼 Unicast Frame을 복제. 허나 Unicast가 여러 개로 복제된다는 것은 Unicast 전송 방식에 맞지 않으며 Host 입장에서도 동일한 Unicast Frame을 수신하게 되어 Ethernet Frame Loop 발생

**플러딩**

정적 알고리즘으로, 어떤 노드에서 온 하나의 패킷을 라우터에 접속되어 있는 다른 모든 노드로 전달하는 것이다. 대규모 네트워크에서 수정된 라우팅 정보를 모든 노드에 빠르게 배포하는 수단이다.

## **8.2. STP 동작 과정**

**8.2.1. STP 선정 과정**

1) Bridge ID가 가장 낮은 Bridge를 Root Bridge로 선출

2) Root Bridge가 아닌 각 Bridge에서 Root Port(BPDU 송신 포트) 선출

- 각 Bridge에서의 최소 비용 경로(Path Cost가 가장 낮은) 포트

- 연결된 상대방의 Bridge ID가 가장 낮은 포트

- 연결된 상대방의 Port ID가 가장 낮은 포트

3) 각 세그먼트마다 하나의 Designate Port(지명 포트, BDPU 수신 포트) 선출

- Root Bridge의 모든 포트

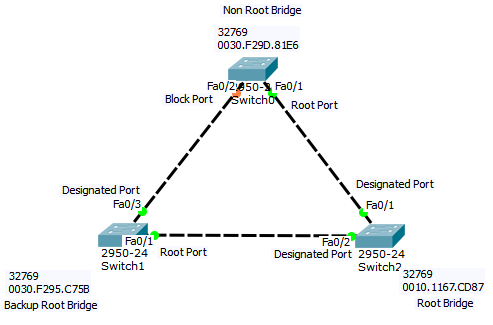
- 각 세그먼트에서의 최소 비용 경로(Path Cost가 가장 낮은) Switch의 포트

- 자신의 Bridge ID가 가장 낮은 Switch의 포트

- 자신의 Port ID가 가장 낮은 Switch의 포트

4. 역할이 없는 나머지 포트 Blocking (Alternated Port 혹은 Block Port)

**8.2.2. 3개의 스위치 연결**



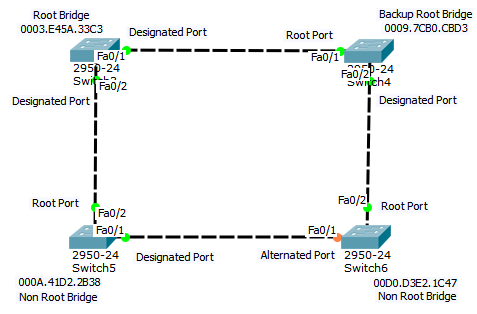
1) Bridge ID가 가장 낮은 Swtich2가 Root Bridge, 다음으로 낮은 Swtich1이 Backup Root Bridge, 남은 Switch0은 Non Root Bridge로 선정된다.

2) Switch1과 Swtich3에서 Root Bridge(Switch2)로 가는 최단 경로(Path Cost 값이 가장 낮은) 포트가 Root Port로 선정된다. -> Switch0은 Fa0/1, Switch1은 Fa0/1

3) Root Bridge에 연결된 포트와 나머지 세그먼트에서 Path Cost가 낮은 Switch에 연결된 포트가 지정 포트로 선정된다. -> Switch0과 Switch1을 연결한 세그먼트에서 Switch1의 Fa0/3

4) 남은 Switch0의 Fa0/2가 Alternated Port(Block Port)가 된다. (Blocking)

**8.2.3. 4개의 스위치 연결**



1) Bridge ID가 가장 낮은 Swtich3이 Root Bridge, 다음으로 낮은 Swtich4가 Backup Root Bridge, 나머지 Switch5와 Switch6은 Non Root Bridge로 지정된다.

2) Switch4와 Switch5에서 Root Bridge(Switch3)로 가는 최단 경로 포트인 Swtich4의 Fa0/1와 Switch5의 Fa0/2가 Root Port로 선정된다.

Switch6은 두 포트 모두 최소 경로이므로 Bridge ID가 더 낮은 Swtich4의 Fa0/2가 Root Port로 선정된다.

3) Root Bridge에 연결된 Switch3의 Fa0/1과 Fa0/2가 지정 포트로 선정된다.

Switch5와 Switch6을 연결한 세그먼트의 포트 중 Path Cost가 낮은 Switch5의 Fa0/1가 지정 포트로 선정된다. Switch4와 Switch5를 연결한 세그먼트의 포트 중 Path Cost가 낮은 Switch4의 Fa0/2가 지정 포트로 선정된다.

4) 남은 Switch6의 Fa0/1가 Alternated Port(Blocking Port)가 된다. (Blocking)

## **8.3. STP 확인**

명령어: (관리자 모드) show spanning-tree vlan 1

텍스트이(가) 표시된 사진

자동 생성된 설명

1) 관리자 모드에서 show spanning-tree vlan 1 명령어 입력

2) Root Bridge의 Bridge ID 3) 접속한 Switch의 Bridge ID

4) 연결된 인터페이스 5) 포트 유형 - Root, Desg, Altn

6) Path Cost 7) Port ID

8) STP 상태

텍스트, 영수증, 스크린샷이(가) 표시된 사진

자동 생성된 설명

텍스트, 영수증, 스크린샷이(가) 표시된 사진

자동 생성된 설명 텍스트, 영수증, 스크린샷이(가) 표시된 사진

자동 생성된 설명

텍스트, 영수증, 스크린샷이(가) 표시된 사진

자동 생성된 설명

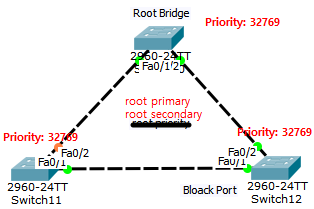
텍스트, 영수증, 스크린샷이(가) 표시된 사진

자동 생성된 설명

## **8.4. STP 수동 설정**

Priority 값을 변경하거나 Primary/Secondary 지정을 통해 Root Bridge 및 Blocking 수동 설정이 가능하다.

**1.4.1. Primary/Secondary 지정**



Priority 값을 변경하여 Switch10이 Root Bridge가 되고 Switch12의 Fa0/1이 Block Port가 되도록 만든다.

**Switch10 - Root Bridge**

텍스트이(가) 표시된 사진

자동 생성된 설명

전역 설정 모드에서 ‘spanning-tree vlan 1 root primary’ 명령어를 사용

STP 상태를 확인해 보면 Switch10의 Priority 값이 조정되고 Root Bridge가 되어있다.

**Switch11 – Backup Root Bridge**

텍스트이(가) 표시된 사진

자동 생성된 설명

전역 설정 모드에서 ‘spanning-tree vlan 1 root secondary’ 명령어를 사용

STP 상태를 확인해 보면 Switch11의 Priority 값이 조정되어 있지만 연결 포트가 Blocking되지는 않는다.

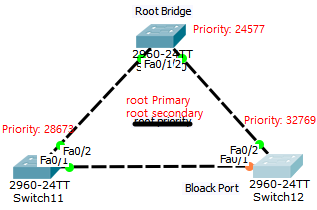
**Switch 12 - Non** **Root Bridge 중 Block Port와 연결된 Bridge**

텍스트이(가) 표시된 사진

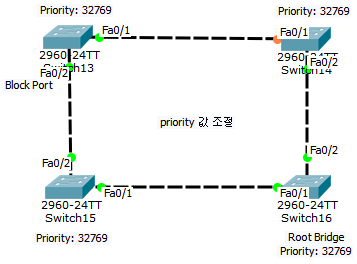
자동 생성된 설명

연결된 포트 중 Root Bridge와 먼 포트가 Block Port가 되어있다.

**최종 상태**



**1.4.2. Priority 값 변경**



**Switch16 - Root Bridge**



전역 설정 모드에서 ‘spanning-tree vlan 1 priority 4096’ 명령어 사용 (4096의 배수만 가능)

-> priority 값이 4096으로 변경된다.

**Switch14 - Backup Root Bridge**

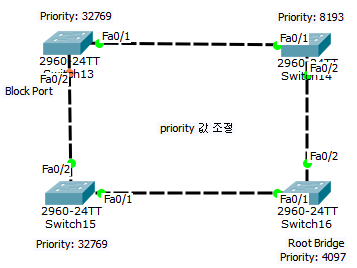


Switch13의 Block Port가 아닌 포트와 이어지는 Switch14가 Switch13보다 우선순위가 높아야 한다.

전역 설정 모드에서 ‘spanning-tree vlan 1 priority 8192’ 명령어 사용 (무조건 Root Bridge보다 우선순위 낮게)

-> priority 값이 8192으로 변경된다.

**최종 상태**

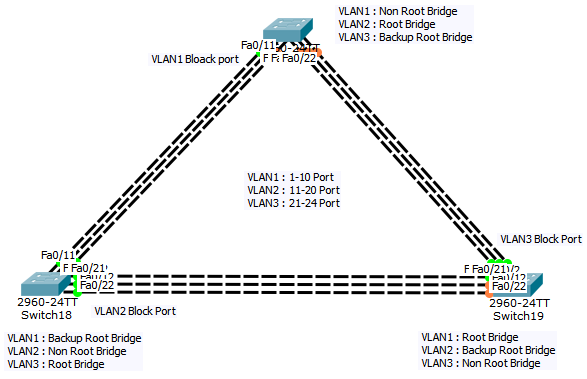


Switch16이 Root Bridge가 되고 Switch13의 Fa0/2가 Block Port가 되어있는 것을 확인

## **8.5. PVST**

PVST(Per VLAN Spanning-Tree): VLAN 별 이중화를 위해 VLAN 별로 STP를 구현한다.

**8.5.1. 구상도**



**8.5.2. VLAN 설정**

텍스트이(가) 표시된 사진

자동 생성된 설명

3개의 스위치 모두 동일하게 설정

테이블이(가) 표시된 사진

자동 생성된 설명 테이블이(가) 표시된 사진

자동 생성된 설명

STP 확인 (Switch17의 STP 상태)

**8.5.3. VLAN 1 설정**



Switch19(Root Bridge) VLAN1 priority 변경



Switch18(Backup Root Bridge) VLAN1 priority 변경

테이블이(가) 표시된 사진

자동 생성된 설명텍스트이(가) 표시된 사진

자동 생성된 설명

Switch17 Switch18

텍스트이(가) 표시된 사진

자동 생성된 설명

Switch19

**8.5.4. VLAN 2 설정**



Switch17(Root Bridge) VLAN2 root primary 설정



Switch19(Backup Root Bridge) VLAN2 root secondary 설정

텍스트이(가) 표시된 사진

자동 생성된 설명 텍스트이(가) 표시된 사진

자동 생성된 설명

Switch17 Switch18

텍스트이(가) 표시된 사진

자동 생성된 설명

Switch19

**8.5.5. VLAN 3 설정**



Switch18(Root Bridge) VLAN3 root priority 변경



Switch17(Backup Root Bridge) VLAN3 root priority 변경

테이블이(가) 표시된 사진

자동 생성된 설명텍스트이(가) 표시된 사진

자동 생성된 설명

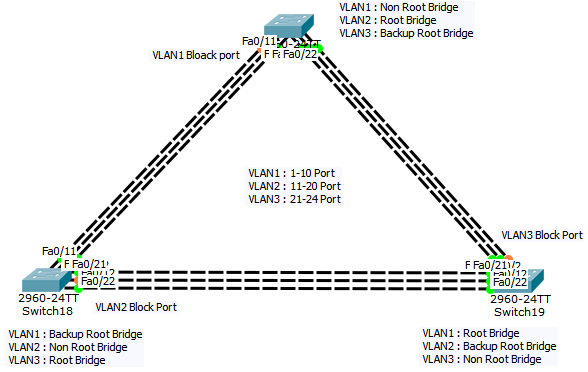
Switch17 Switch18

테이블이(가) 표시된 사진

자동 생성된 설명

Switch19

**1.5.6. 확인**



Switch17의 Fa0/1, Switch18의 Fa0/12, Switch19의 Fa0/21이 Block Port가 된 것을 확인

# **9. VTP**

## **9.1. VTP**

**9.1.1. VTP란?**

VTP(VLAN Trunking Protocol)은 연결된 스위치끼리 VLAN 정보를 자동으로 주고받아 동기화하게 해주는 Cisco 전용 프로토콜이다. 2계층 트렁크 프레임을 사용하여 VTP 서버 모드의 핵심 스위치로부터의 네트워크 측에 존재하는 VLAN들의 추가, 삭제, 이름 변경을 관리하여 전체 네트워크에 걸쳐 VLAN 구성의 일관성을 유지시키고 각 스위치의 동일한 VLAN 정보를 구성할 필요성을 줄여준다.

**9.1.2. VTP 설정 조건**

1) 스위치에서는 VTP가 기본적으로 동작되며 끌 수 없는 프로토콜이다.

2) 스위치들이 **VLAN Domain Name**을 갖도록 설정해야만 VLAN 정보를 동기화 할 수 있다.

3) VTP 동기화 메시지를 주고받으려면 스위치 간에 연결된 포트를 **Trunk Port**로 설정해야 한다.

4) VLAN 정보가 무분별하게 동기화 될 수 있기에 VTP password 설정을 권장하며 스위치 간에 **패스워드가 일치**하지 않으면 동기화 되지 않는다.

5) 확장 VLAN(1006~4094)은 Transparent Mode에서만 사용이 가능하다.

6) 패스워드 설정 -> 도메인 설정 -> 모드 설정 -> Trunk Port 설정 -> VLAN 설정 -> Port VLAN 설정 순으로 해줘야 안전하다.

7) 보안상의 문제로 VTP Transparent Mode를 권장한다.

**9.1.3. VTP Mode**

1) VTP Server Mode

VLAN 정보를 직접 생성, 전송할 수 있다. (VLAN 1~1005)

2) VTP Client Mode

VTP Server로부터 VLAN 정보를 받아 저장하며 직접 VLAN 정보를 설정할 수 없다.

3) VTP Transparent Mode

자신만의 VLAN 정보를 설정할 수 있고 다른 스위치에게 자신의 VLAN 정보를 전송하지 않으며 VLAN Server로부터 받은 정보로 동기화하지 않지만 받은 정보는 다른 스위치에게 전송한다. (VLAN 1~4049, Revision Number 0)

**9.1.4. VTP Message**

1) Summary Advertisement

VTP Server가 자신과 연결된 스위치에게 5분 주기로 전달하는 메시지이다. 자신이 관리하는 VTP Domain에 Revision Number를 전송한다. 다른 스위치들은 Revision Number를 받아서 자신의 VLAN 정보가 최신인지 아닌지 구분한다. VLAN 구성에 변화가 생겼을 시에는 5분 주기 전송이 아닌 즉시 전송을 한다.

2) Subnet Advertisement

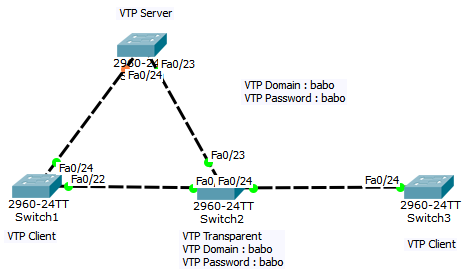
VLAN 구성이 변경되었을 때나 VTP Client로부터 Advertisement Request를 수신했을 때 전송하는 VLAN 정보를 가지고 있는 메시지이다.

3) Advertisement Request

VTP Client가 Server에게 메시지를 요청하거나 자신이 가지고 있는 Revision Number보다 높은 Revision Number를 가지고 있거나 VTP Domain 변동 등 여러가지 VLAN에 변화가 생겼을 때 VTP Server에게 전송하는 메시지이다.

## **9.2. VTP 설정**

**9.2.1. 구성도**



**9.2.2. Trunk 설정**

텍스트이(가) 표시된 사진

자동 생성된 설명

모든 스위치의 21-24 Port를 Trunk Mode 설정

**9.2.3. VTP Server 설정**

**Switch0**

텍스트이(가) 표시된 사진

자동 생성된 설명

VTP 설정 및 확인

1) Domain Name 설정 2) VTP Password 설정 3) VTP 정보 보기



VTP Password 확인

**9.2.4. VTP Transparent 설정**

**Switch2**



VTP Transparent Mode로 변경

Domain Name 설정 Password 설정

텍스트이(가) 표시된 사진

자동 생성된 설명

VTP 설정 확인

2.2.5. VTP Client 설정

**Switch1 & Switch3**

텍스트, 테이블이(가) 표시된 사진

자동 생성된 설명

1) VTP Client Mode로 변경 2) Domain Name 설정 3) Password 설정

텍스트이(가) 표시된 사진

자동 생성된 설명

VTP 설정 확인



Client Mode에서 VLAN을 생성할 수 없다.

**9.2.5. VLAN 구성**

**VTP Server**

텍스트이(가) 표시된 사진

자동 생성된 설명 텍스트, 스크린샷, 노트북이(가) 표시된 사진

자동 생성된 설명

VLAN 생성 Number of existing VLANs(기존 VLAN 수) 변화 확인

**VTP Client**

테이블이(가) 표시된 사진

자동 생성된 설명

VTP Server에 생성한 VLAN이 VTP Client에 동일하게 생성되었다.

**VTP Transparent**

테이블이(가) 표시된 사진

자동 생성된 설명

VTP Transparent에는 VLAN이 생성되지 않았다.



VTP Transparent에 따로 VLAN 생성

**VTP Client & VTP Server**

테이블이(가) 표시된 사진

자동 생성된 설명

VTP Transparent에 생성한 VLAN이 VTP Server나 VTP Client에 생성되지 않는다.

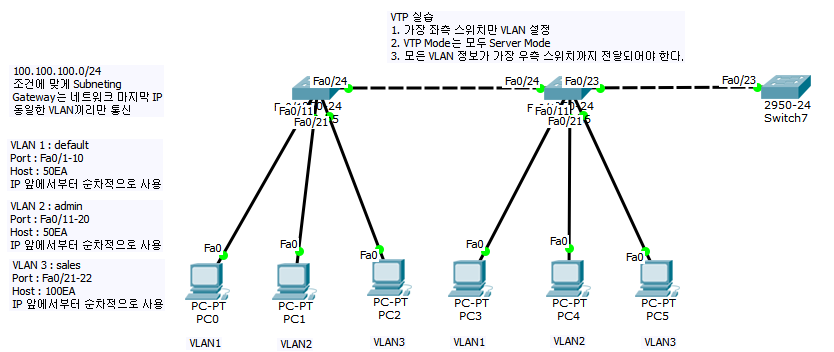
## **9.3. VTP Pruning**

(Pruning: 가지치기) VLAN을 조금 더 효율적으로 관리하기 위해 만든 기술로 VLAN 트래픽이 이동할 때 갈 필요가 없는 Trunk Port 방향을 잘라서 자신과 상관없는 VLAN 정보에 대한 트래픽을 Trunk Port일지라도 수신하지 않게 하는 기술이다. -> Trunk 대역폭을 절약

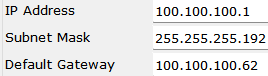
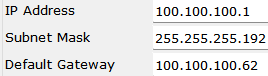
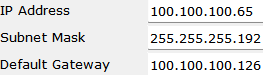
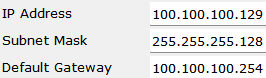
VTP Server에서 전역 설정 모드 상태로 ‘**vtp pruning**’ 명령어를 입력하면 연결된 Client들에게 자동으로 설정

## **9.4. VTP 실습**

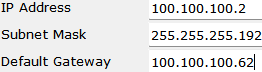
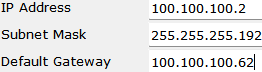
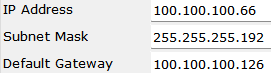
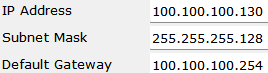
**9.4.1. 구성도**



**9.4.2. 서브넷팅**

PC0 PC1 PC2

PC3 PC4 PC5

**9.4.3. VTP Server 설정**

텍스트이(가) 표시된 사진

자동 생성된 설명텍스트이(가) 표시된 사진

자동 생성된 설명

VTP Password, VTP Domain Name 설정 (기본적으로 VTP Server Mode이기 때문에 따로 Mode 설정x)

3개의 스위치 동일하게 설정 (반드시 동일한 Domain Name, 동일한 Password)

텍스트이(가) 표시된 사진

자동 생성된 설명

VTP 정보 확인

**9.4.4. Trunk Port 설정**

텍스트이(가) 표시된 사진

자동 생성된 설명

Fa0/23-24 Trunk Port 설정 (3개 스위치 동일하게 설정)

**9.4.5. VLAN 구성**

**Switch5**

텍스트이(가) 표시된 사진

자동 생성된 설명 텍스트이(가) 표시된 사진

자동 생성된 설명

VLAN 2, 3 생성 Port 할당

테이블이(가) 표시된 사진

자동 생성된 설명

VLAN 확인

**Switch6 & Switch7**

테이블이(가) 표시된 사진

자동 생성된 설명

VTP에 의하여 VLAN 2, 3이 생성되어 있지만 Port는 할당되어 있지 않다. **(VTP는 Port 정보는 옮기지 않는다.)**

텍스트이(가) 표시된 사진

자동 생성된 설명

VLAN Port 할당 및 확인

**9.4.6. Ping 테스트**

텍스트이(가) 표시된 사진

자동 생성된 설명

PC0(100.100.100.1)에서 Ping Test

텍스트이(가) 표시된 사진

자동 생성된 설명

PC1(100.100.100.65)에서 Ping Test

텍스트이(가) 표시된 사진

자동 생성된 설명

PC2(100.100.100.129)에서 Ping Test

같은 VLAN끼리만 통신이 가능하다.

# **10. Cisco 장비 복구**

## **10.1. 장비 동작에 필요한 파일 및 메모리**

Cisco 장비(Switch와 Router) 동작에 필요한 파일과 메모리

**10.1.1. File**

**IOS 이미지 파일 (Internet Operating System Image File)**

Switch 혹은 Router가 사용하는 OS(운영체제)로 특정 하드웨어 모델에 특화되어 있다.

**구성 파일 (Configuration File)**

Switch 혹은 Router 동작에 필요한 모든 명령어들을 포함하는 명령어 파일

**10.1.2. Memory**

**Flash Memory**

ISO 이미지 파일, VLAN 정보 등이 저장되어 있다. (비휘발성)

**NVRAM (Nonvoratile RAM)**

Configuration 파일 저장 (비휘발성)

startup-config 파일 -> write로 저장된 설정, 스위치를 키면 NVRAM에서 RAM으로 적재된다.

**RAM**

스위치 테이블, 큐잉, 시스템과 인터페이스를 위한 버퍼 등 다양한 용도로 사용 (휘발성)

running-config 파일 -> RAM에서 사용하는 구성 파일. 스위치를 켜면 NVRAM에서 RAM으로 적재되는 startup-config 파일이 running-conifg 파일이 된다.

## **10.2. 패스워드 초기화**

**10.2.1. 비밀번호 설정**

 텍스트이(가) 표시된 사진

자동 생성된 설명

관리자 모드 비밀번호 설정 및 저장

**10.2.2. 장비 재부팅**



장비 재부팅

**10.2.3. Rommon Mode 진입**

텍스트이(가) 표시된 사진

자동 생성된 설명

부팅 or 재부팅 중에 ‘Ctrl + Break’ 혹은 ‘Ctrl + c’를 눌러 Rommon 모드로 진입한다.

(Rommom Mode: 장비 문제 해결용 작은 운영체제)

텍스트이(가) 표시된 사진

자동 생성된 설명

Rommom 모드에서 사용할 수 있는 명령어들



0x2142번지(대화형 구성 모드가 들어가 있다)로 접근하고 reset으로 재부팅

**10.2.4. 초기 대화형 구성 모드 진입**

텍스트이(가) 표시된 사진

자동 생성된 설명

초기 대화형 구성 모드로 부팅된다.

텍스트이(가) 표시된 사진

자동 생성된 설명

NVRAM에 있던 startup-config를 running-config로 불러온다.

**10.2.5. 비밀번호 변경**



전역 설정 모드로 진입해서 패스워드 재설정 (바로 재부팅x)

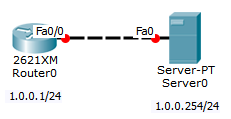
**10.2.6. Register 지정 및 재부팅**

텍스트이(가) 표시된 사진

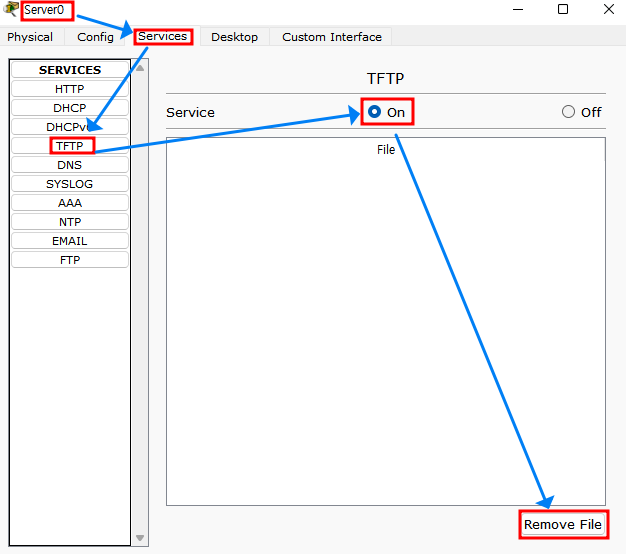
자동 생성된 설명

Config-register 명령어로 0x2102번지로 부팅하도록 설정하고 저장 후 재부팅

## **10.3. IOS 및 Config 파일 Backup/Restore**

TFTP를 이용해 IOS 이미지 파일과 Configuration 파일을 백업/복구하기

**10.3.1. Server TFTP 설정**



Server0 -> Services -> TFTP -> Service On (보통 기본으로 On되어 있다.) -> 편의상 기존 파일 모두 삭제

**10.3.2. Router 기본 설정**

텍스트이(가) 표시된 사진

자동 생성된 설명

간단한 기본 설정 및 저장

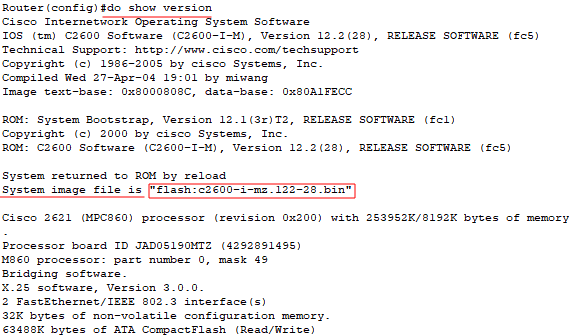
**10.3.3. ISO 및 Config 파일 Backup**

텍스트이(가) 표시된 사진

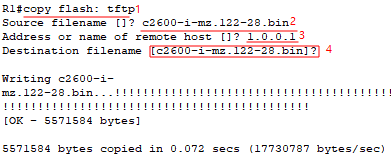
자동 생성된 설명

Configuration 파일 Backup

1) startup-config TFTP로 복사 2) 서버의 IP 주소 3) 저장할 파일명



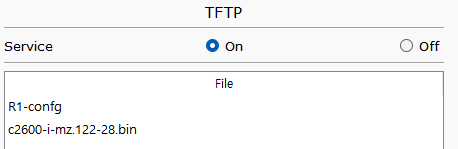
‘show version’ 명령어를 사용하여 장비 정보 중에 IOS 이미지 파일 정보 확인



IOS 이미지 파일 Backup

1) flash memory에 있는 파일 TFTP로 복사 2) IOS 이미지 파일명

3) 서버의 IP 주소 4) 저장할 파일명



TFTP를 통해 Backup된 파일 확인

**10.3.4. 파일 삭제**

텍스트이(가) 표시된 사진

자동 생성된 설명

startup-config 파일 삭제



IOS 이미지 파일 삭제

**10.3.5. Rommon Mode 진입**



재부팅

텍스트이(가) 표시된 사진

자동 생성된 설명

부팅이 실패하여 Rommon Mode로 진입된다.

**10.3.6. IOS 이미지 파일 불러오기**

텍스트이(가) 표시된 사진

자동 생성된 설명

tftpdnld 명령어를 입력하면 TFTP를 사용하기 위해 입력해야 하는 것들이 나온다.

텍스트이(가) 표시된 사진

자동 생성된 설명

정보 입력 (rommon 3에서 오타: IP\_ADDRES=1.0.0.254 -> IP\_ADDRESS=1.0.0.254)

텍스트이(가) 표시된 사진

자동 생성된 설명

tftpdnld 명령어를 입력하여 TFTP Server에서 IOS 이미지 파일 불러오기



재부팅 -> 초기 대화형 구성 모드로 부팅된다.

**10.3.7. Configuration 파일 불러오기**

텍스트, 스크린샷, 조류이(가) 표시된 사진

자동 생성된 설명

IP 설정

텍스트이(가) 표시된 사진

자동 생성된 설명

TFTP Server에서 Configuration 백업 파일 불러오기

1) TFTP Server에서 파일 running-config로 불러오기

2) 서버의 IP 주소 2) 파일명 (Configure 백업 파일)

**10.3.8. 재부팅**

텍스트이(가) 표시된 사진

자동 생성된 설명 텍스트이(가) 표시된 사진

자동 생성된 설명

저장 후 재부팅 설정 복구 확인

# **11. RIP**

## **11.1. RIP**

**11.1.1. RIP란?**

RIP(Routing Information Protocol): 동적 라우팅 프로토콜 중 가장 오래된 것으로 동작 방식이 간단하며 설정도 간편하게 할 수 있다. 버전 1과 버전 2가 있는데 버전 1인 RIPv1은 Classful Routing Protocol이라 거의 사용하지 않고 버전 2인 RIPv2는 Classless Routing Protocol으로 Bellman-Ford 알고리즘을 사용한다.

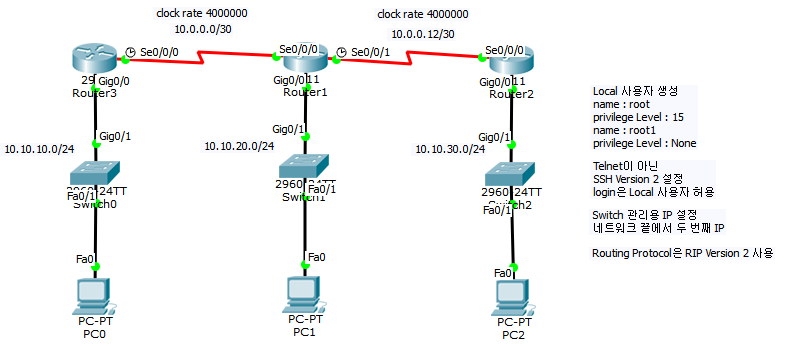
**11.1.2. RIP 특징**

1) Distance Vector AI 사용 2) Routing Protocol 3) Classful Routing Protocol

4) RFC 1058 명세서 번호 6) UDP 520 Port

## **11.2. RIPv2 설정**

**11.2.1. 구성도**



**11.2.2. Router3 설정**

텍스트이(가) 표시된 사진

자동 생성된 설명텍스트이(가) 표시된 사진

자동 생성된 설명텍스트이(가) 표시된 사진

자동 생성된 설명

라우터 기본 설정 Routing 설정 SSH 설정

**11.2.3. Router1 설정**

텍스트이(가) 표시된 사진

자동 생성된 설명 텍스트이(가) 표시된 사진

자동 생성된 설명 텍스트이(가) 표시된 사진

자동 생성된 설명

라우터 기본 설정 Routing 설정 SSH 설정

**11.2.4. Router2 설정**

텍스트이(가) 표시된 사진

자동 생성된 설명텍스트이(가) 표시된 사진

자동 생성된 설명텍스트이(가) 표시된 사진

자동 생성된 설명

라우터 기본 설정 Routing 설정 SSH 설정

**11.2.5. Routing Table 확인**

텍스트이(가) 표시된 사진

자동 생성된 설명

R(RIP 프로토콜)에 의해 라우팅 테이블이 작성된 것을 확인

# **0. 최하단**