CCNA_210804

OSPF (설정 후)

1.neighbor 관계를 수립(Hello packet)

4가지 항목이 일치: timer (Hello/Dead), 영역ID, 인증유형/인증암호, Stub Area 설정

기본설정(H:10초, D:40초) 정의(반드시 설정) 정의(기본설정x) 정의

OSPF 네트워크 유형

-BMA/p2p : 10/40(H/D)

1가치 반드시 일치하지 않아야함 : router ID

neighbor 관계를 맺으면 neighor 테이블에 등록됨.

---

show ip ospf neighbor

2.neighbor간에 라우팅 정보를 교환.

교환된 라우팅 정보를 LSDB(Link State Database)에 저장함.

해당 라우터가 알고있는 OSPF 경로정보가 저장되어있음. show ip ospf database명력어를 통해 LSDB 내용을 확인 할 수 있음.

3.LSDB에 저장된 경로정보를 이용하여 최적의 경로를 결정함. 이때 SPF 알고리즘으로 다익스트라 알고리즘을 사용하여 최적의 경로를 계산함.

최적의 경로를 계산 한 후 해당 경로를 라우팅 테이블에 등록함.

---

show ip route

*OSPF

Link State Routing Protocol

상태

Link는 라우터의 인터페이스

IP/SM, OSPF 네트워크타입, Cost(메트릭) 등. => 링크상태정보로 이러한것들을 OSPF 업데이트 패킷에 담아서 보내는것.

*OSPF 설정

Router(config)# router ospf Process_ID ! Process_ID 범위 : 1 ~ 65535

Router(config-router)# network Address Wildcard_Mask area area_ID

-Single Area : 하나의 영역만 정의된 OSPF 구성

-Multi Area : 여러개의 영역으로 정의된 OSPF 구성

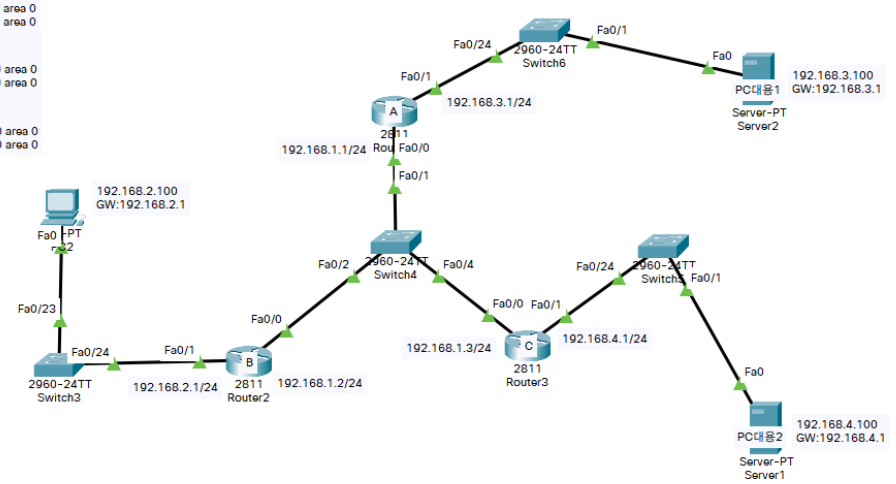
*OSPF 메트릭 공식

COST = 참조 대역폭 (10에8승)

인터페이스 대역폭 (bps)

*실습하기

```
A
 A(config)# router ospf 1
 A(config-router)# network 192.168.3.1 0.0.0.0 area 0
 A(config-router)# network 192.168.1.1 0.0.0.0 area 0
B
 B(config)# router ospf 1
 B(config-router)# network 192.168.1.2 0.0.0.0 area 0
 B(config-router)# network 192.168.2.1 0.0.0.0 area 0
C
 C(config)# router ospf 1
 C(config-router)# network 192.168.1.3 0.0.0.0 area 0
 C(config-router)# network 192.168.4.1 0.0.0.0 area 0
```



*DR/BDR 선출조건

1.우선 순위 값을 비교해서 가장 큰 우선순위 값을 가진 라우터가 DR이 되고, 그 다음 우선순위가 높은 라우터는 BDR이 된다. 그 외에 나머지 라우터는 자동으로 DROther로 결정된다.

>>모든 라우터의 우선순위 값은 동일함. 즉, 기본값으로 1을 사용함.
>>특정 라우터에 우선 순위 값을 0으로 정의하면 해당 라우터는 DRother로 결정됨.

>>Router(config-if)# ip ospf priority priority_value (0 ~ 255)

다수의 네이버 라우터와 연결된 인터페이스에 우선순위값을 설정한다.

2.라우터 ID를 비교해서 가장 큰 라우터 ID를 가진 라우터가 DR이 되고, 그 다음 라우터가 BDR이된다.
그 외에 나머지 라우터는 자동으로 DRother로 결정이 된다.

*Timer (H/D) 설정
Router(config-if)# ip ospf hello-interval timer_values
Router(config-if)# ip ospf dead-interval timer_values

*OSPF 인증설정
평문 암호 인증
Step 1. 인증에 사용할 암호 정의
Router(config-if)# ip ospf authentication-key 인증암호
Step 2. 인증 유형 지정(평문 암호 인증 활성화)
Router(config-if)# ip ospf authentication

MD5 암호 인증
Step 1. 인증에 사용할 암호 정의
Router(config-if)# ip ospf authentication-key 인증암호
Step 2. 인증 유형 지정(MDR 암호 인증 활성화)
Router(config-if)# ip ospf authentication message-digest

*문제 해결 (debug 명령어는 장비에 많은 부하를 줄 수 있기때문에 해당 내용을 확인한 반드시 중지시켜야함)
undebug all (모든 디버그 비활성화)

Router# debug ip ospf events
>> timers 가 일치하지 않으면 해당 디버그 명령어를 통해 확인할 수 있음.

Router# debug ip ospf adj

>> neighbor 인증 유형/암호가 일치하는지 여부를 확인할 수 있음.

*ACL(Access Control List, 접근 제어 목록)
: 패킷 필터링
: IP 주소를 패킷 필터링
: IP(v4) ACL

ACL 유형
1.Standard ACL (표준ACL) : 패킷의 출발지 주소만 확인하여 필터링을 함

IP 헤더의 Source Address를 의미 함.

2.Extended ACL (확장ACL) : 패킷의 출발지 주소/ 목적지 주소
TCP/UDP 헤더의 출발지 포트 번호/ 목적지 포트번호
를 이용해서 패킷을 필터링 함.

Standar ACL 설정
Step 1.정의
Router(config)# access-list list_number [permit | deny] address wildcard_mask
---
1~99사이의 숫자

Step 2.적용
Router(config-if)# ip access-group list_number [in | out] |or의 뜻

>> Standard ACL 정의 예제
Router(config)# access-list 1 permit 192.168.1.0 0.0.0.255

출발지 네트워크
192.168.1.0 255.255.255.0
= 192.168.1.0 / 24
= 192.168.1.0 ~ 192.168.1.255
--> 192.168.1.1 ~ 192.168.1.254

>> 수신 패킷의 출발지 주소(IP헤더)가 192.168.1.1 ~ 192.168.1.254 범위에 속한다면, 해당 패킷은 허용(permit)하겠다.