# 확장 ACL

표준 ACL은 단순히 출발지 주소만을 가지고 패킷을 전달할 것인지 전달하지 않을 것인지 결정한다

예를 들어 PC0가 R2에 텔넷 접속을 허락하지만 Ping은 보낼 수 없도록 설정하고자 할 때 표준 ACL은 이 조건을 만족 시킬 수 없다

만약 표준 ACL을 사용하여 ping을 막았다면 다른 모든 서비스도 다 막혔을 것이다

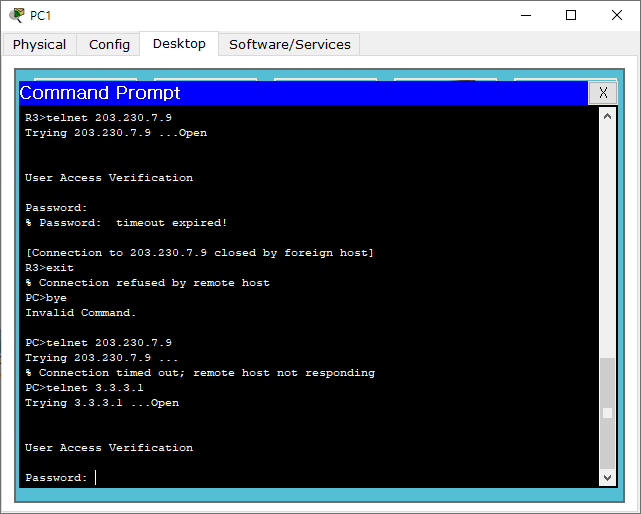
이러한 단점을 보완하고자 확장 ACL을 사용하는데 확장 ACL은 출발지 주소뿐만이 아니라 목적지 주소 및 프로토콜까지 제어할 수 있기 때문에 표준 ACL보다 훨씬 넓은 범위의 제어 기능을 제공한다

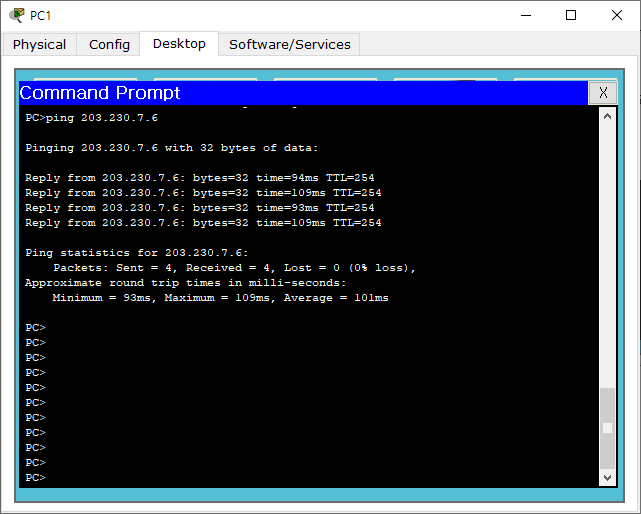
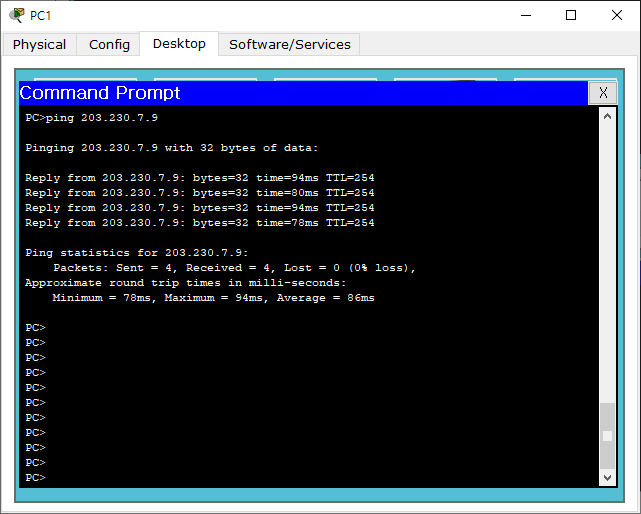
그럼 네트워크 토폴로지에서 PC0는 R3에만 ping을 보낼 수 없도록 설정해 보자

ping을 제외한 다른 모든 서비스는 사용 가능하여야 하므로 텔넷 접속 시 반드시 접속이 되어야 한다 ACL은 R1에 다음과 같이 설정한다.

(CPT\_실습과제18\_1\_1EACLLIST실습\_2020.03.30\_이인환.pkt 참조)

♣ R1 라우터에 ACL 설정 전 통신



♣R1 라우터에 ACL 설정

R1(config)#access-list 100 deny icmp(차단할프로토콜) host 1.1.1.2 host 203.230.7.9 echo(차단할 실제프로토콜)

R1(config)#access-list 100 deny icmp(차단할프로토콜) host 1.1.1.2 host 203.230.7.6 echo(차단할 실제프로토콜)

R1(config)#access-list 100 deny icmp(차단할프로토콜) host 1.1.1.2 host 3.3.3.1 echo(차단할 실제프로토콜)

R1(config)#access-list 100 permit ip any any

R1(config)interface fastethernet 0/0

R1(config-if)ip access-group 100 in

♣사용된 확장 ACL 구문의 각 구성요소는 다음과 같은 의미를 가진다

♧ Access-list 100 : 확장 ACL이므로 번호는 100-199번 ,2000-2699사이의 번호를 사용한다

♧ Deny : 조건에 맞는 트래픽을 전달할(permit) 것인지 버림(deny)것인지 결정한다

♧ Icmp : 확장 ACL을 통해 제어하고자 하는 프로토콜의 이름을 입력한다

♧ Host 1.1.1.2: 관찰 대상의 출발지 주소를 적는다

♧ Host 203.230.7.9 : 관찰 대상의 목적지 주소를 적는다

♧ Echo : 옵션 항목으로 프로토콜을 선택 할 수 있다

♧ access-list 100 permit any : ACL이 deny 구문으로 이루어져 있을 경우에는 deny 된 트래픽을 제외한 다른 모든 트래픽을 전달시키겠다는 의미로 반드시 작성하여야 한다

♧ IP access-group 100 in : 위에서 작성한 ACL 100번을 적용하는데 들어오는 트래픽에 적용할 것인지 아니면 나가는 트래픽(out)에 적용 할 것인지 선언한다

♣R1 라우터에 ACL 설정 후 통신테스트

