네트워크 보안

* 표준액세스 리스트
* 확장 액세스 리스트
* Vpn과 NAT
* 액세스 리스트
  + 라우터에서 특정한 패킷을 차단 또는 허용
  + 출발지 IP 주소 == 표준 액세스
  + 출발지 /목적지 IP, 프로토콜번호, 전송계층 포트번호를 사용하는 확장 액세스 리스트
* 상황에 따라 다른 HDLC 통신 상태
  + 방화벽 (asa, pix, 라우터)
  + VPN 게이트웨이, 공중망을 사설망처럼 (라우터, asa pix)
  + 침입방지 시스템(IPS) : 가변적 공격 트래픽 차단.
* 표준 액세스 리스트
  + Access list 번호 허가된 번호list
  + Permit
  + Deny
  + Source 네트워크
  + Source 네트워크 wild mask
  + Log 로 구성
* 표준 IP 액세스 리스트
  + 프로토콜당, 인터페이스당, 방향당 하나씩
  + 라우터와 인터페이스, 방향을 미리 결정
  + 외부 넽웤 연결되는 라우터
    - 경계라우터
    - 경계 라우터의 외부 인터페이스에서 내부로 들어오는 패킷 제어
  + 액세스 리스트 만드는 법
    - 액세스 리스트 번호 선택 (원하는 것)
    - 명령 선택 (permit, deny, remark)
    - 출발지, wild mask 지정
    - 앞서 지정되지 않은 패킷들은 모두 차단
    - 리스트를 적용할 인터페이스 설정
    - List active 명령어 입력
    - R2에서 차단 => 액세스 리스트에 의해서 패킷 차단 ICMP 메시지 ( ‘U’ )
    - ICMP 를 번갈아서 보냄
    - Show ip access list 명령어로 R2에서 액세스 리스트가 동작하는지 확인
* R3의 라우터가 내부망에서
  + 1.1.30.0/24 내부 망을 가질 때 내부망 내부 통신을 어떻게 할까?

=> 넷웤 호스트 부분 파악

* + 24는 subnet 마스크 : subnet mask는 wild 마스크와 달리 연속된 1로 표현함
  + 와일드 마스크
    - 기준이 되는 주소와 일치해야 하는 비트 0
    - 아닌 경우는 1
    - 1.1.30.0 ~ 1.1.30.255 : 1.1.30.0/24 로 표시
      * + Wild mask 에선 1.1.30.0.0.0.0.255
    - 범위가 좁은 문장을 먼저 지정해야함.
      * 1.1.3.0/24 IP 차단, 1.1.0.0/16 허용 순서로 기술
      * 1.1.3.0/24 가 더 좁은 범위라서 해당 범위에 IP가 소속되어 있으면   
        이후 문장 확인 x
      * 액세스 리스트 라우팅테이블 적용 순서
        + 입력 액세스 리스트 적용(수신)
        + 라우팅 테이블 확인
        + 출력 액세스 리스트 확인(송신)
    - 액세스 리스트 문장 삭제
      * No access-list 1 deny 1.1.3.0 0.0.0.255 는 access list 1 번을 삭제하는 명령
* 확장 액세스 리스트
  + 더 넓은 범위를 제어
  + 출발지 IP ,목적지 IP, 출발지 포트 번호, 목적지 포트번호
  + AWS 에서 이거 쓰는 거 같음
  + R3 L3 나오는데 R3는 그냥 라우터 객체 말하는 거고 L3,L4 이거는 역할이 다름
  + L4헤더는 포트번호까지 보나보다 ? L3스위치는 IP 까지만?
  + 적용하려는 인터페이스의 설정모드 들어가서 ip access -group 명령어 다음  
    액세스 리스트 번호와 방향 지정
  + 이름을 사용한 액세스리스트를 사용할 수 있음. 번호대신 이름 사용
    - 의미있는 적절한 이름을 사용하면 장애처리에도 편함.
    - 별도의 액세스 리스트 설정 명령어를 표현

VPN 과 NAT

* 공중망을 사설망처럼 사용하는 것
* 기밀성 유지: 암호화 C
* 무결성 I
* 인증 상대방이 맞는지 A uthor~
* 재생방지: 순서번호 매김
* CIA기능
  + VPN 제외 네트워크는 A를 가용성으로 할 수 있음
* IPSec VPN
  + IETF 에서 권고하는 IPSec 기술 준수하여 만든 VPN
  + VPN LAN안에서 평문
  + 밖으로 나가는 router에서 암호화
  + 방식에는 AH(인증), ESP (암호와 재생 방지)
  + 라우터가 복호화도 해줌 (DES, AES,3DES 등의 알고리즘 사용).
* SSL VPN
  + 넷스케이프사에서 1.0 2.0 발표
  + 전송계층을 포함하여 그 상위계층에 도착
  + 전자상거래 등 비롯한 인터넷 통신에 사용
  + HTTPS: SSL 사용 Port 443
  + PC 와 VPN 게이트웨이 (Router) 사이에서 작동
  + 인증에는 RSA,DSS
  + 암호화 DES
  + 무결성에는 SHA-1 등의 알고리즘 사용
* NAT
  + IP 주소를 다른 것으로 변환
  + 사설 IP 주소를 인터넷으로 라우팅 시킬 때
  + 인터넷에서 수신한 공인 IP 주소를 내부망으로 전송할당
    - 사설 주소는 IANA 에서 할당 x
    - 보통 10.0.0.0/9 172.16.0.0/12 192.168.0.0/16 사용
  + 공인 IP 주소 절약
  + 네트워크 보안
    - 내부 IP 주소를 외부에서 알 수 없음
  + 효과적인 주소 할당
    - 효율적 네트워크 할당 가능, 효과적 축약으로 routing table 부하 줄이기 가능
  + 대신 특정한 IP를 대상으로 서비스 할 수 있는 Application에는 제약이 따른다.
* 정적 NAT, 동적 NAT
  + 정적 NAT
    - 변환되는 두 IP 주소가 미리 지정
    - 외부에서 사설 IP 주소를 가진 내부장비 접속이 필요한 경우
  + 동적 NAT
    - 사설 IP 주소와 변환되는 공인 IP 주소가 사전에 지정 X
    - 통신이 시작할 때 정해지는 것

문제 C 클래스 IP 주소 전체를 표현 와일드 카드 마스크

192.0.0.0 31.255.255.255

C클래스는 110network ~ .host(8bit) 라서

192.0.0.0~223.255.255.255 까지 가능

그러므로 해당 주소와 일치해야하는 부분은 앞에 31만큼의 0이 일치해야함. ㅇㅇ 뒷부터

1\*5개는 자유임

(0 이 일치 1이 비일치해도됨 임.)

참고로 subnet /24 는 앞에서부터 1 개수고 해당 숫자만큼 network 주소라고 생각하면 됨.