Network Infrastructure Security

Packet Tracer · OSPF · Dynamic Routing · Static Route · HSRP · Inter Vlan

ABYLBEK KYZY MARAL

Junior Network & Infrastructure Engineer

개발 경험을 바탕으로 네트워크 인프라와 보안 구성을 직접 실습하며 “구조를 이해하고 안정적으로 운영하는 것”에 집중하고 있습니다. 저는 구성의 이유를 이해하고 안정적인 운영을 목표로 설정 상태를 점검하는 엔지니어가 되고 싶습니다. 실제 환경에서 필요한 설정을 정확히 적용하고, 서비스 관점에서 “사용자가 문제 없이 이용할 수 있는 네트워크”를 만드는 데 기여하고자 합니다.

전공: 컴퓨터정보과 네트워크 인프라 · 보안

이력서 PDF 다운로드

ABOUT

네트워크 인프라 & 웹 구현 역량을 갖춘 엔지니어

Packet Tracer 기반 라우팅·스위칭 실습을 통해 트래픽 흐름과 설정 변경이 서비스 품질에 어떤 영향을 주는지 직접 확인해 왔고, 문제 발생 시 원인을 분석하고 검증하는 절차를 중요하게 생각합니다.

또한 학교 프로젝트와 개인 포트폴리오 작업을 통해 웹 화면 구현 역량을 함께 갖추고 있어, 네트워크 구성과 사용자 경험을 함께 바라보는 시각을 지향합니다.

- IPv4, VLAN, 라우팅, 포트 보안 등 인프라 핵심 요소를 직접 구성
- 문제 상황에서 `ping`, `traceroute`, 각종 `show` 명령어로 원인 추적 경험
- 사용자 입장에서 “접속이 잘 되는 네트워크”를 목표로 설정을 검토

SKILLS

네트워크 지원 직무에서 바로 업무에 연결될 수 있는 기본 영역을 중심으로 정리했습니다.

Network Fundamentals

IPv4 주소 체계, Subnetting, 주소 체계 설계

Broadcast / Collision Domain 구분

L2 · L3 계층 구조와 역할 이해

Routing & Switching

Static Routing / OSPF 기반 Dynamic Routing 구성 & 검증

VLAN / Inter-VLAN Routing 환경 설계 및 실습

EtherChannel(LACP) 활용한 링크 집성과 STP 환경 이해

Network Security

Port Security를 통한 MAC 기반 접속 제어 구성

기본적인 네트워크 공격 시나리오와 대응 개념 이해

보안 설정 변경이 서비스에 미치는 영향 확인 경험

Troubleshooting & Tools

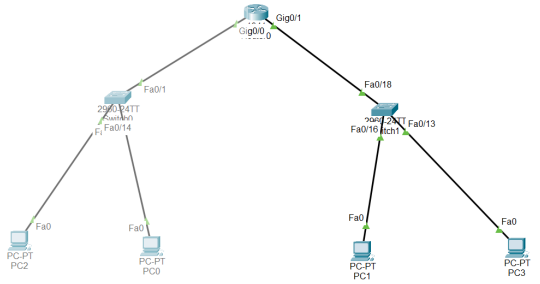
show 명령을 활용한 인터페이스/라우팅 테이블 확인

Cisco Packet Tracer 기반 Topology 설계 및 실습

Ubuntu / Windows 환경의 기본 네트워크 점검 경험

Practice Labs

Packet Tracer를 활용해 실제 환경을 가정하고 구성한 주요 실습입니다. Topology 설계 → 설정(Config) → 검증(Verification) → 문제 분석 순서로 진행했습니다.



DHCP Configuration

Address Management

Problem PC들이 자동으로 IP를 받지 못해 통신이 되지 않는 상황

Analysis DHCP 풀 범위 및 `excluded-address` 설정이 실제 네트워크 대역과 맞지 않음을 확인

Solution 네트워크/게이트웨이/DNS 정보를 재설정하고, 각 PC에서 IP 재할당 후 통신을 검증

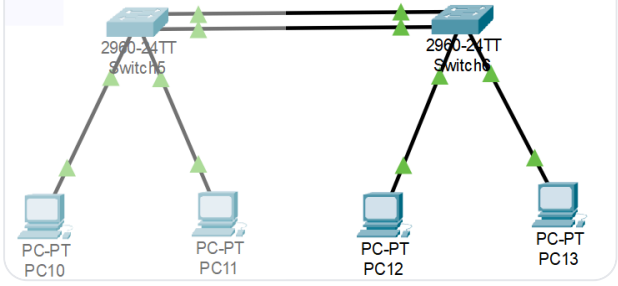
192.168.1.0/24 네트워크에서 DHCP 서버를 구성하여 IP 주소, 게이트웨이, DNS를 자동으로 할당하는 환경을 설계했습니다.

Network: 192.168.1.0/24 · Gateway: 192.168.1.1 · DNS: 192.168.1.10 · Domain: com.kr

Config | Verification

```
ip dhcp excluded-address 1.1.1.1 1.1
ip dhcp pool VLAN1
 network 192.168.1.0 255.255.255.0
 default-router 192.168.1.1
 dns-server 192.168.1.10
 domain-name com.kr
```

각 PC가 올바른 게이트웨이와 DNS 정보를 할당받는지 확인하고, 잘못된 설정이 있을 때 PC 단에서 보이는 증상을 비교했습니다.



EtherChannel (LACP)

Link Aggregation

Problem 스위치 간 여러 링크를 연결했지만 STP에 의해 일부 링크가 차단되는 상황

Analysis STP가 동일 경로로 인식해 하나의 포트만 활성화하고 나머지는 Blocking 상태로 유지되는 것을 확인

Solution EtherChannel(LACP)로 물리 링크를 하나의 논리 Port-Channel로 묶어, STP와 충돌 없이 대역폭을 증가하도록 구성

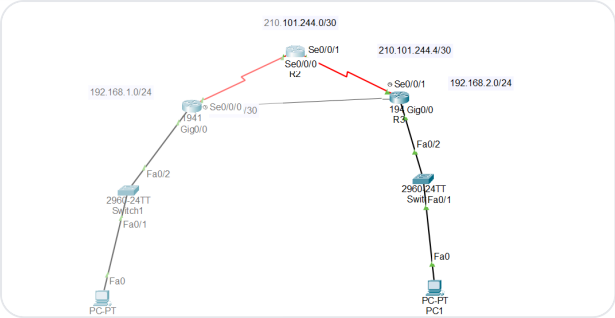
스위치 사이 다중 링크를 LACP 기반 EtherChannel로 구성하여, STP와 충돌 없이 안정적으로 링크를 사용하는 실습을 진행했습니다.

LACP 기반 링크 집성 · Port-Channel 인터페이스 설정 및 검증

Config | Verification

```
interface range fa0/1 - 2
 channel-group 1 mode active
!
interface port-channel 1
 switchport mode trunk
```

EtherChannel 구성 전·후의 STP 상태와 사용 가능한 대역폭 변화를 비교하며 링크 집성의 효과를 정리했습니다.



OSPF Single-Area Routing

Dynamic Routing

Problem 여러 라우터에 연결된 네트워크 간에 라우팅 정보가 자동으로 공유되지 않는 상황

Analysis 정적 라우팅만으로는 관리가 비효율적이며, Dynamic Routing 프로토콜 (OSPF)이 필요함을 확인

Solution Area 0 기반 OSPF를 구성하고 Router-ID와 network 범위를 정의하여 경로를 자동으로 교환하도록 설정

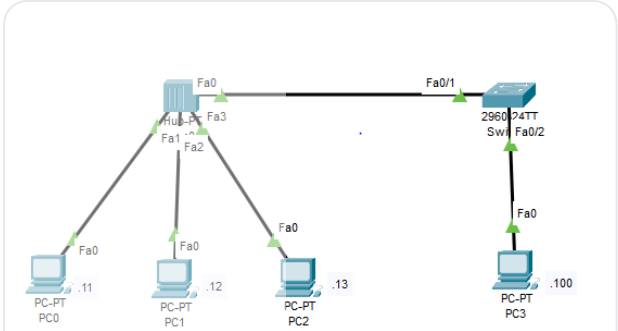
여러 라우터를 단일 Area 0으로 구성하고 OSPF를 적용하여 링크 상태 기반 경로 계산과 라우팅 테이블 변화를 확인했습니다.

Area 0 · Router-ID 설정 · Neighbor 관계 및 라우팅 테이블 검증

Config Verification

```
router ospf 1
 router-id 1.1.1.1
 network 192.168.1.0 0.0.0.255 area
 network 210.101.244.0 0.0.0.3 area
```

OSPF Neighbor 상태 변화와 라우팅 테이블 업데이트를 단계별로 확인하며, Dynamic Routing이 필요한 이유를 다시 정리했습니다.



Port Security

Access Control

Problem 허가되지 않은 단말이 스위치 포트에 연결되어도 네트워크에 접근 가능한 상황

Analysis Access Port에 대한 보안 설정이 없어 MAC 기반 제어가 이뤄지지 않고 있음을 확인

Solution Port Security로 허용 MAC 개수와 Violation 동작을 정의하고, Sticky MAC 옵션으로 실제 접속 단말을 고정

특정 포트에 허용된 단말만 접속하도록 Port Security를 구성하고, MAC 주소 기반으로 접속을 제한하는 실습을 진행했습니다.

MAC 기반 제한 · 최대 접속 수 지정 · Violation 동작 설정

Config Verification

```
interface fa0/1
 switchport mode access
 switchport port-security
 switchport port-security maximum 1
 switchport port-security violation
 switchport port-security mac-addres
```

허용된 단말과 허용되지 않은 단말을 번갈아 연결해 보며 포트 상태 변화와 로그를 확인했습니다.

Security (보안)

네트워크 실습을 진행하면서 트래픽이 실제로 어떻게 흐르고, 어떤 지점에서 취약점이 발생할 수 있는지 구조적인 관점에서 함께 확인했습니다.

특히 “보안은 추가 기능이 아니라 기본 구성의 일부”라는 관점으로 네트워크 환경에서 자주 발생할 수 있는 위험 요소를 체크하는 습관을 갖고자 했습니다.

- ARP 스푸핑 등 L2 단계에서 발생할 수 있는 기본 공격 개념 이해
- Unknown Unicast Flooding 구조 이해 및 스위치 동작 방식 검토
- 불필요한 서비스·포트를 비활성화하여 공격 표면을 최소화하는 원칙 학습
- 로그 기반 모니터링을 통해 정상/비정상 트래픽 패턴 구분 연습
- 네트워크 변경 시 영향도와 잠재적 보안 리스크를 함께 점검하는 습관 형성

CONTACT

연락처 & 기본 정보

이름	ABYLBEK KYZY MARAL (마랄)
생년월일	2001.02.09
이메일	abylbekmaral@gmail.com maraltolonova@naver.com
연락처	010-6528-0102
지역	대한민국 – 서울 / 대구 거주 및 근무 가능
비자	D-10(구직)