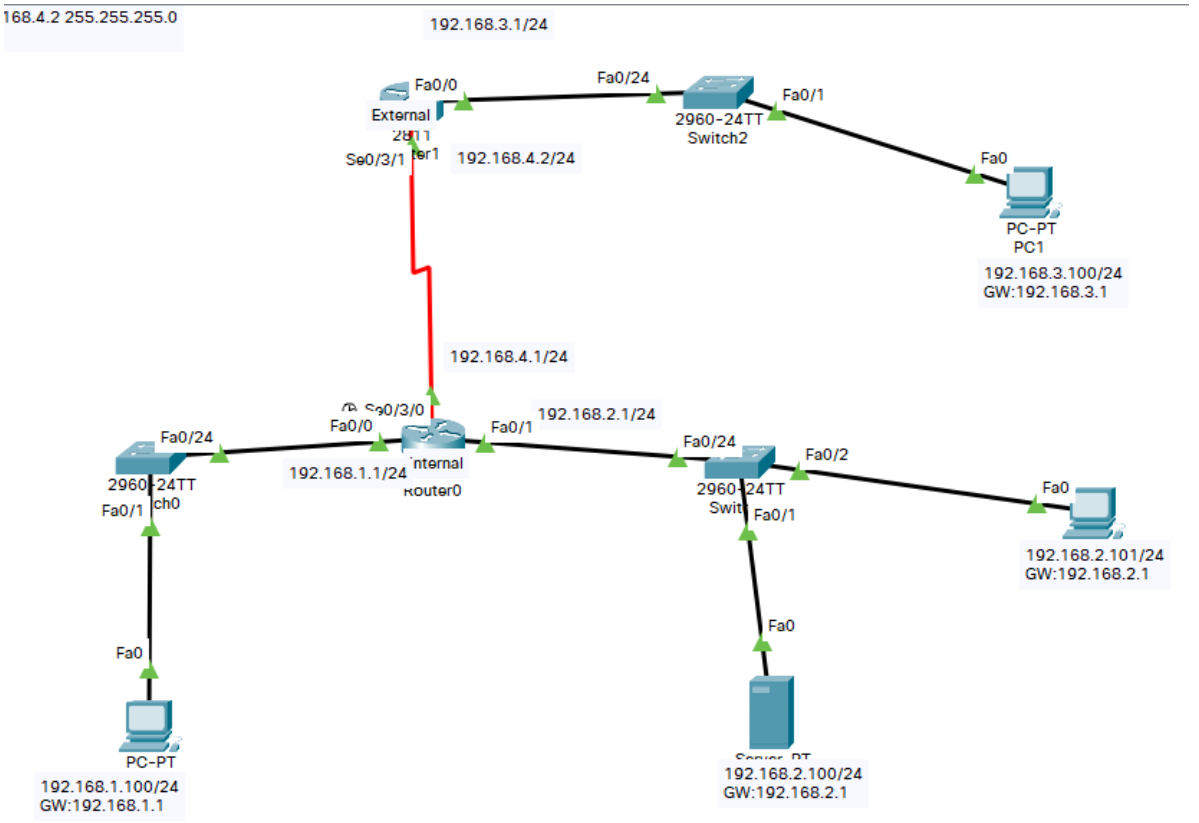
CCNA_210805

ACL



Router(config)# access-list 1 permit 192.168.1.128 0.0.0.127

--> 192.168.1.128 255.255.255.128

--> 192.168.1.128 /25

192.168. 1.1000 0000

255.255.255.1000 0000 (AND연산)

192.168.1.128

= 192.168.1.128 ~ 192.168.1.255 (범위계산)

-> 192.168.1.129 ~ 192.168.1.254

>> 라우터가 수신한 패킷의 출발지 주소가 192.168.1.129 ~ 192.168.1.254에 속하면 해당 패킷은 허용(permit)한다.

ex) 출발지 네트워크가 10.0.0.0/24인 패킷에 대해서 거부하는 표준 ACL 정의 구문은?

access-list 1 deny 10.0.0.0 0.0.0.255

Router(config)# access-list 1 deny 192.168.1.100 0.0.0.0 (어드레스에 인터페이스주소, 와일드카드에 0.0.0.0)

>>단일 호스트에 대해 거부나 허용을 정의할때 와일드카드 마스크에 0.0.0.0을 사용.

>>수신 패킷의 출발지 주소가 192.168.1.100이면 해당 패킷은 거부함.

>>192.168.1.100 0.0.0.0 = host 192.168.1.100 (권장) 자동으로 변환되어 저장됨.

Router(config)# access-list 1 deny 0.0.0.0 255.255.255.255

>>0.0.0.0 255.255.255.255의 의미는 모든 출발지 네트워크를 의미.

>>0.0.0.0 255.255.255.255 = any

>>모든 출발지 네트워크에서 발생하는 패킷은 거부함의 의미.

ex) Standard ACL 예제

Router(config)# access-list 1 permit 192.168.1.0 0.0.0.255
Router(config)# access-list 1 permit 192.168.2.0 0.0.0.255
Router(config)# access-list 1 permit 192.168.3.0 0.0.0.255

* Standard ACL 설정 (Internal Router에서 설정)

[실습1] 192.168.1.0/24, 192.168.2.0/24, 192.168.3.0/24

요구사항 : 192.168.1.0/24 네트워크와 192.168.2.0/24 네트워크 에서만 패킷전송이 가능하도록 설정

[실습2] 192.168.1.0/24, 192.168.2.0/24 서로간의 통신.

요구사항: 192.168.2.0/24 네트워크에서 호스트 192.168.2.101은 192.168.1.0/24와 통신이 되지않도록 설정.

*Extended ACL (확장 ACL) : source / destination ip, protocol
source/ destination port

Router(config)# access-list list_number [permit|deny] protocol_name
source_address wildcard_mask { operator {eq|neq|lt|gt}
source_port_number

--> list_number : 100 ~ 199
protocol_name : ip, tcp, udp, icmp, gre 등
operator : 연산자, eq, neq, lt, gt (가장 많이 사용하는 연산자는 eq)
(eqaul, not equal, less than, greater than의 약자들)

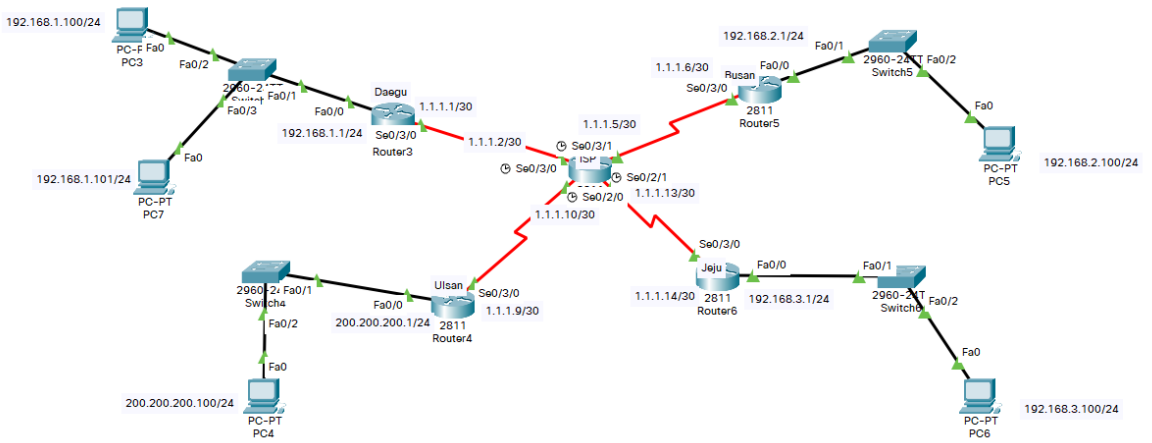
[실습1] 192.168.1.0/24, 192.168.2.0/24, 192.168.3.0/24

요구사항 : 192.168.1.0/24 -> 192.168.2.100 : 웹트래픽만 허용(나머지 유형의 서비스는 거부)
192.168.3.0/24 -> 192.168.2.100 : 웹트래픽만 거부(나머지 유형의 서비스는 허용)

서브넷팅
/24 = 255.255.255.0 -> 1111 1111. 1111 1111. 1111 1111. 0000 0000
/25 = 255.255.255.0 -> 1111 1111. 1111 1111. 1111 1111. 1000 0000 = 255.255.255.128

128

/26 = 1111 1111. 1111 1111. 1111 1111. 1100 0000 = 255.255.255.192
/27 = 1111 1111. 1111 1111. 1111 1111. 1110 0000 = 255.255.255.224
/28 = 1111 1111. 1111 1111. 1111 1111. 1111 0000 = 255.255.255.240
/29 = 1111 1111. 1111 1111. 1111 1111. 1111 1000 = 255.255.255.248
/30 = 1111 1111. 1111 1111. 1111 1111. 1111 1100 = 255.255.255.252



*NAT (Network Address Translation) 주소변환기술

inside local address : 내부에서 사용하는 사설 IP주소
inside global address : 외부로 나갈때 변환되는 공인 IP주소

outside local address : 외부에 존재하는 네트워크에서 사용하는 사설 IP 주소
outside global address : 외부에 존재하는 네트워크에서 사용하는 공인 IP 주소

NAT 종류 (매핑 방식에 따라 구분)

1)Static NAT : 1: 1

하나의 사설 IP주소를 하나의 공인 IP주소로 매핑

2)Dynamic NAT : 1: 1

매핑 작업을 누가하느냐에 따라 구분을 하는데, Dynamic NAT는 라우터에 의해 매핑 작업이 이루어진다. 하지만 매핑에 필요한 정보는 관리자가 설정해야함.

3)PAT(Port Address Translation) : 다 대 1

NAT overload

다수의 사설 IP주소에 대해서 하나의 공인 IP 주소로 매핑 하는 기술.

>> Static NAT (매핑 : 관리자가 함)

Step 1. 매핑(정의)

Router(config)# ip nat inside source static local_address global_address

ex) Router(config)#ip nat inside source static 192.168.1.100 100.100.100.100

Step 2.적용(인터페이스)

Step 2-1) 내부 인터페이스 (사설 Ip주소가 설정이 된 인터페이스)

Router(config)# interface int_type slot#/port#

Router(config-if)# ip nat inside

Step 2-2) 외부 인터페이스 (공인 Ip주소가 설정이 된 인터페이스, 외부와 연결된 인터페이스)