12. 접근 제어 목록

ICT폴리텍대학

강 상 희

12. 접근 제어 목록

목 차

- 표준 ACL
- 확장 ACL
- Named 표준 ACL
- Named 확장 ACL
- TCP Established
- ACL 중간 삽입
- 락-앤-키(Lock-and-key) 인증
- RACL(Reflexive ACL)
- 시간 기반의 time-based ACL

12. 접근 제어 목록(Access Control List)

- 라우터 : 출발지주소와 목적지 주소를 참조하여 라우팅 테이블 기초로 패킷 전달
- **ACL : 주소기반의 패킷 출입 통제 문장, IP주소 기반의 패킷 전달 여부 통제,일명 “패킷 필터링”(packet Filtering)**
- 목적 : 보안 제공 및 트래픽 제어

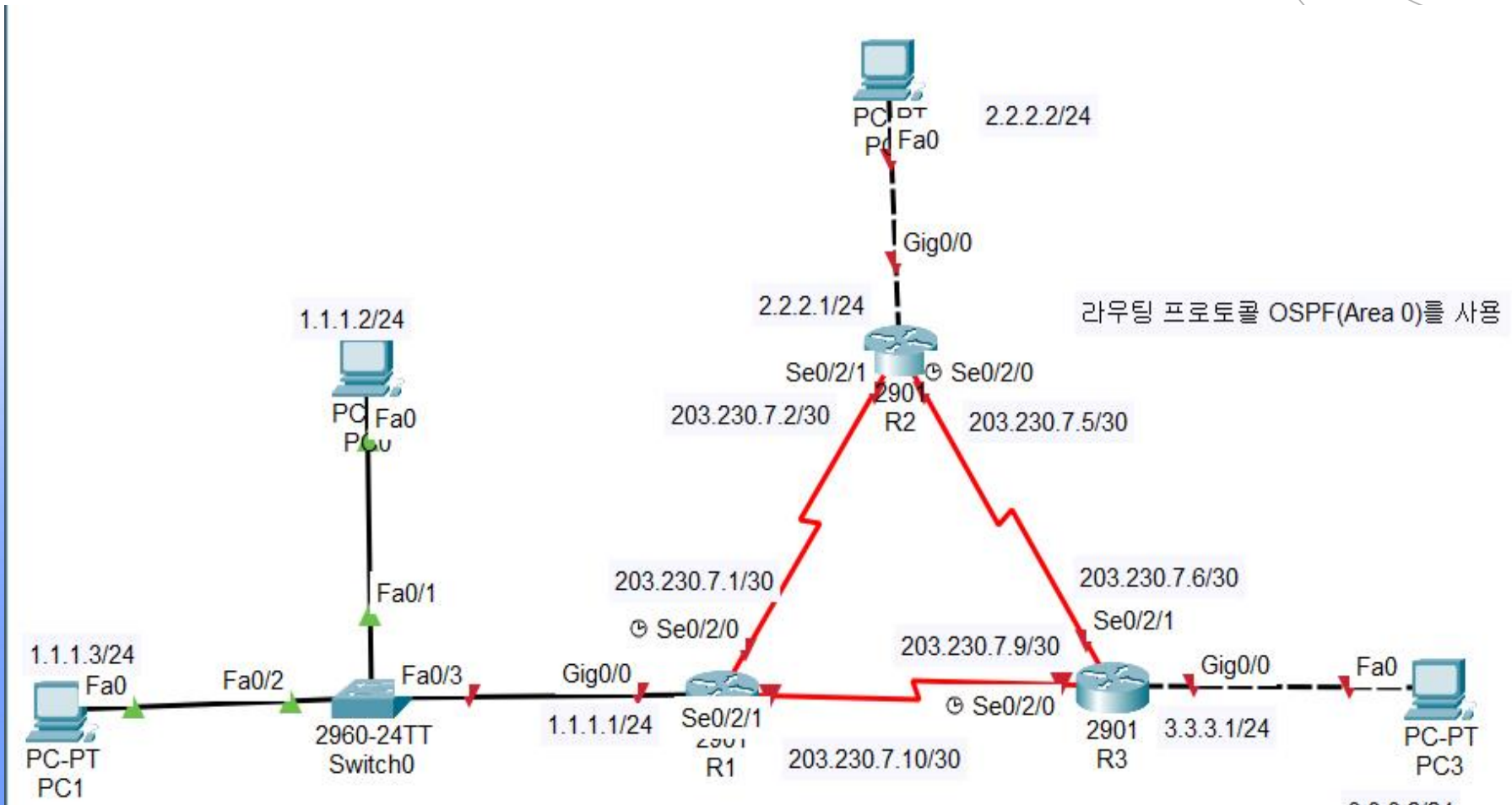
ACL 종류

- **표준 ACL : 출발지 IP 주소 참조하여 패킷 필터링, 1~99, 1300~1999**
- **확장 ACL : 출발지 및 목적지 IP 주소, TCP, UDP, 포트 번호 참조하여 패킷 필터링, 100~199, 2000~2699**
- **Named 표준 ACL : 표준 ACL와 사용자(번호X) 설정 값 사용**
- **Named 확장 ACL : 확장 ACL와 사용자(번호X) 설정 값 사용**

트래픽 종류

- **inbound Traffic(들어오는 트래픽), Outbound Traffic(나가는 트래픽)**

12. 접근 제어 목록(Access Control List)



12. 접근 제어 목록(Access Control List)

R1 설정 스크립트

```
1.  Router#conf t
2.  Router(config)#hostname R1
3.  R1(config)#int g0/0
4.  R1(config-if)#ip add 1.1.1.1 255.255.255.0
5.  R1(config-if)#no shut
6.  R1(config)#int S0/2/0
7.  R1(config-if)#ip add 203.230.7.1 255.255.255.252
8.  R1(config-if)#clock rate 64000
9.  R1(config-if)#no shut
10. R1(config)#int S0/2/1
11. R1(config-if)#ip add 203.230.7.10 255.255.255.252
12. R1(config-if)#no shut
13. R1(config-if)#exit
14. R1(config)#router ospf 1
15. R1(config-router)#network 1.1.1.1 0.0.0.0 area 0
16. R1(config-router)#network 203.230.7.1 0.0.0.0 area 0
17. R1(config-router)#network 203.230.7.10 0.0.0.0 area 0
18. R1(config-router)#do show ip int brief
```

12. 접근 제어 목록(Access Control List)

R2 설정 스크립트

1. Router#conf t
2. Router(config)#hostname R2
3. R2(config)#int g0/0
4. R2(config-if)#ip add 2.2.2.1 255.255.255.0
5. R2(config-if)#no shut
6. R2(config)#int S0/2/0
7. R2(config-if)#ip add 203.230.7.5 255.255.255.252
8. R2(config-if)#clock rate 64000
9. R2(config-if)#no shut
10. R2(config)#int S0/2/1
11. R2(config-if)#ip add 203.230.7.2 255.255.255.252
12. R2(config-if)#no shut
13. R2(config-if)#exit
14. R2(config)#router ospf 1
15. R2(config-router)#network 2.2.2.1 0.0.0.0 area 0
16. R2(config-router)#network 203.230.7.5 0.0.0.0 area 0
17. R2(config-router)#network 203.230.7.2 0.0.0.0 area 0
18. R2(config-router)#do show ip int brief

12. 접근 제어 목록(Access Control List)

R3 설정 스크립트

1. Router#conf t
2. Router(config)#hostname R3
3. R3(config)#int g0/0
4. R3(config-if)#ip add 3.3.3.1 255.255.255.0
5. R3(config-if)#no shut
6. R3(config)#int S0/2/0
7. R3(config-if)#ip add 203.230.7.9 255.255.255.252
8. R3(config-if)#clock rate 64000
9. R3(config-if)#no shut
10. R3(config)#int S0/2/1
11. R3(config-if)#ip add 203.230.7.6 255.255.255.252
12. R3(config-if)#no shut
13. R3(config-if)#exit
14. R3(config)#router ospf 1
15. R3(config-router)#network 3.3.3.1 0.0.0.0 area 0
16. R3(config-router)#network 203.230.7.9 0.0.0.0 area 0
17. R3(config-router)#network 203.230.7.6 0.0.0.0 area 0
18. R3(config-router)#do show ip int brief

표준 ACL(Access Control List)

- 출발지 IP 주소만 판단하여 패킷 필터링 실시

조건 : **PC1(모든 장치와 통신), PC0(차단)**

1. **R1(config)#access-list 1 deny 1.1.1.2 0.0.0.0**
2. **R1(config)#access-list 1 permit any**
3. **R1(config)#int g0/0**
4. **R1(config-if)#ip access-group 1 in /*1번 들어오는(in) 트래픽 적용**
5. **R1(config-if)#no shut**
6. **R1(config-if)#do show access-list /* access-list 확인 */**

조건 : **1.1.1.3 주소만 허용, 나머지 차단**

1. **R1(config)#access-list 1 permit 1.1.1.3 0.0.0.0**
2. **R1(config)#access-list 1 deny any**
3. **R1(config)#int g0/0**
4. **R1(config-if)#ip access-group 1 in**
5. **R1(config-if)#no shut**
6. **R1(config-if)#do show access-list /* access-list 확인 */**

표준 ACL(Access Control List)

- ACL Remark 설정

간단히 주석 달기

1. **R1(config)#access-list 1 remark PC0 packet deny and PC1 packet permit**
2. **R1(config)#do show run /* 확인 */**

표준 ACL(Access Control List)

- 와일드 카드 마스크

서브넷 마스크의 반대되는 값
255.255.0.0(서브넷) -> 0.0.255.255(와일드카드 마스크)

- 표현하고자 하는 주소를 줄일 수 있음
- 패턴 추출할때 : **0:일치, 1:상관없음**
  ex) 203.230.7.0/24 네트워크 중 203.230.7.1/24~7.5/24만 정의할 경우 : 와일드카드(0.0.0.7)로 표시

표준 ACL(Access Control List)

- ACL 문장 구성 및 순서

- **ACL 항목 간의 순서에 의해 접근제어**
- **Any : 0.0.0.0 255.255.255.255 의미(모든 패킷)**
- **Host : 단 하나의 IP 주소 지정할 때 사용하는 인자**
  203.230.7.1 0.0.0.0 = host 203.230.7.1

1. **R1(config)#access-list 1 deny host 1.1.1.2**
2. **R1(config)#access-list 1 permit 1.1.1.0 0.0.0.255**
3. **R1(config)#int g0/0**
4. **R1(config-if)#ip access-group 1 in**

표준 ACL(Access Control List)

- ACL을 이용한 원격 접속 제어

- 원격접속 방법 : 텔넷, SSH(Secure Shell), http, https

PC0에서 R2에 텔넷 접속 설정 /* PC0 GW설정, R1 초기화 재설정*/

1. **R2(config)#access-list 1 permit host 1.1.1.2**
2. **R2(config)#line vty 0 4**
3. **R2(config-line)#password cisco**
4. **R2(config-line)#login**
5. **R2(config-line)#access-class 1 in /*1번 들어오는(in)트래픽적용 */**
6. **R2(config-line)#do show run**

확장 ACL(Access Control List)

- PC0에서 R2에 텔넷 접속 허락,Ping 거부 할 경우 -> 확장 ACL
- 출발지와 목적지 주소 및 프로토콜 제어

조건 : PC0에 R3 접속시(ping 거부, 나머지 허락)

1. R1(config)#access-list 100 deny icmp host 1.1.1.2 host 203.230.7.9 echo /*100(확장 ACL번호), icmp(제어코자하는 프로토콜)
2. R1(config)#access-list 100 deny icmp host 1.1.1.2 host 203.230.7.6 echo
3. R1(config)#access-list 100 deny icmp host 1.1.1.2 host 3.3.3.1 echo
4. R1(config)#access-list 100 permit ip any any
5. R1(config)#int g0/0
6. R1(config-if)#ip access-group 100 in
7. R1(config-if)#do show run

또는

1. R3(config)#access-list 100 deny icmp host 1.1.1.2 host 203.230.7.9 echo
2. R3(config)#access-list 100 deny icmp host 1.1.1.2 host 203.230.7.6 echo
3. R3(config)#access-list 100 deny icmp host 1.1.1.2 host 3.3.3.1 echo
4. R3(config)#access-list 100 permit ip any any
5. R3(config)#int S0/2/0
6. R3(config-if)#ip access-group 100 in
7. R3(config)#int S0/2/1
8. R3(config-if)#ip access-group 100 in

확장 ACL(Access Control List)

- **PC0에서 ping 203.230.7.9 테스트 (거부)**
- **PC0에서 ping 203.230.7.6 테스트 (거부)**
- **PC0에서 ping 3.3.3.1 테스트 (거부)**
- **PC0에서 telnet 3.3.3.1 테스트**

확장 ACL(Access Control List)

조건 : PC1에 R2 접속시 (telnet 거부)

1. R1(config)#access-list 100 deny tcp host 1.1.1.3 host 203.230.7.2 eq telnet
2. R1(config)#access-list 100 deny tcp host 1.1.1.3 host 203.230.7.5 eq telnet
3. R1(config)#access-list 100 deny tcp host 1.1.1.3 host 2.2.2.1 eq telnet
4. R1(config)#access-list 100 permit ip any any
5. R1(config)#int g0/0
6. R1(config-if)#ip access-group 100 in
7. R1(config-if)#do show run

Named 표준 ACL(Access Control List)

- 표준 ACL + 번호 대신 문자 정의하여 사용

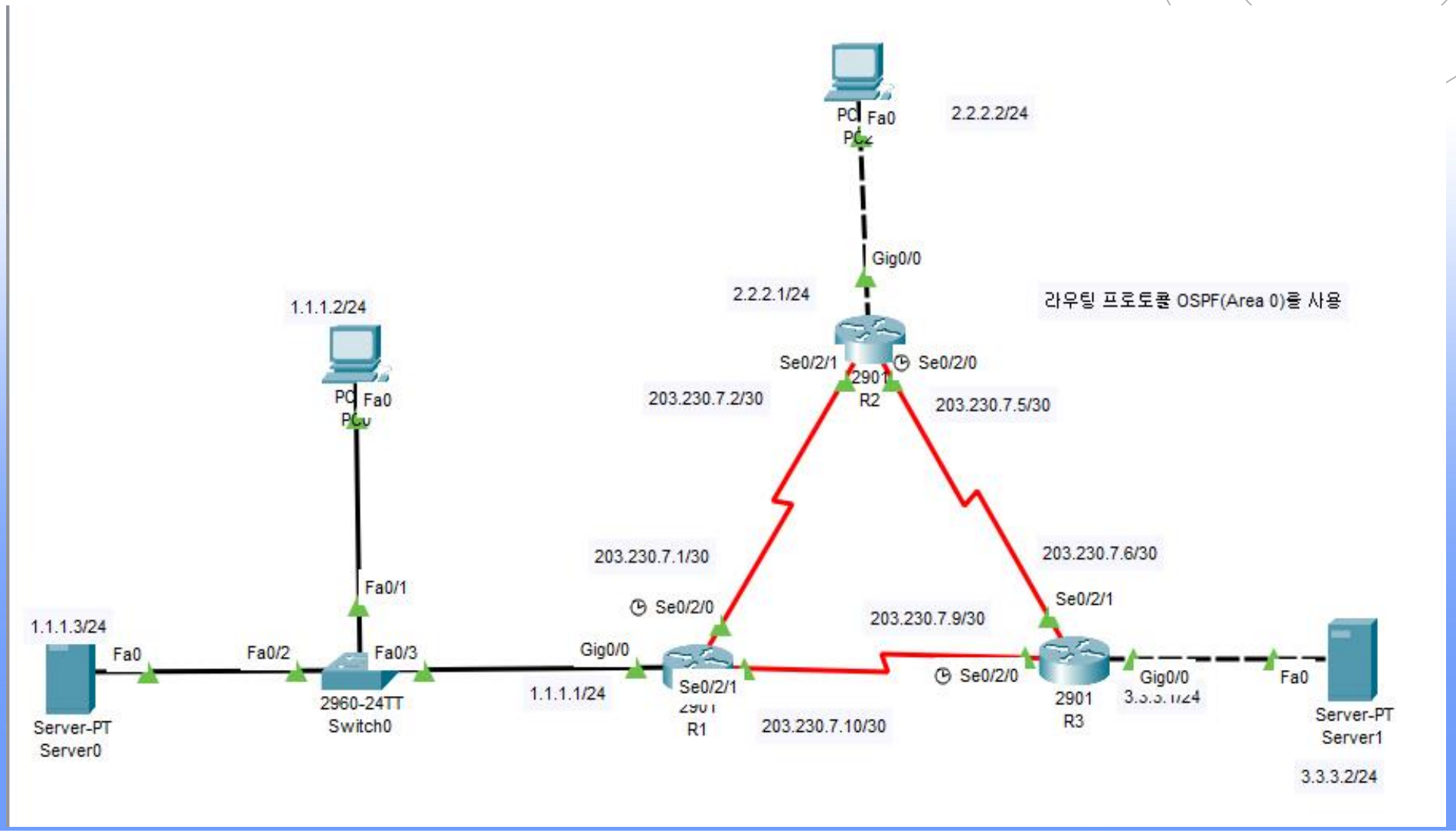
1. R1(config)#ip access-list standard infocomm /* ip access-list(named 확장ACL 경우 사용), standard(named표준ACL경우),extended(named확장ACL 경우)
2. R1(config-std-nacl)#permit host 1.1.1.3
3. R1(config-std-nacl)#deny any
4. R1(config-std-nacl)#exit
5. R1(config)#int g0/0
6. R1(config-if)#ip access-group infocomm in
7. R1(config-if)#do show run

Named 확장 ACL(Access Control List)

조건 : PC0에 R3 접속시(ping 거부, 나머지 허락)

1. R1(config)#ip access-list extended ping
2. R1(config-ext-nacl)#deny icmp host 1.1.1.2 host 3.3.3.1
3. R1(config-ext-nacl)#deny icmp host 1.1.1.2 host 203.230.7.6
4. R1(config-ext-nacl)#deny icmp host 1.1.1.2 host 203.230.7.9
5. R1(config-ext-nacl)#permit ip any any
6. R1(config-ext-nacl)#remark PC0 ping deny(R3)
7. R1(config-ext-nacl)#exit
8. R1(config)#do show access-list
9. R1(config)#int g0/0
10. R1(config-if)#ip access-group ping in
11. R1(config-if)#do show run

Named 확장 ACL(Access Control List)



Named 확장 ACL(Access Control List)

R1 설정 스크립트

1. Router#conf t
2. Router(config)#hostname R1
3. R1(config)#int g0/0
4. R1(config-if)#ip add 1.1.1.1 255.255.255.0
5. R1(config-if)#no shut
6. R1(config)#int S0/2/0
7. R1(config-if)#ip add 203.230.7.1 255.255.255.252
8. R1(config-if)#clock rate 64000
9. R1(config-if)#no shut
10. R1(config)#int S0/2/1
11. R1(config-if)#ip add 203.230.7.10 255.255.255.252
12. R1(config-if)#no shut
13. R1(config-if)#exit
14. R1(config)#router ospf 1
15. R1(config-router)#network 1.1.1.1 0.0.0.0 area 0
16. R1(config-router)#network 203.230.7.1 0.0.0.0 area 0
17. R1(config-router)#network 203.230.7.10 0.0.0.0 area 0
18. R1(config-router)#do show ip int brief

Named 확장 ACL(Access Control List)

R2 설정 스크립트

1. Router#conf t
2. Router(config)#hostname R2
3. R2(config)#int g0/0
4. R2(config-if)#ip add 2.2.2.1 255.255.255.0
5. R2(config-if)#no shut
6. R2(config)#int S0/2/0
7. R2(config-if)#ip add 203.230.7.5 255.255.255.252
8. R2(config-if)#clock rate 64000
9. R2(config-if)#no shut
10. R2(config)#int S0/2/1
11. R2(config-if)#ip add 203.230.7.2 255.255.255.252
12. R2(config-if)#no shut
13. R2(config-if)#exit
14. R2(config)#router ospf 1
15. R2(config-router)#network 2.2.2.1 0.0.0.0 area 0
16. R2(config-router)#network 203.230.7.5 0.0.0.0 area 0
17. R2(config-router)#network 203.230.7.2 0.0.0.0 area 0
18. R2(config-router)#do show ip int brief

Named 확장 ACL(Access Control List)

R3 설정 스크립트

1. Router#conf t
2. Router(config)#hostname R3
3. R3(config)#int g0/0
4. R3(config-if)#ip add 3.3.3.1 255.255.255.0
5. R3(config-if)#no shut
6. R3(config)#int S0/2/0
7. R3(config-if)#ip add 203.230.7.9 255.255.255.252
8. R3(config-if)#clock rate 64000
9. R3(config-if)#no shut
10. R3(config)#int S0/2/1
11. R3(config-if)#ip add 203.230.7.6 255.255.255.252
12. R3(config-if)#no shut
13. R3(config-if)#exit
14. R3(config)#router ospf 1
15. R3(config-router)#network 3.3.3.1 0.0.0.0 area 0
16. R3(config-router)#network 203.230.7.9 0.0.0.0 area 0
17. R3(config-router)#network 203.230.7.6 0.0.0.0 area 0
18. R3(config-router)#do show ip int brief

Named 확장 ACL(Access Control List)

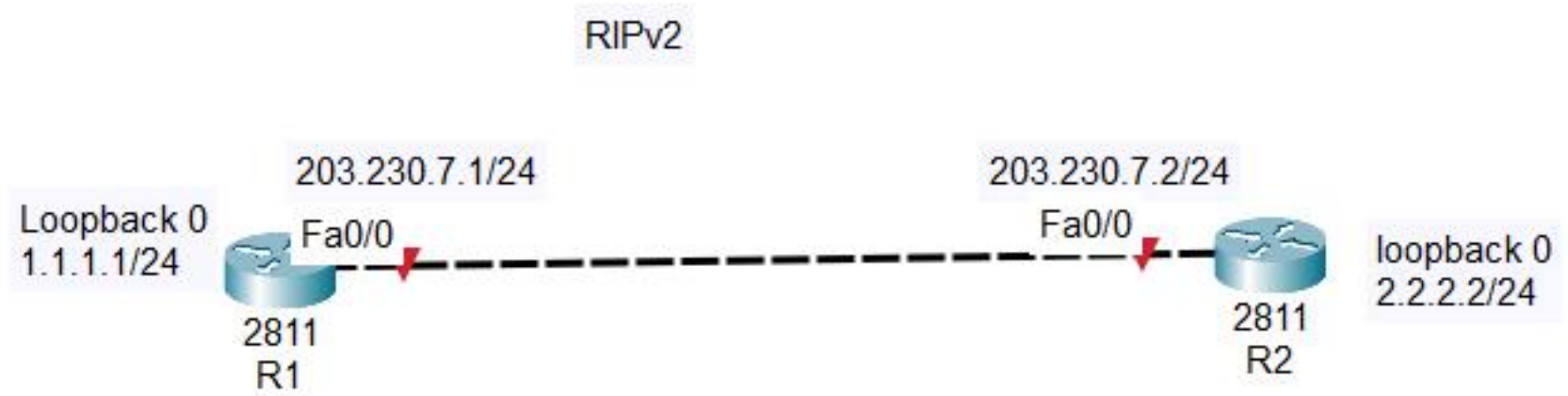
PC2(2.2.2.2)에서 www, ftp 테스트
http://1.1.1.3, C:\ftp 1.1.1.3

1. **R2(config)#access-list 100 deny tcp host 2.2.2.2 host 1.1.1.3 eq www**
2. **R2(config)#access-list 100 deny tcp host 2.2.2.2 host 1.1.1.3 eq ftp**
3. **R2(config)#access-list 100 deny tcp host 2.2.2.2 host 1.1.1.3 eq 20**
4. **R2(config)#access-list 100 permit ip any any**
5. **R2(config)#int S0/2/0**
6. **R2(config-if)#ip access-group 100 in**

또는

1. **R2(config)#ip access-list extended http_ftp**
2. **R2(config-ext-nac)#deny tcp host 2.2.2.2 host 1.1.1.3 eq www**
3. **R2(config-ext-nac)#deny tcp host 2.2.2.2 host 1.1.1.3 eq ftp**
4. **R2(config-ext-nac)#deny tcp host 2.2.2.2 host 1.1.1.3 eq 20**
5. **R2(config-ext-nac)#permit ip any any**
6. **R2(config-ext-nac)#int gi0/0**
7. **R2(config-if)#ip access-group http_ftp in**

TCP Established



TCP Established

R1 설정 스크립트

1. **Router#conf t**
2. **Router(config)#hostname R1**
3. **R1(config)#int g0/0**
4. **R1(config-if)#ip add 203.230.7.1 255.255.255.0**
5. **R1(config-if)#no shut**
6. **R1(config)#int lo 0**
7. **R1(config-if)#ip add 1.1.1.1 255.255.255.0**
8. **R1(config)#router rip**
9. **R1(config-router)#version 2**
10. **R1(config-router)#network 203.230.7.1**
11. **R1(config-router)#network 1.1.1.1**

TCP Established

R2 설정 스크립트

1. Router#conf t
2. Router(config)#hostname R2
3. R2(config)#int g0/0
4. R2(config-if)#ip add 203.230.7.2 255.255.255.0
5. R2(config-if)#no shut
6. R2(config)#int lo 0
7. R2(config-if)#ip add 2.2.2.2 255.255.255.0
8. R2(config)#router rip
9. R2(config-router)#version 2
10. R2(config-router)#network 203.230.7.2
11. R2(config-router)#network 2.2.2.2

TCP Established

1. R1(config)#access-list 100 permit tcp any 1.0.0.1 0.255.255.255 established
2. R1(config)#access-list 100 deny ip any any
3. R1(config)#int F0/0
4. R1(config-if)#ip access-group 100 in
5. R1(config-if)#do show run

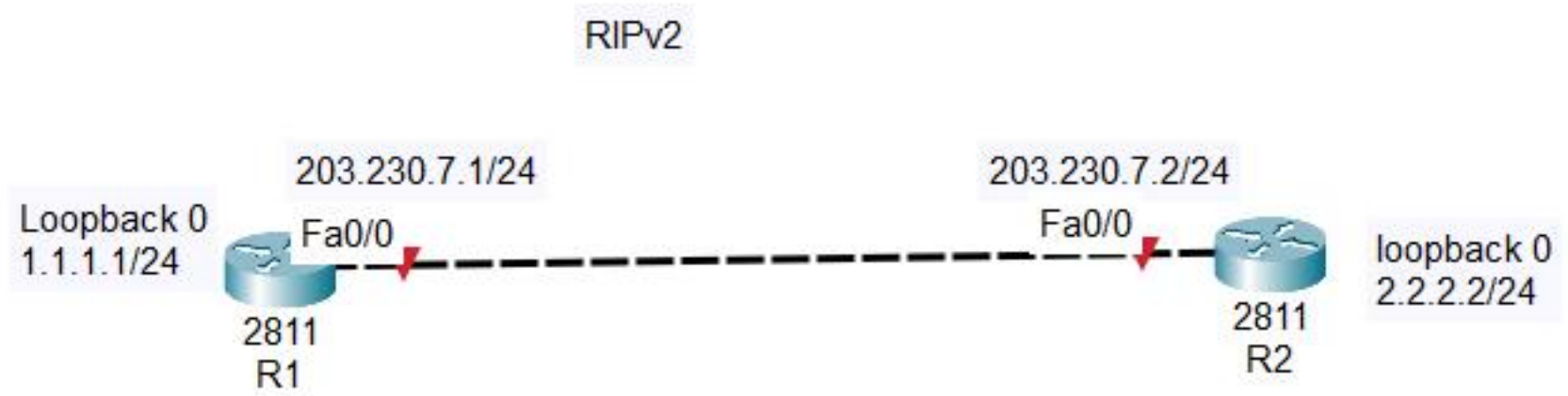
ACL 중간 삽입

ACL을 작성후 10번과 20번 사이에 ACL 삽입 경우

1. **R2(config)#ip access-list extended inokyuni**
2. **R2(config-ext-nacl)#permit tcp any host 1.1.1.1**
3. **R2(config-ext-nacl)#deny ip any any**
4. **R2(config-ext-nacl)#exit**
5. **R2(config)#show access-list**
6. **R2(config)#ip access-list extended inokyuni**
7. **R2(config-ext-nacl)#15 permit tcp any host 203.230.7.1**
8. **R2(config-ext-nacl)#do show access-list /* 15.. 중간 삽입 */**

락-앤-키(Lock-and-Key) 인증

Telnet으로 라우터에 접속시 : 아이디와 패스워드 인증하는 방법
- 작동 안됨 : **dynamic** 오류



락-앤-키(Lock-and-Key) 인증

R1 설정 스크립트

1. **Router#conf t**
2. **Router(config)#hostname R1**
3. **R1(config)#int g0/0**
4. **R1(config-if)#ip add 203.230.7.1 255.255.255.0**
5. **R1(config-if)#no shut**
6. **R1(config)#int lo 0**
7. **R1(config-if)#ip add 1.1.1.1 255.255.255.0**
8. **R1(config)#router rip**
9. **R1(config-router)#version 2**
10. **R1(config-router)#network 203.230.7.1**
11. **R1(config-router)#network 1.1.1.1**
12. **R1(config-router)#line vty 0 4**
13. **R1(config-line)#password 1234**

락-앤-키(Lock-and-Key) 인증

R2 설정 스크립트

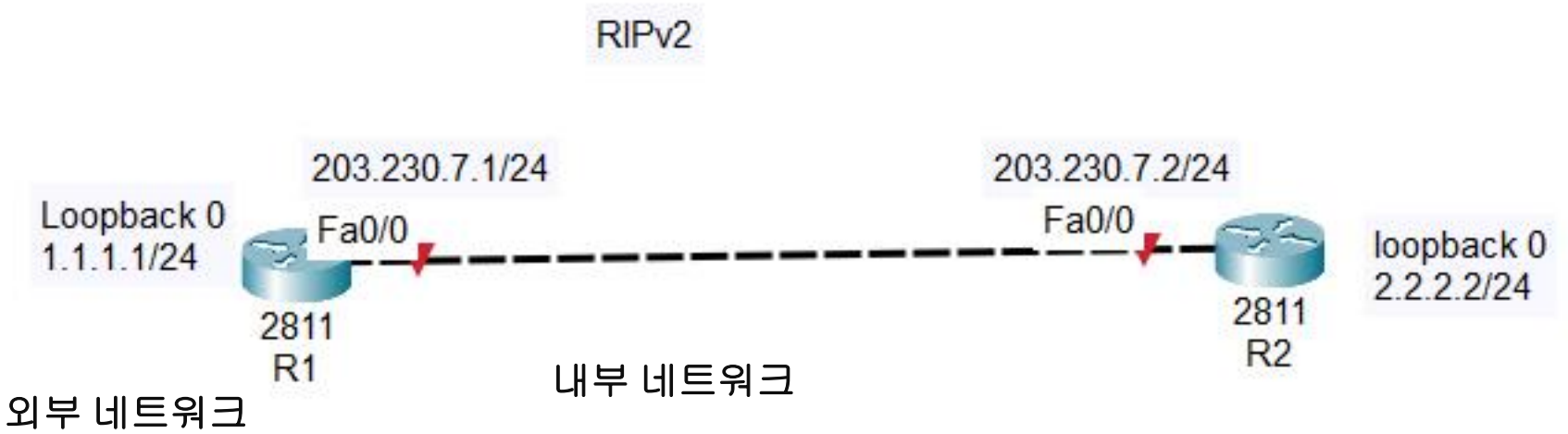
1. **Router#conf t**
2. **Router(config)#hostname R2**
3. **R2(config)#int g0/0**
4. **R2(config-if)#ip add 203.230.7.2 255.255.255.0**
5. **R2(config-if)#no shut**
6. **R2(config)#int lo 0**
7. **R2(config-if)#ip add 2.2.2.2 255.255.255.0**
8. **R2(config)#router rip**
9. **R2(config-router)#version 2**
10. **R2(config-router)#network 203.230.7.2**
11. **R2(config-router)#network 2.2.2.2**
12. **R2(config-router)#line vty 0 4**
13. **R2(config-line)#password 1234**

락-앤-키(Lock-and-Key) 인증

1. R1(config)#username inokyuni password infocomm /* 텔넷 접속시 인증시 아이디와 암호 생성 */
2. R1(config)#ip access-list extended LK /*락앤키 적용될 ACL
3. R1(config-ext-nacl)#permit tcp any host 203.230.7.1 eq telnet /* 텔넷 접속 가능한 주소설정 */
4. R1(config-ext-nacl)#dynamic LK_test permit ip any any(기능없음)
5. R1(config-ext-nacl)#deny ip any any
6. R1(config-ext-nacl)#exit
7. R1(config)#show access-list
8. R1(config)#int F0/0
9. R1(config-if)#ip access-group LK in
10. R1(config-if)#line vty 0 4
11. R1(config-line)#login local
12. R1(config-line)#autocommand access-enable host timeout 1
13. R1(config-line)#exit
14. R1(config)#show access-list

RACL(Reflexive ACL)

내부에서 외부로 통신가능, 외부에서 내부로 통신 불가 설정
패킷 트래이셔는 작동 불가



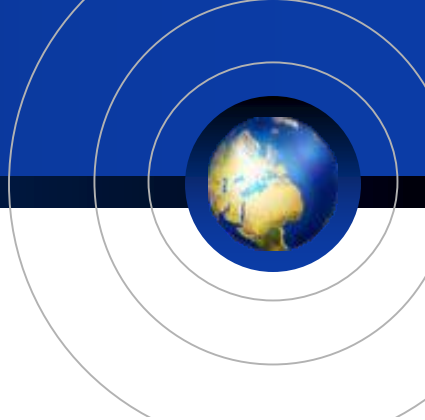
RACL(Reflexive ACL)

1. R2(config)#ip access-list extended in_in
2. R2(config-ext-nacl)#permit tcp any any reflect tcp
3. R2(config-ext-nacl)#permit udp any any reflect udp
4. R2(config-ext-nacl)#deny ip any any
5. R2(config-ext-nacl)#exit
6. R2(config)#show access-list
7. R2(config)#ip access-list extended out_out
8. R2(config-ext-nacl)#evaluate tcp (기능 없음)
9. R2(config-ext-nacl)#evaluate udp
10. R2(config-ext-nacl)#deny ip any any
11. R2(config-ext-nacl)#exit
12. R2(config)#int F0/0
13. R2(config-if)#ip access-group in_in in
14. R2(config-if)#ip access-group out_out out
15. R2(config-if)#exit
16. R2(config)#show access-list

시간 기반의(time-based) ACL

특정 시간에만 동작 할수 있도록 설정
월~금요일 오전8시부터 ~ 오후 6시간 사용 설정

1. R1(config)#time-range weekday
2. R1(config-time-range)#periodic ?
3. R1(config-time-range)#periodic weekdays 8:00 to 18:00
4. R1(config-time-range)#exit
5. R1(config)#access-list 100 permit ip any any time-range weekday
6. R1(config)#access-list 100 deny ip any any time-range weekday
7. R1(config)#show access-list
8. R1(config)#ip f0/0
9. R1(config-if)#ip access
10. R1(config-if)#ip access-group 100 in



Q & A

감 사 합 니 다`