[네트워크 팀 프로젝트]

방화벽

3조 Shell work

김진호
김현욱
임원택
정혁준

목차

1 구성도

- 물리적 구성도
- 논리적 구성도

2 스위치 설정

- SW1
- SW2
- SW3
- SW4

3 라우터 설정

- R1
- R2
- R3
- R4
- R5
- R6

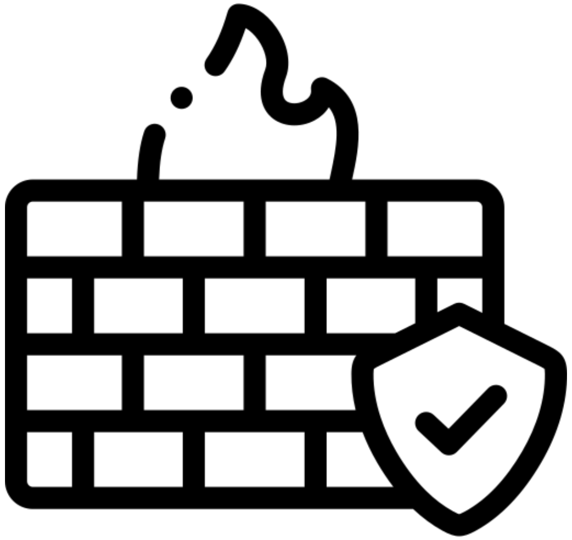
4 방화벽 - 1 설정

- FW1

5 방화벽 - 2 설정

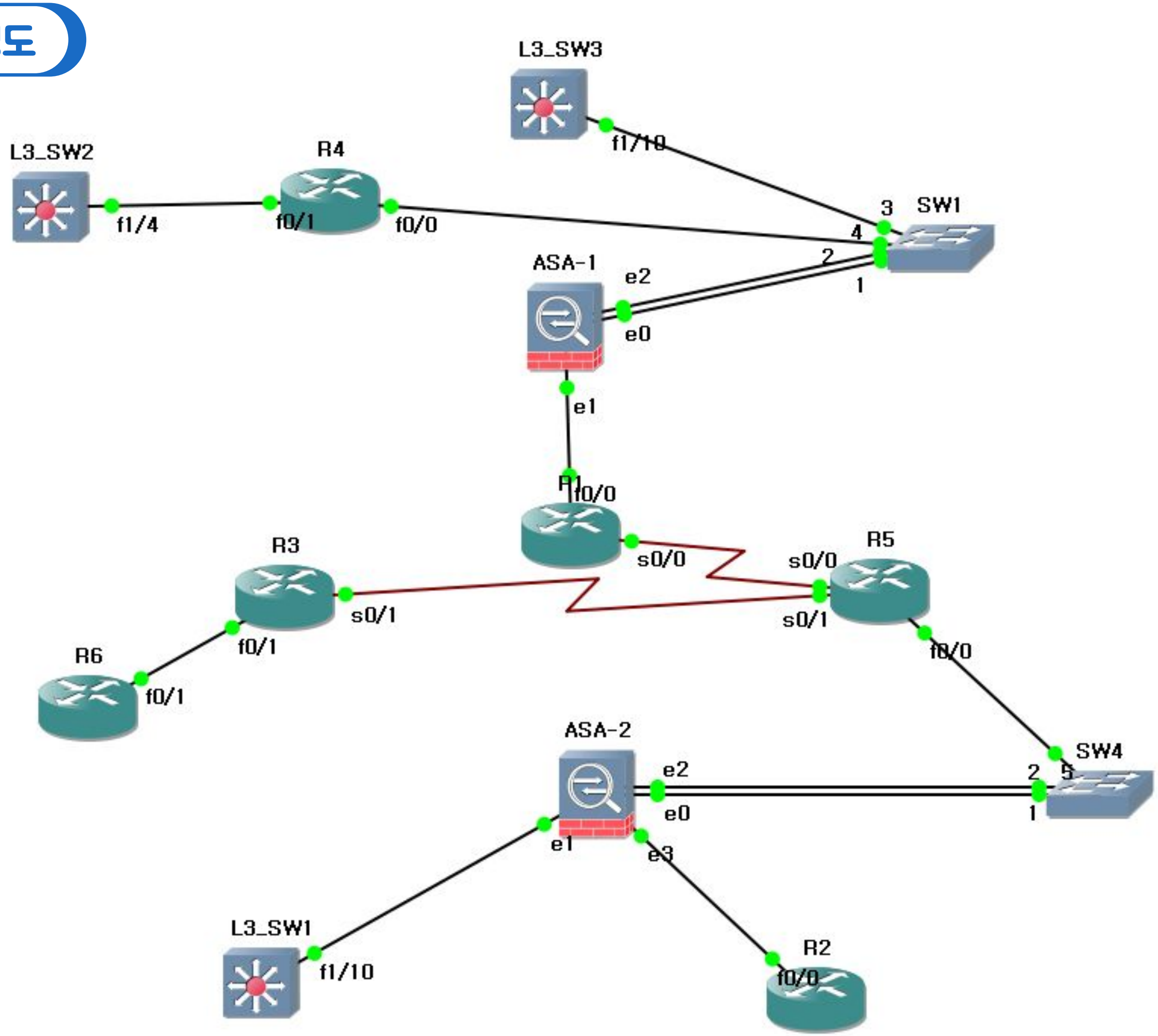
- FW2

구성도



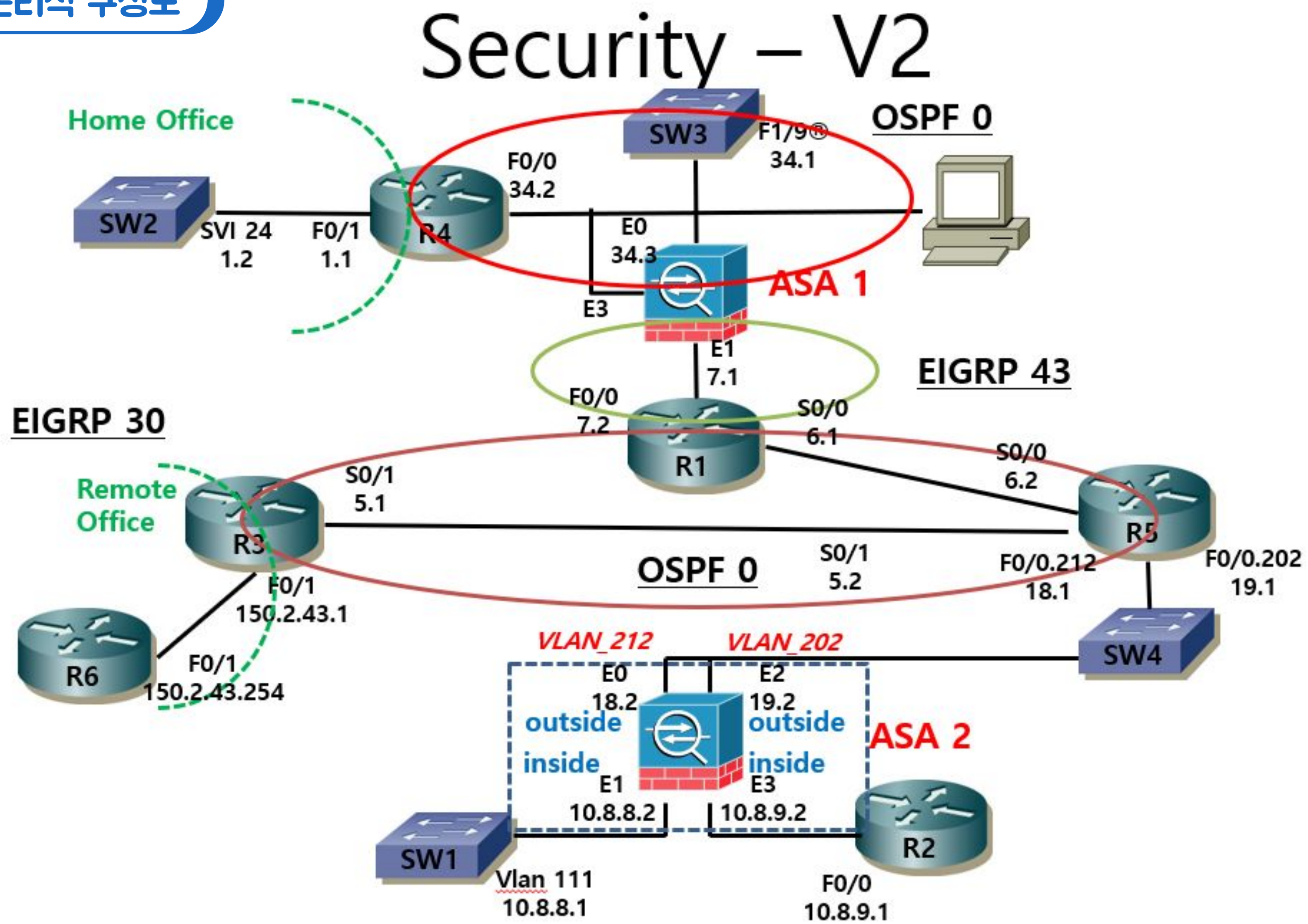
01. 구성도

1 - 1. 물리적 구성도



01. 구성도

1 - 2. 논리적 구성도

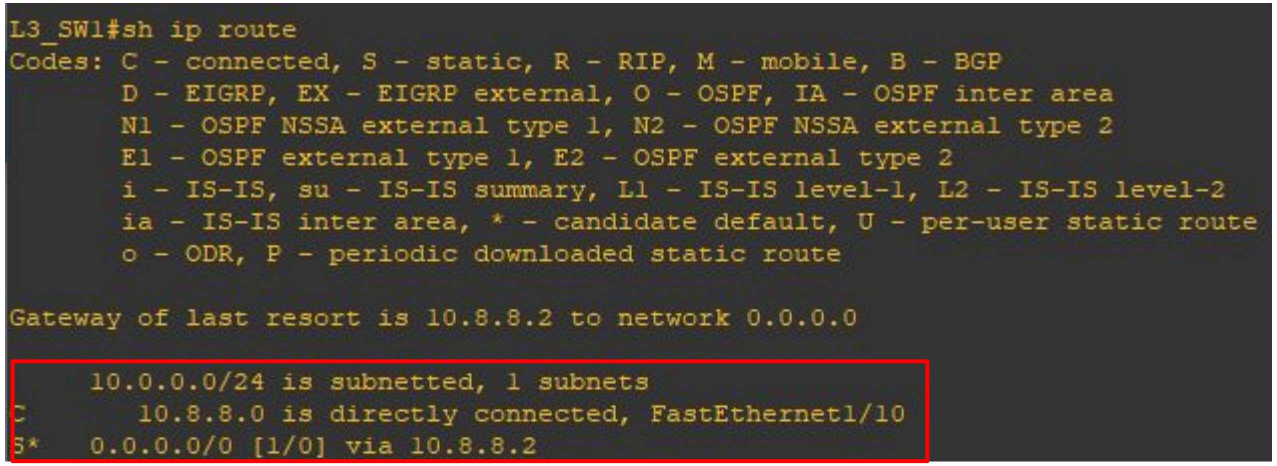


스위치 설정

02. 스위치 설정

2 - 1. SW1

```
int f1/10
no sw
ip add 10.8.8.1 255.255.255.0
ip route 0.0.0.0 0.0.0.0 10.8.8.2
```

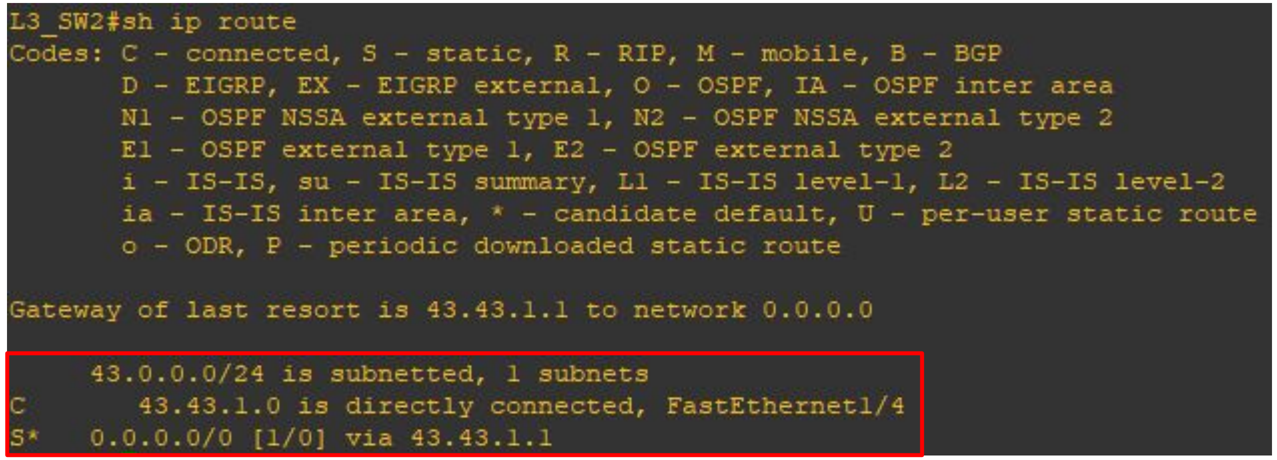


```
L3_SW1#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is 10.8.8.2 to network 0.0.0.0

     10.0.0.0/24 is subnetted, 1 subnets
C       10.8.8.0 is directly connected, FastEthernet1/10
S*   0.0.0.0/0 [1/0] via 10.8.8.2
```

2 - 2. SW2

int f1/4
no sw
ip add 43.43.1.2 255.255.255.0

ip route 0.0.0.0 0.0.0.0 43.43.1.1

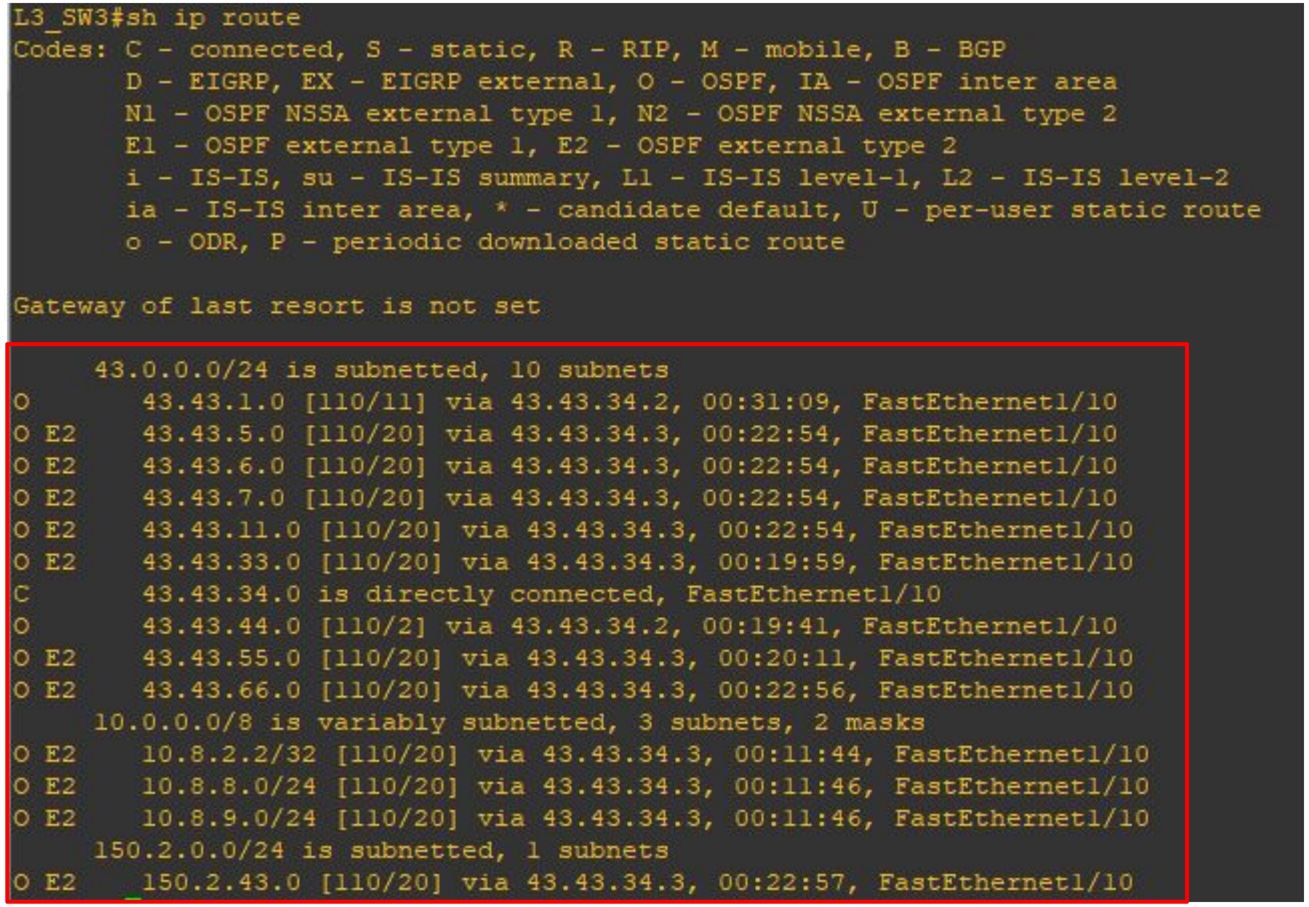


```
L3_SW2#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is 43.43.1.1 to network 0.0.0.0

     43.0.0.0/24 is subnetted, 1 subnets
C       43.43.1.0 is directly connected, FastEthernet1/4
S*   0.0.0.0/0 [1/0] via 43.43.1.1
```

02. 스위치 설정

2 - 3. SW3

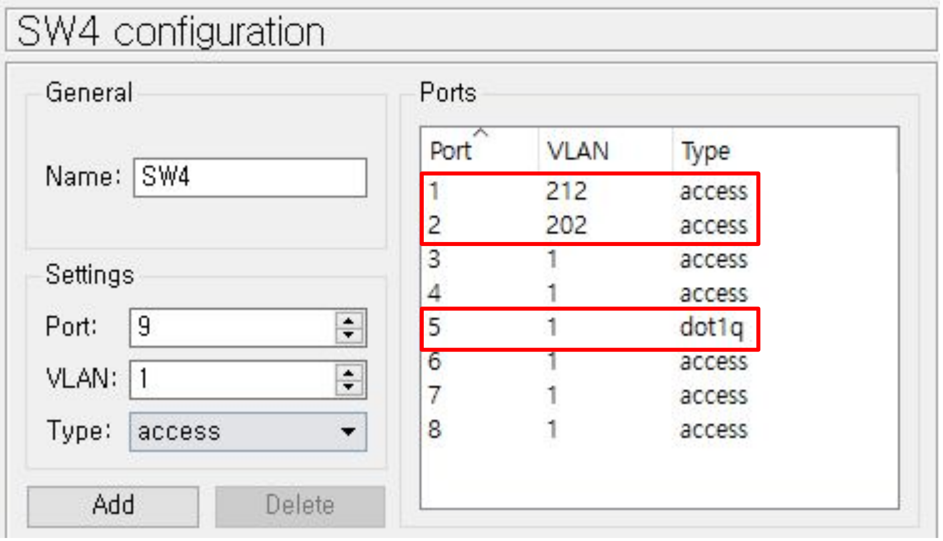
```
int f1/10
no sw
ip add 43.43.34.1 255.255.255.0

router ospf 1
net 43.43.34.1 0.0.0.0 area 0
```



```
L3_SW3#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     43.0.0.0/24 is subnetted, 10 subnets
O       43.43.1.0 [110/11] via 43.43.34.2, 00:31:09, FastEthernet1/10
O E2    43.43.5.0 [110/20] via 43.43.34.3, 00:22:54, FastEthernet1/10
O E2    43.43.6.0 [110/20] via 43.43.34.3, 00:22:54, FastEthernet1/10
O E2    43.43.7.0 [110/20] via 43.43.34.3, 00:22:54, FastEthernet1/10
O E2    43.43.11.0 [110/20] via 43.43.34.3, 00:22:54, FastEthernet1/10
O E2    43.43.33.0 [110/20] via 43.43.34.3, 00:19:59, FastEthernet1/10
C       43.43.34.0 is directly connected, FastEthernet1/10
O       43.43.44.0 [110/2] via 43.43.34.2, 00:19:41, FastEthernet1/10
O E2    43.43.55.0 [110/20] via 43.43.34.3, 00:20:11, FastEthernet1/10
O E2    43.43.66.0 [110/20] via 43.43.34.3, 00:22:56, FastEthernet1/10
     10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
O E2    10.8.2.2/32 [110/20] via 43.43.34.3, 00:11:44, FastEthernet1/10
O E2    10.8.8.0/24 [110/20] via 43.43.34.3, 00:11:46, FastEthernet1/10
O E2    10.8.9.0/24 [110/20] via 43.43.34.3, 00:11:46, FastEthernet1/10
     150.2.0.0/24 is subnetted, 1 subnets
O E2    150.2.43.0 [110/20] via 43.43.34.3, 00:22:57, FastEthernet1/10
```

2 - 3. SW4

```
vlan 212
vlan 202

int f0/5
sw trunk en dot1q
sw mo trunk

int f0/1
sw mo access
sw access vlan 212

int f0/2
sw mo access
sw access vlan 202
```



SW4 configuration

General

Name: SW4

Settings

Port: 9

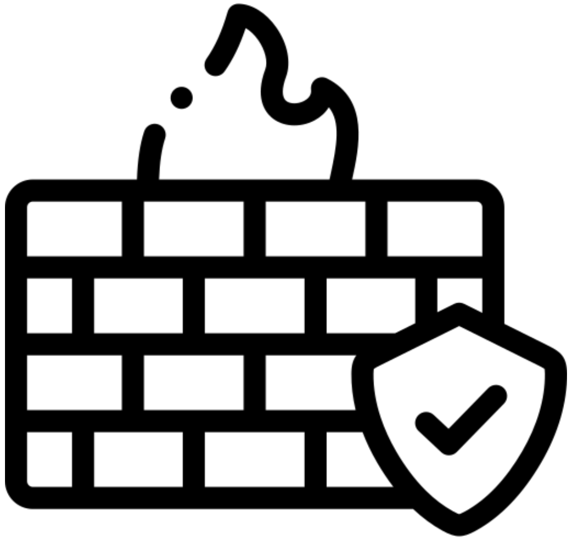
VLAN: 1

Type: access

Ports

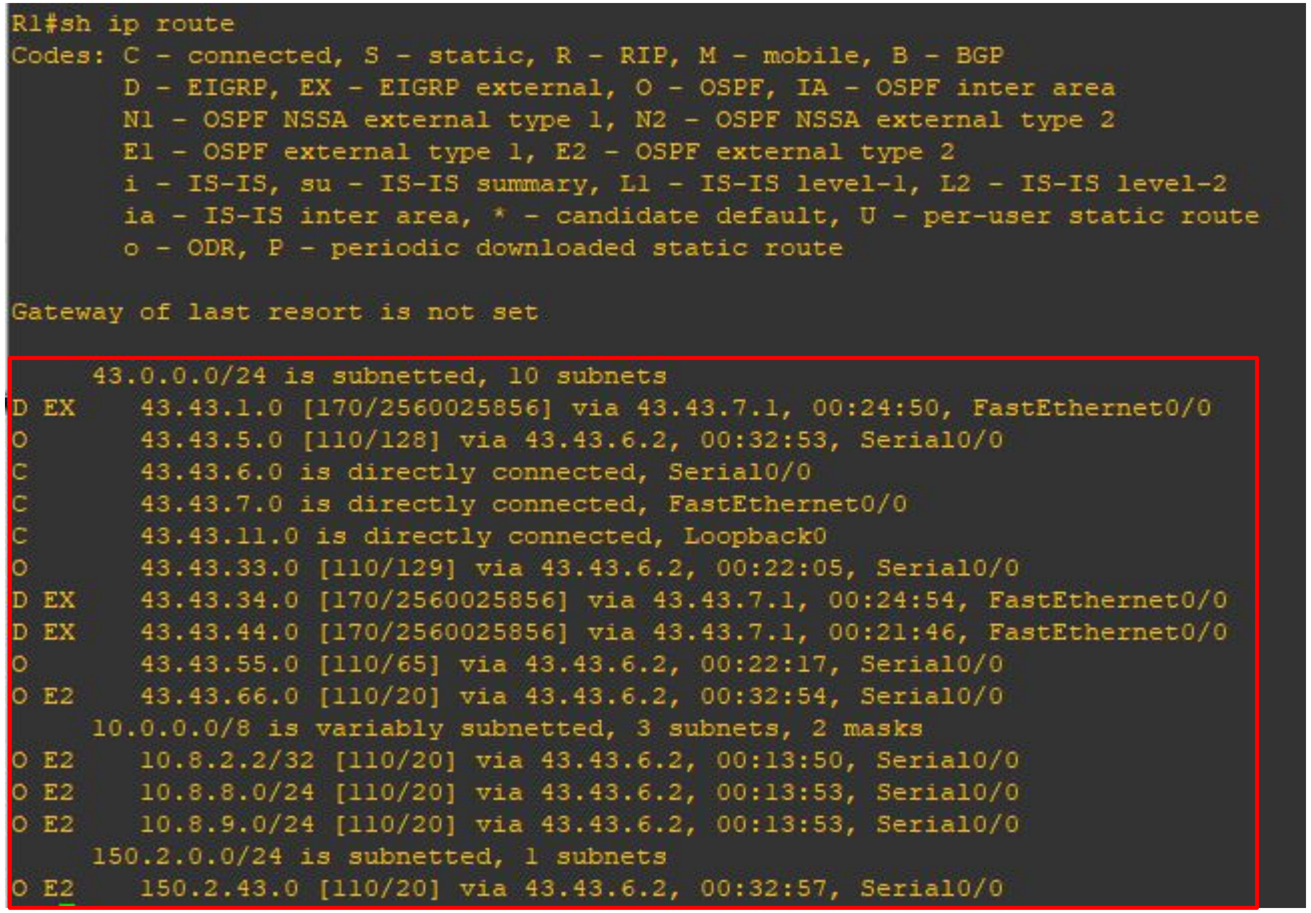
Port	VLAN	Type
1	212	access
2	202	access
3	1	access
4	1	access
5	1	dot1q
6	1	access
7	1	access
8	1	access

라우터 설정



3 - 1. R1

```
int lo0
ip add 43.43.11.1 255.255.255.0

int f0/0
no shut
ip add 43.43.7.2 255.255.255.0

int s0/0
no shut
ip add 43.43.6.1 255.255.255.0

router eigrp 43
no auto
net 43.43.7.2 0.0.0.0
redis os 1 met 1 1 1 1 1

router ospf 1
net 43.43.6.1 0.0.0.0 area 0
net 43.43.11.1 0.0.0.0 area 0
default-inf ori always
redis ei 43 sub

ip route 43.43.18.0 255.255.255.0
43.43.6.2
ip route 43.43.19.0 255.255.255.0
43.43.6.2
```

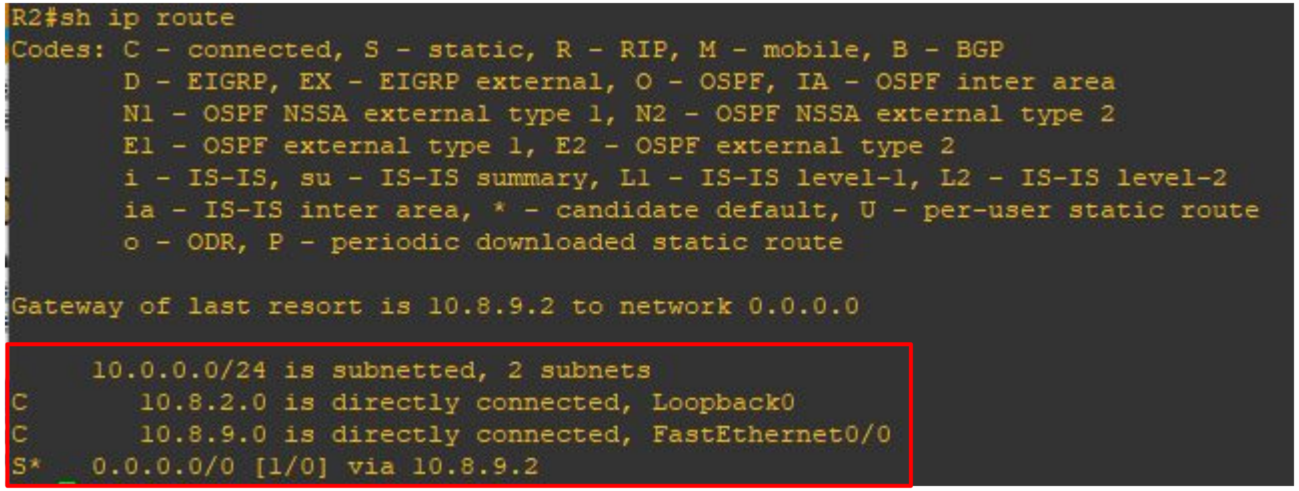


```
R1#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     43.0.0.0/24 is subnetted, 10 subnets
D EX    43.43.1.0 [170/2560025856] via 43.43.7.1, 00:24:50, FastEthernet0/0
O       43.43.5.0 [110/128] via 43.43.6.2, 00:32:53, Serial0/0
C       43.43.6.0 is directly connected, Serial0/0
C       43.43.7.0 is directly connected, FastEthernet0/0
C       43.43.11.0 is directly connected, Loopback0
O       43.43.33.0 [110/129] via 43.43.6.2, 00:22:05, Serial0/0
D EX    43.43.34.0 [170/2560025856] via 43.43.7.1, 00:24:54, FastEthernet0/0
D EX    43.43.44.0 [170/2560025856] via 43.43.7.1, 00:21:46, FastEthernet0/0
O       43.43.55.0 [110/65] via 43.43.6.2, 00:22:17, Serial0/0
O E2    43.43.66.0 [110/20] via 43.43.6.2, 00:32:54, Serial0/0
     10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
O E2    10.8.2.2/32 [110/20] via 43.43.6.2, 00:13:50, Serial0/0
O E2    10.8.8.0/24 [110/20] via 43.43.6.2, 00:13:53, Serial0/0
O E2    10.8.9.0/24 [110/20] via 43.43.6.2, 00:13:53, Serial0/0
     150.2.0.0/24 is subnetted, 1 subnets
O E2    150.2.43.0 [110/20] via 43.43.6.2, 00:32:57, Serial0/0
```

03. 라우터 설정

3 - 2. R2

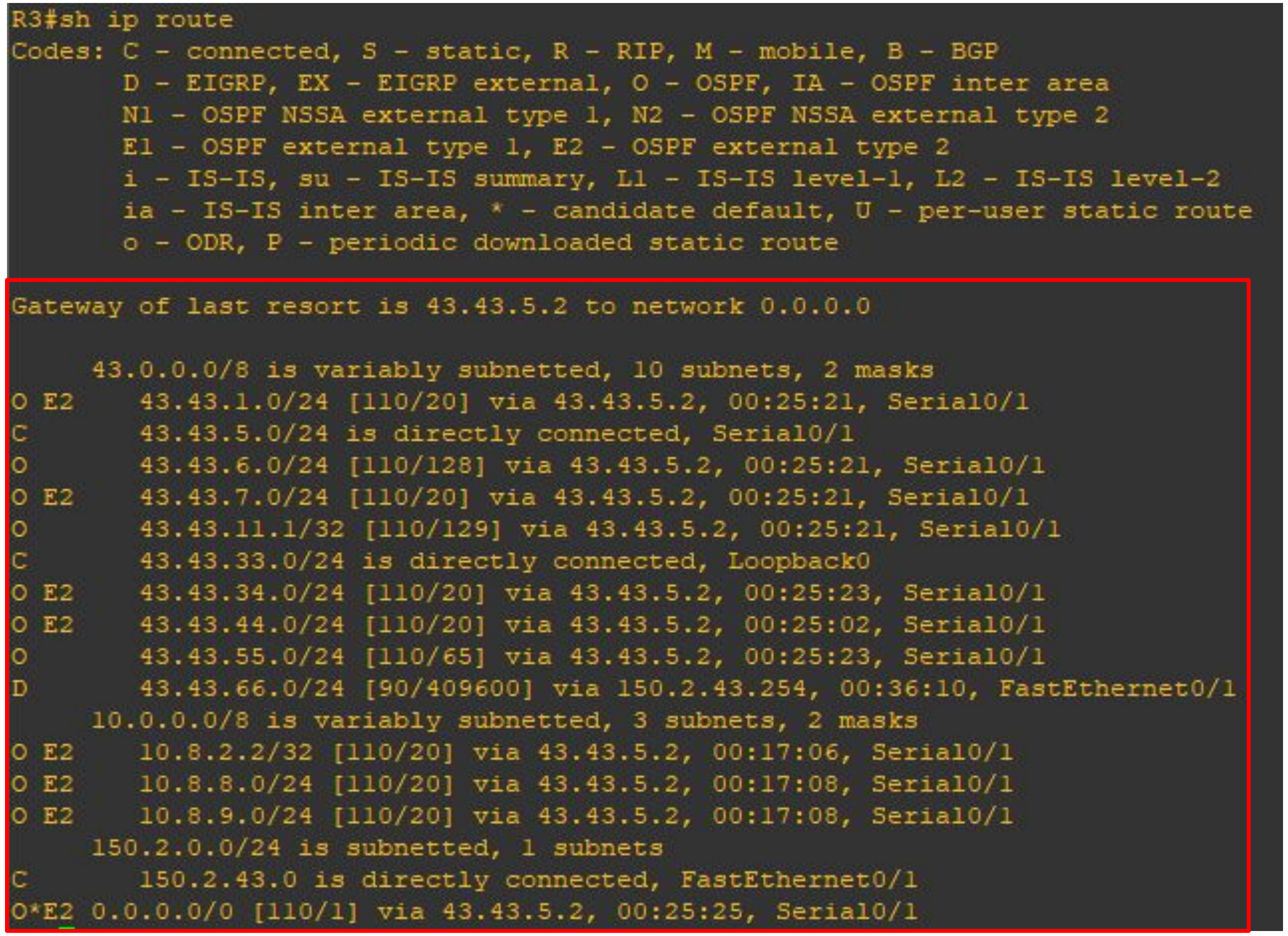
```
int lo0
ip add 10.8.2.2 255.255.255.0

int f0/0
no shut
ip add 10.8.9.1 255.255.255.0

ip route 0.0.0.0 0.0.0.0 10.8.9.2
```



```
R2#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is 10.8.9.2 to network 0.0.0.0

     10.0.0.0/24 is subnetted, 2 subnets
C       10.8.2.0 is directly connected, Loopback0
C       10.8.9.0 is directly connected, FastEthernet0/0
S*   0.0.0.0/0 [1/0] via 10.8.9.2
```

3 - 3. R3

```
int lo0
ip add 43.43.33.3 255.255.255.0

int f0/1
no shut
ip add 150.2.43.1 255.255.255.0

int s0/1
no shut
ip add 43.43.5.1 255.255.255.0

router ospf 1
router-id 43.43.33.3
net 43.43.33.3 0.0.0.0 area 0
net 43.43.5.1 0.0.0.0 area 0
redi eigrp 30 sub

router eigrp 30
no au
net 150.2.43.1 0.0.0.0
redi ospf 1 met 1 1 1 1 1
```



```
R3#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is 43.43.5.2 to network 0.0.0.0

     43.0.0.0/8 is variably subnetted, 10 subnets, 2 masks
O E2    43.43.1.0/24 [110/20] via 43.43.5.2, 00:25:21, Serial0/1
C       43.43.5.0/24 is directly connected, Serial0/1
O       43.43.6.0/24 [110/128] via 43.43.5.2, 00:25:21, Serial0/1
O E2    43.43.7.0/24 [110/20] via 43.43.5.2, 00:25:21, Serial0/1
O       43.43.11.1/32 [110/129] via 43.43.5.2, 00:25:21, Serial0/1
C       43.43.33.0/24 is directly connected, Loopback0
O E2    43.43.34.0/24 [110/20] via 43.43.5.2, 00:25:23, Serial0/1
O E2    43.43.44.0/24 [110/20] via 43.43.5.2, 00:25:02, Serial0/1
O       43.43.55.0/24 [110/65] via 43.43.5.2, 00:25:23, Serial0/1
D       43.43.66.0/24 [90/409600] via 150.2.43.254, 00:36:10, FastEthernet0/1
     10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
O E2    10.8.2.2/32 [110/20] via 43.43.5.2, 00:17:06, Serial0/1
O E2    10.8.8.0/24 [110/20] via 43.43.5.2, 00:17:08, Serial0/1
O E2    10.8.9.0/24 [110/20] via 43.43.5.2, 00:17:08, Serial0/1
     150.2.0.0/24 is subnetted, 1 subnets
C       150.2.43.0 is directly connected, FastEthernet0/1
O*E2 0.0.0.0/0 [110/1] via 43.43.5.2, 00:25:25, Serial0/1
```

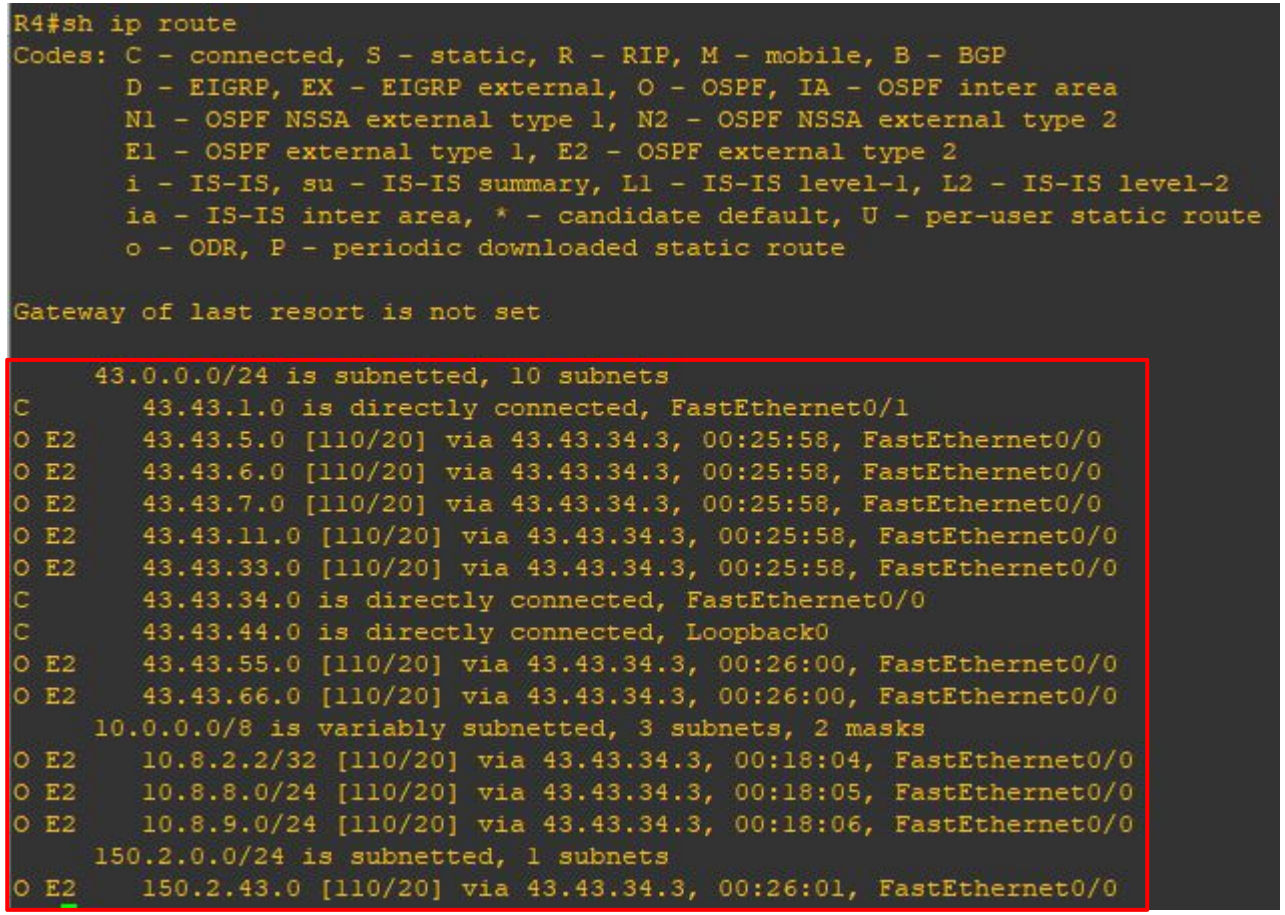
3 - 4. R4

int lo0
ip add 43.43.44.4 255.255.255.0

int f0/1
no shut
ip add 43.43.1.1 255.255.255.0

int f0/0
no shut
ip add 43.43.34.2 255.255.255.0

router ospf 1
router-id 43.43.44.4
net 43.43.34.2 0.0.0.0 area 0
net 43.43.44.4 0.0.0.0 area 0
net 43.43.1.1 0.0.0.0 area 0

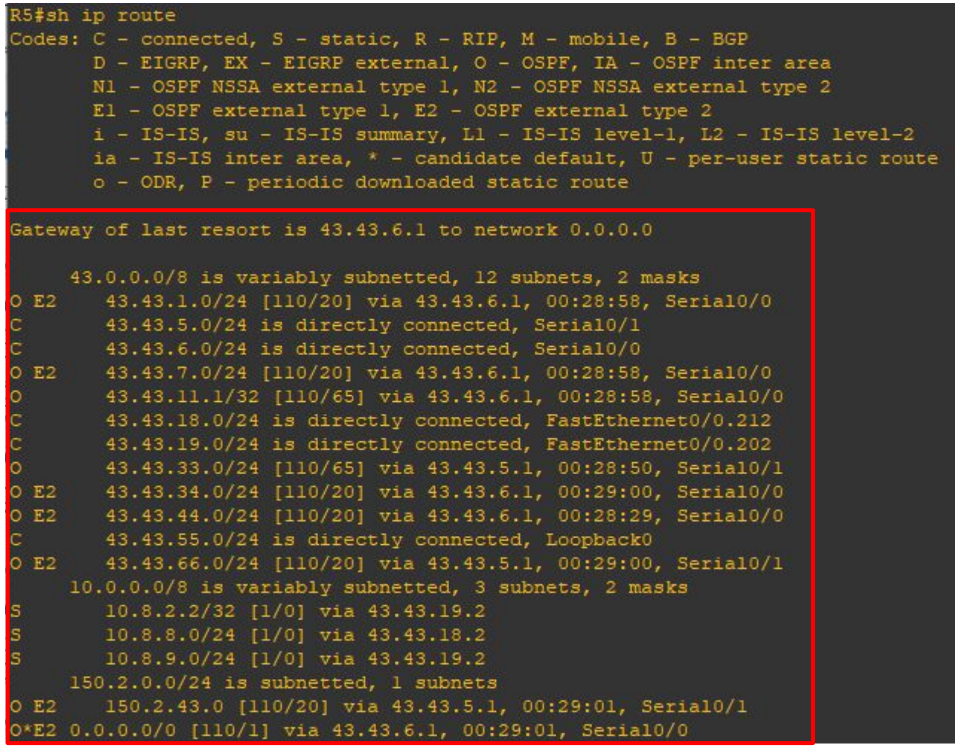


```
R4#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     43.0.0.0/24 is subnetted, 10 subnets
C       43.43.1.0 is directly connected, FastEthernet0/1
O E2    43.43.5.0 [110/20] via 43.43.34.3, 00:25:58, FastEthernet0/0
O E2    43.43.6.0 [110/20] via 43.43.34.3, 00:25:58, FastEthernet0/0
O E2    43.43.7.0 [110/20] via 43.43.34.3, 00:25:58, FastEthernet0/0
O E2    43.43.11.0 [110/20] via 43.43.34.3, 00:25:58, FastEthernet0/0
O E2    43.43.33.0 [110/20] via 43.43.34.3, 00:25:58, FastEthernet0/0
C       43.43.34.0 is directly connected, FastEthernet0/0
C       43.43.44.0 is directly connected, Loopback0
O E2    43.43.55.0 [110/20] via 43.43.34.3, 00:26:00, FastEthernet0/0
O E2    43.43.66.0 [110/20] via 43.43.34.3, 00:26:00, FastEthernet0/0
     10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
O E2    10.8.2.2/32 [110/20] via 43.43.34.3, 00:18:04, FastEthernet0/0
O E2    10.8.8.0/24 [110/20] via 43.43.34.3, 00:18:05, FastEthernet0/0
O E2    10.8.9.0/24 [110/20] via 43.43.34.3, 00:18:06, FastEthernet0/0
     150.2.0.0/24 is subnetted, 1 subnets
O E2    150.2.43.0 [110/20] via 43.43.34.3, 00:26:01, FastEthernet0/0
```

3 - 5. R5

```
int lo0
ip add 43.43.55.5 255.255.255.0

int s0/0
no shut
ip add 43.43.6.2 255.255.255.0

int s0/1
no shut
ip add 43.43.5.2 255.255.255.0

int f0/0
no shut

int f0/0.202
en dot 202
ip add 43.43.19.1 255.255.255.0

int f0/0.212
en dot 212
ip add 43.43.18.1 255.255.255.0
```

```
router ospf 1
router-id 43.43.55.5
net 43.43.55.5 0.0.0.0 area 0
net 43.43.6.2 0.0.0.0 area 0
net 43.43.5.2 0.0.0.0 area 0
redi static sub

ip route 10.8.9.0 255.255.255.0 43.43.19.2
ip route 10.8.8.0 255.255.255.0 43.43.18.2
ip route 10.8.2.2 255.255.255.255 43.43.19.2
```

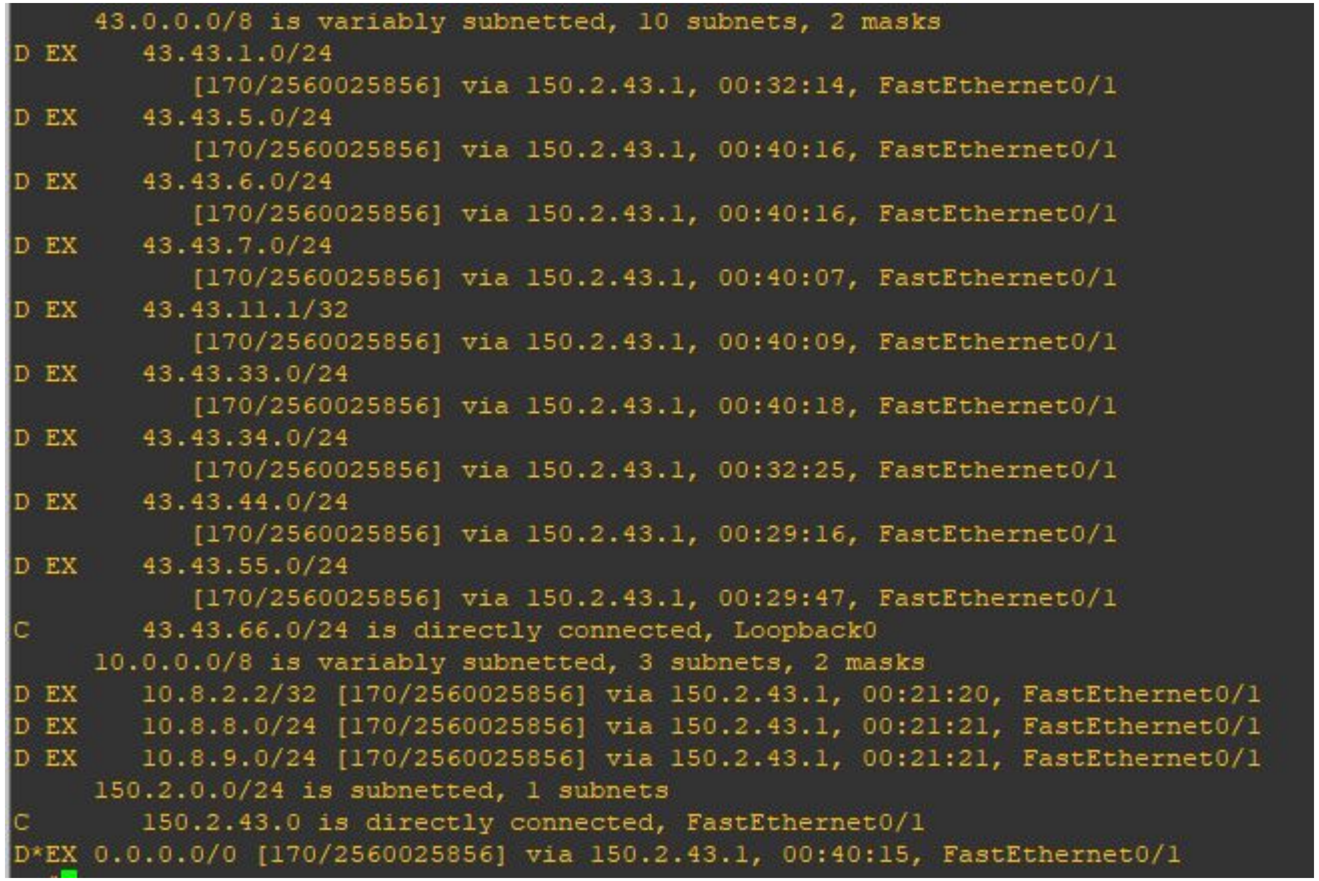


```
R5#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is 43.43.6.1 to network 0.0.0.0

     43.0.0.0/8 is variably subnetted, 12 subnets, 2 masks
O E2    43.43.1.0/24 [110/20] via 43.43.6.1, 00:28:58, Serial0/0
C       43.43.5.0/24 is directly connected, Serial0/1
C       43.43.6.0/24 is directly connected, Serial0/0
O E2    43.43.7.0/24 [110/20] via 43.43.6.1, 00:28:58, Serial0/0
O       43.43.11.1/32 [110/65] via 43.43.6.1, 00:28:58, Serial0/0
C       43.43.18.0/24 is directly connected, FastEthernet0/0.212
C       43.43.19.0/24 is directly connected, FastEthernet0/0.202
O       43.43.33.0/24 [110/65] via 43.43.5.1, 00:28:50, Serial0/1
O E2    43.43.34.0/24 [110/20] via 43.43.6.1, 00:29:00, Serial0/0
O E2    43.43.44.0/24 [110/20] via 43.43.6.1, 00:28:29, Serial0/0
C       43.43.55.0/24 is directly connected, Loopback0
O E2    43.43.66.0/24 [110/20] via 43.43.5.1, 00:29:00, Serial0/1
     10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
S       10.8.2.2/32 [1/0] via 43.43.19.2
S       10.8.8.0/24 [1/0] via 43.43.18.2
S       10.8.9.0/24 [1/0] via 43.43.19.2
     150.2.0.0/24 is subnetted, 1 subnets
O E2    150.2.43.0 [110/20] via 43.43.5.1, 00:29:01, Serial0/1
O*E2 0.0.0.0/0 [110/1] via 43.43.6.1, 00:29:01, Serial0/0
```

03. 라우터 설정

3 - 6. R6

```
int lo0
ip add 43.43.66.6 255.255.255.0

int f0/1
no shut
ip add 150.2.43.254 255.255.255.0

router eigrp 30
no au
net 150.2.43.254 0.0.0.0
net 43.43.66.6 0.0.0.0
```



```
     43.0.0.0/8 is variably subnetted, 10 subnets, 2 masks
D EX    43.43.1.0/24
           [170/2560025856] via 150.2.43.1, 00:32:14, FastEthernet0/1
D EX    43.43.5.0/24
           [170/2560025856] via 150.2.43.1, 00:40:16, FastEthernet0/1
D EX    43.43.6.0/24
           [170/2560025856] via 150.2.43.1, 00:40:16, FastEthernet0/1
D EX    43.43.7.0/24
           [170/2560025856] via 150.2.43.1, 00:40:07, FastEthernet0/1
D EX    43.43.11.1/32
           [170/2560025856] via 150.2.43.1, 00:40:09, FastEthernet0/1
D EX    43.43.33.0/24
           [170/2560025856] via 150.2.43.1, 00:40:18, FastEthernet0/1
D EX    43.43.34.0/24
           [170/2560025856] via 150.2.43.1, 00:32:25, FastEthernet0/1
D EX    43.43.44.0/24
           [170/2560025856] via 150.2.43.1, 00:29:16, FastEthernet0/1
D EX    43.43.55.0/24
           [170/2560025856] via 150.2.43.1, 00:29:47, FastEthernet0/1
C       43.43.66.0/24 is directly connected, Loopback0
     10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
D EX    10.8.2.2/32 [170/2560025856] via 150.2.43.1, 00:21:20, FastEthernet0/1
D EX    10.8.8.0/24 [170/2560025856] via 150.2.43.1, 00:21:21, FastEthernet0/1
D EX    10.8.9.0/24 [170/2560025856] via 150.2.43.1, 00:21:21, FastEthernet0/1
     150.2.0.0/24 is subnetted, 1 subnets
C       150.2.43.0 is directly connected, FastEthernet0/1
D*EX 0.0.0.0/0 [170/2560025856] via 150.2.43.1, 00:40:15, FastEthernet0/1
```

방화벽-1 설정

04. 방화벽 - 1 설정

4 - 1. 인터페이스 설정

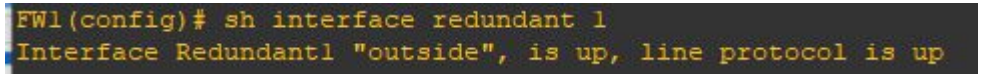
```
int g0
no shut

int g1
no shut

int g2
no shut

int g1
nameif inside
ip add 43.43.7.1 255.255.255.0
```

4 - 2. Redundant 기술

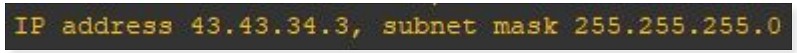
Redundant Interface
: 두 개의 물리적 인터페이스를 하나의 논리 인터페이스로 묶어, 하나가 다운 되더라도 자동으로 인터페이스가 동작하도록 하는 인터페이스 이중화 기술

하나는 active, 다른 하나는 standby로 동작

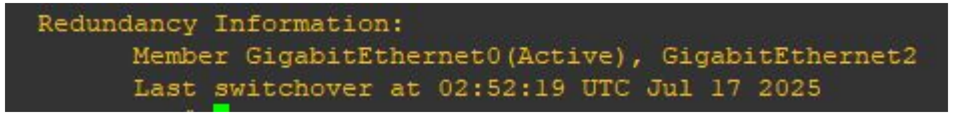
```
int redundant 1

member-interface g0
member-interface g2

nameif outside
ip add 43.43.34.3 255.255.255.0
```



```
FW1(config)# sh interface redundant 1
Interface Redundant1 "outside", is up, line protocol is up
```



```
IP address 43.43.34.3, subnet mask 255.255.255.0
```

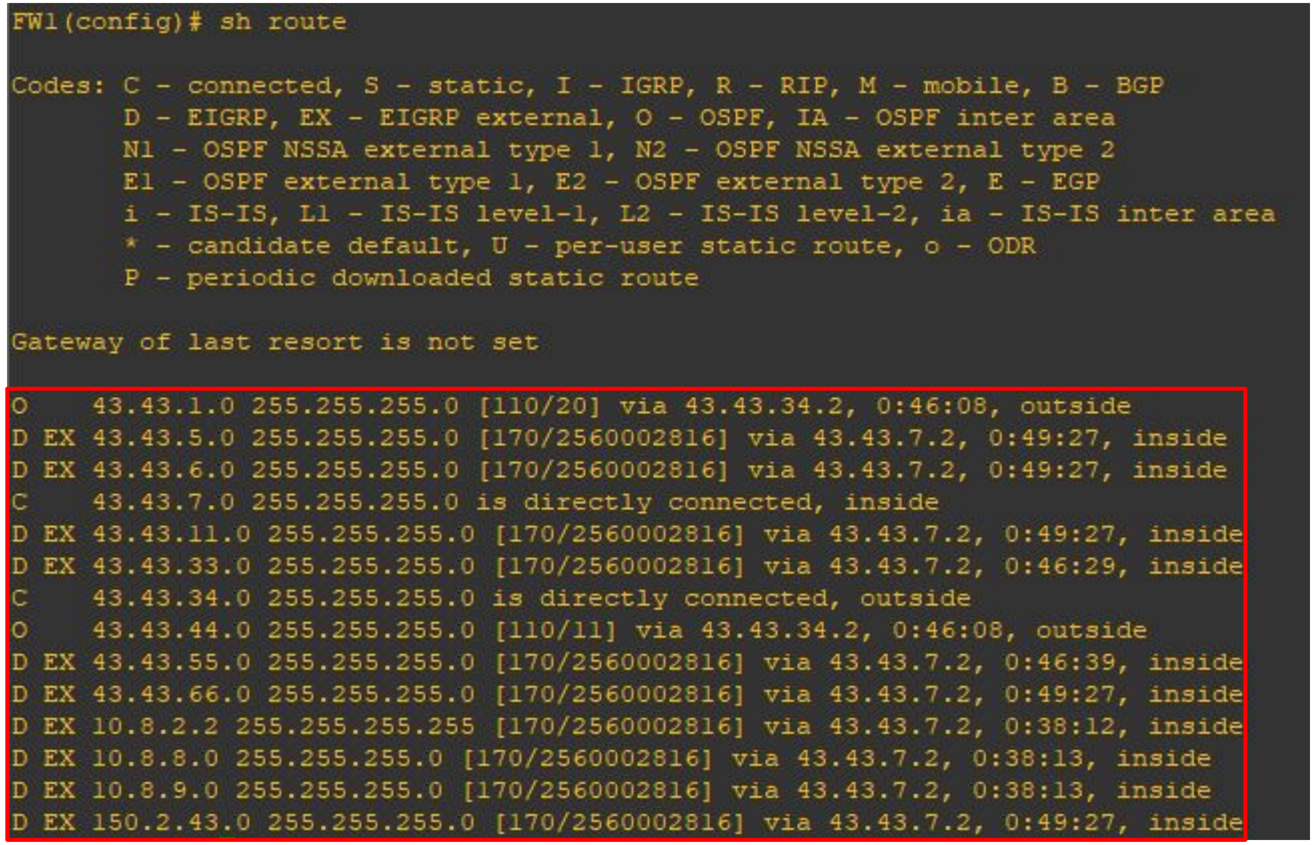


```
 Redundancy Information:
       Member GigabitEthernet0(Active), GigabitEthernet2
       Last switchover at 02:52:19 UTC Jul 17 2025
```

04. 방화벽 - 1 설정

4 - 3. 라우팅 설정

```
router ospf 1
net 43.43.34.3 255.255.255.255 area 0
redi eigrp 43 sub

router eigrp 43
no auto
net 43.43.7.1 255.255.255.255
redi os 1 met 1 1 1 1 1
```



```
FW1(config)# sh route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

O    43.43.1.0 255.255.255.0 [110/20] via 43.43.34.2, 0:46:08, outside
D EX 43.43.5.0 255.255.255.0 [170/2560002816] via 43.43.7.2, 0:49:27, inside
D EX 43.43.6.0 255.255.255.0 [170/2560002816] via 43.43.7.2, 0:49:27, inside
C    43.43.7.0 255.255.255.0 is directly connected, inside
D EX 43.43.11.0 255.255.255.0 [170/2560002816] via 43.43.7.2, 0:49:27, inside
D EX 43.43.33.0 255.255.255.0 [170/2560002816] via 43.43.7.2, 0:46:29, inside
C    43.43.34.0 255.255.255.0 is directly connected, outside
O    43.43.44.0 255.255.255.0 [110/11] via 43.43.34.2, 0:46:08, outside
D EX 43.43.55.0 255.255.255.0 [170/2560002816] via 43.43.7.2, 0:46:39, inside
D EX 43.43.66.0 255.255.255.0 [170/2560002816] via 43.43.7.2, 0:49:27, inside
D EX 10.8.2.2 255.255.255.255 [170/2560002816] via 43.43.7.2, 0:38:12, inside
D EX 10.8.8.0 255.255.255.0 [170/2560002816] via 43.43.7.2, 0:38:13, inside
D EX 10.8.9.0 255.255.255.0 [170/2560002816] via 43.43.7.2, 0:38:13, inside
D EX 150.2.43.0 255.255.255.0 [170/2560002816] via 43.43.7.2, 0:49:27, inside
```

4 - 4. MPF 설정

MPF(Modula Policy Framework)
: 모듈화된 정책 설정 체계

class-map inspection_default
match default-inspection-traffic

클래스 맵: 트래픽을 분류

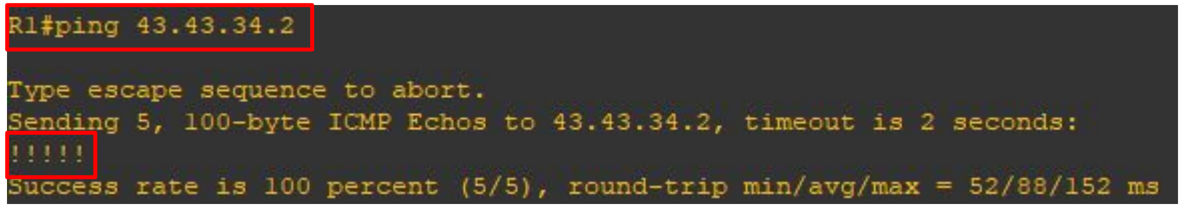
policy-map global_policy
class inspection_default
inspect icmp

폴리시 맵: 클래스 맵에서 분류한 트래픽에 대한 보안 정책 설정

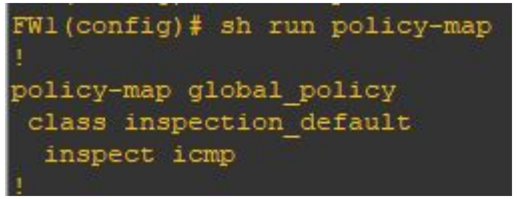
service-policy global_policy int inside
service-policy global_policy int outside

서비스 폴리시: 폴리시 맵 활성화

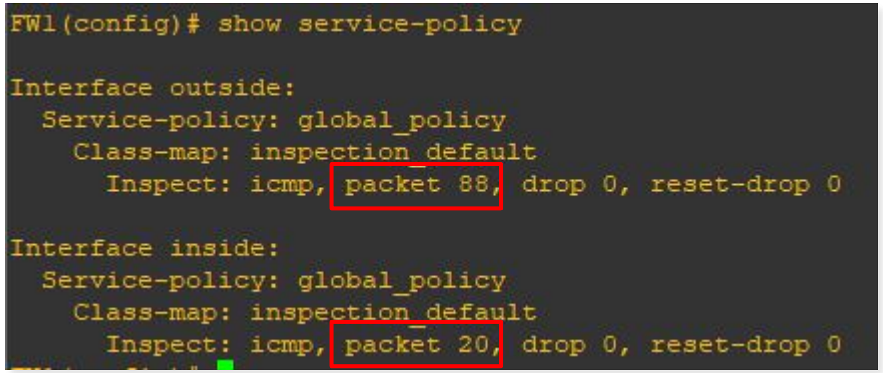
내부-> 외부 Ping (R1 -> R4)



```
R1#ping 43.43.34.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 43.43.34.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 52/88/152 ms
```



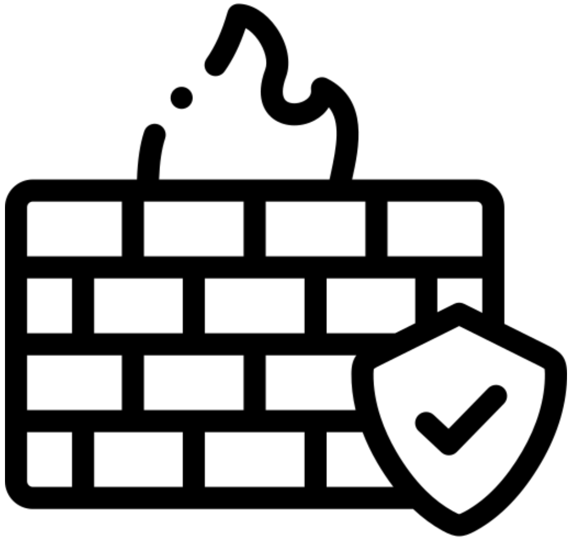
```
FW1(config)# sh run policy-map
!
policy-map global_policy
 class inspection_default
  inspect icmp
!
```



```
FW1(config)# show service-policy

Interface outside:
  Service-policy: global_policy
    Class-map: inspection_default
      Inspect: icmp, packet 88, drop 0, reset-drop 0

Interface inside:
  Service-policy: global_policy
    Class-map: inspection_default
      Inspect: icmp, packet 20, drop 0, reset-drop 0
```

outside와 inside에서 들어온 ICMP 패킷 확인

방화벽-2 설정

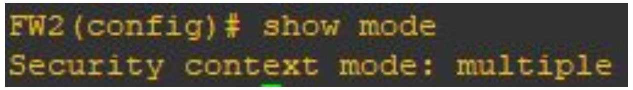


05. 방화벽 - 2 설정

5 - 1. 모드 설정

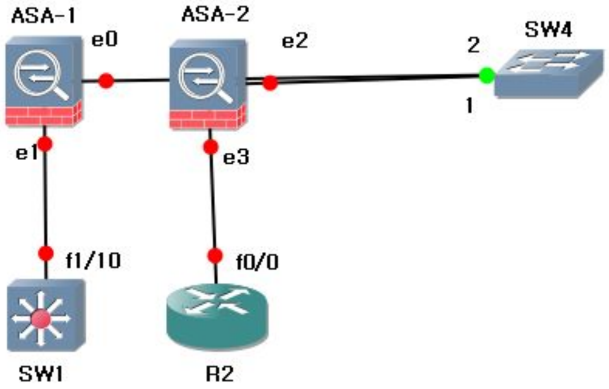
Security Context
: 하나의 ASA를 가상적으로 다수 개의 ASA로 사용하는 기술
물리적으로는 single, 논리적으로는 multiple

mode multiple



```
FW2(config)# show mode
Security context mode: multiple
```

논리적 구성도



5 - 2. 인터페이스 설정

int g0
no shut

int g1
no shut

int g2
no shut

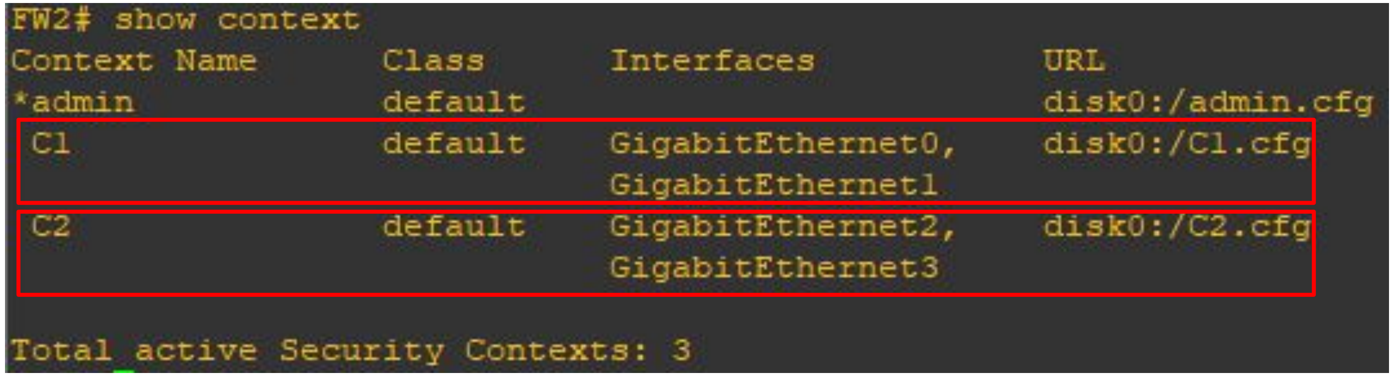
int g3
no shut

5 - 4. Context 설정

```
admin-context admin
context admin
config-url admin.cfg

context C1
allocate-int g0
allocate-int g1
config-url C1.cfg

context C2
allocate-int g2
allocate-int g3
config-url C2.cfg
```

```
changeto context C1

int g1
nameif inside
ip add 10.8.8.2 255.255.255.0

int g0
nameif outside
ip add 43.43.18.2 255.255.255.0
```

```
changeto context C2

int g3
nameif inside
ip add 10.8.9.2 255.255.255.0

int g2
nameif outside
ip add 43.43.19.2 255.255.255.0
```



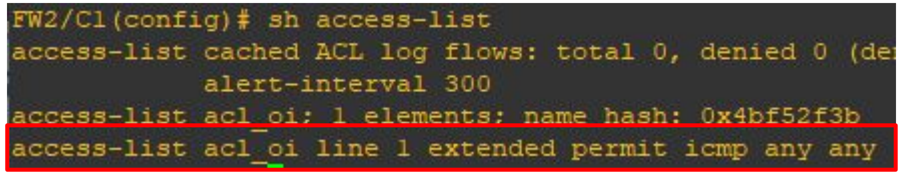
```
FW2# show context
Context Name      Class      Interfaces           URL
*admin            default                         disk0:/admin.cfg
 C1               default    GigabitEthernet0,    disk0:/C1.cfg
                             GigabitEthernet1
 C2               default    GigabitEthernet2,    disk0:/C2.cfg
                             GigabitEthernet3

Total active Security Contexts: 3
```

05. 방화벽 - 2 설정

5 - 5. ACL

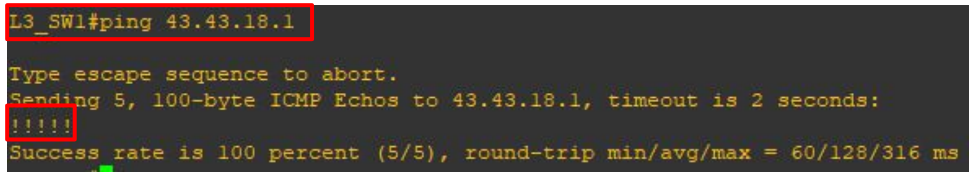
C1 ACL 설정

access-list acl_oi per icmp any any
access-group acl_oi in interface outside



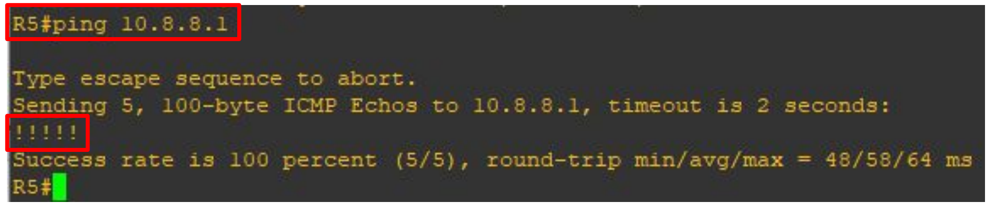
```
FW2/C1(config)# sh access-list
access-list cached ACL log flows: total 0, denied 0 (de
            alert-interval 300
access-list acl_oi; 1 elements; name hash: 0x4bf52f3b
access-list acl_oi line 1 extended permit icmp any any
```

내부 -> 외부 Ping (SW1 -> R5)



```
L3_SW1#ping 43.43.18.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 43.43.18.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 60/128/316 ms
```

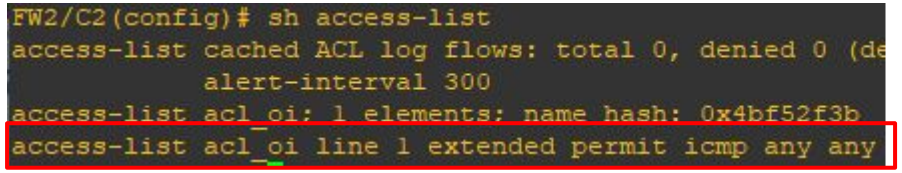
외부 -> 내부 Ping (R5 -> SW1)



```
R5#ping 10.8.8.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.8.8.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 48/58/64 ms
R5#
```

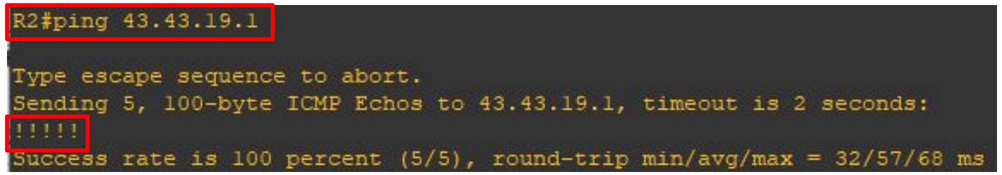
C2 ACL 설정

access-list acl_oi per icmp any any
access-group acl_oi in interface outside



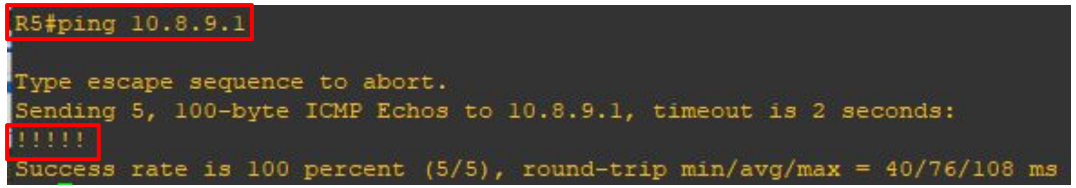
```
FW2/C2(config)# sh access-list
access-list cached ACL log flows: total 0, denied 0 (de
            alert-interval 300
access-list acl_oi; 1 elements; name hash: 0x4bf52f3b
access-list acl_oi line 1 extended permit icmp any any
```

내부 -> 외부 Ping (R2 -> R5)



```
R2#ping 43.43.19.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 43.43.19.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/57/68 ms
```

외부 -> 내부 Ping (R5 -> R2)



```
R5#ping 10.8.9.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.8.9.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 40/76/108 ms
```

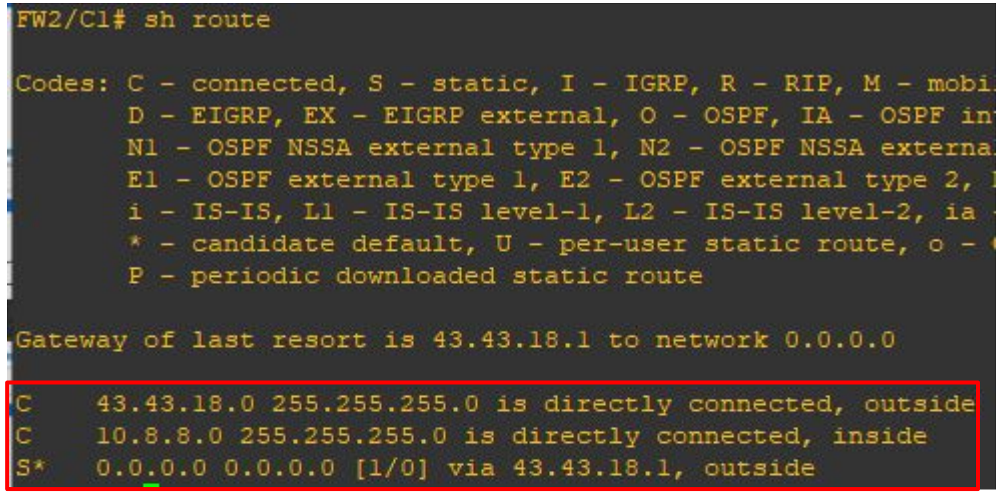
5 - 6. Routing

changeto context C1

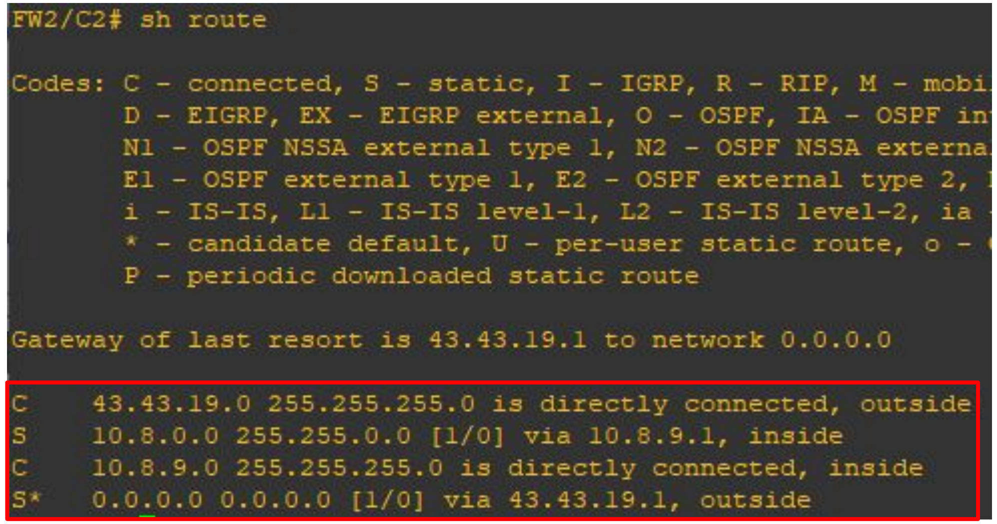
route outside 0 0 43.43.18.1
route inside 10.8.0.0 255.255.0.0 10.8.8.1

changeto content C2

route outside 0 0 43.43.18.2
route inside 10.8.0.0 255.255.0.0 10.8.9.1



```
FW2/C1# sh route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobi
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF in
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA externa
       E1 - OSPF external type 1, E2 - OSPF external type 2,
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia
       * - candidate default, U - per-user static route, o -
       P - periodic downloaded static route

Gateway of last resort is 43.43.18.1 to network 0.0.0.0

C    43.43.18.0 255.255.255.0 is directly connected, outside
C    10.8.8.0 255.255.255.0 is directly connected, inside
S*   0.0.0.0 0.0.0.0 [1/0] via 43.43.18.1, outside
```



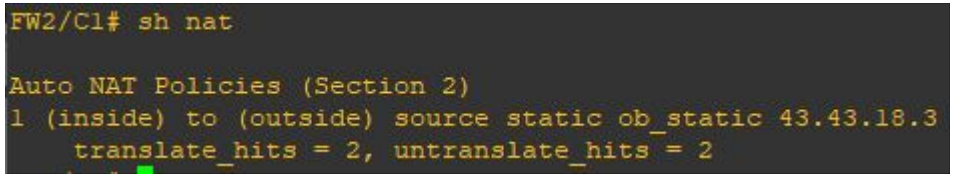
```
FW2/C2# sh route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobi
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF in
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA externa
       E1 - OSPF external type 1, E2 - OSPF external type 2,
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia
       * - candidate default, U - per-user static route, o -
       P - periodic downloaded static route

Gateway of last resort is 43.43.19.1 to network 0.0.0.0

C    43.43.19.0 255.255.255.0 is directly connected, outside
S    10.8.0.0 255.255.0.0 [1/0] via 10.8.9.1, inside
C    10.8.9.0 255.255.255.0 is directly connected, inside
S*   0.0.0.0 0.0.0.0 [1/0] via 43.43.19.1, outside
```

5 - 7. NAT 설정

C1 NAT 설정 (Static)

Static object nat: 사설 IP주소를 외부에 있는 목적지까지 라우팅 가능한 공인 IP 주소로 변환시키거나, 외부에서 내부의 사설 IP 주소를 가진 서버와 통신할 수 있게 하는 기술

```
object network ob_static
host 10.8.8.1
nat (inside,outside) static 43.43.18.3
```

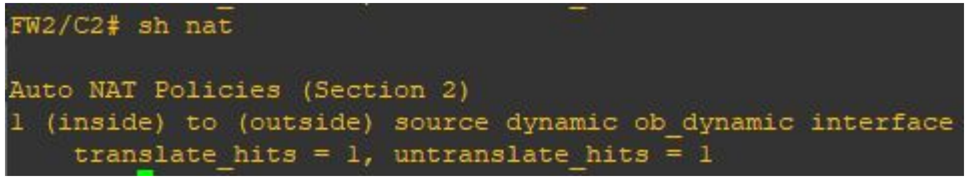


```
FW2/C1# sh nat

Auto NAT Policies (Section 2)
1 (inside) to (outside) source static ob_static 43.43.18.3
    translate_hits = 2, untranslate_hits = 2
```

C2 NAT 설정 (Dynamic PAT)

Dynamic Object Pat: 내부 IP가 외부로 나갈 때 미리 설정된 IP Pool을 이용하여 주소를 변환해주는 기술 , PAT의 경우 하나의 공인 IP를 이용해 다수의 사설 IP가 외부와 통신 가능

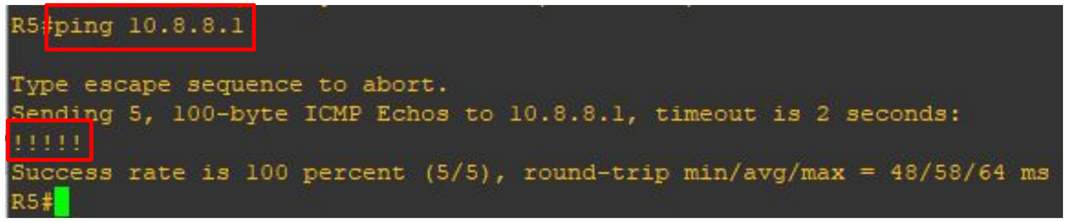
```
object network ob_dynamic
subnet 10.8.0.0 255.255.0.0
nat (inside,outside) dynamic interface
```



```
FW2/C2# sh nat

Auto NAT Policies (Section 2)
1 (inside) to (outside) source dynamic ob_dynamic interface
    translate_hits = 1, untranslate_hits = 1
```

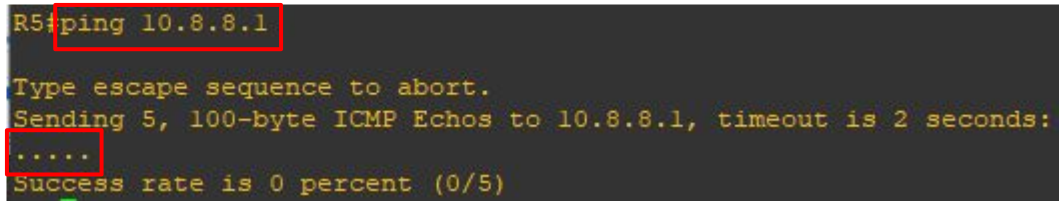
5 - 7. NAT 설정

Static NAT 설정 전

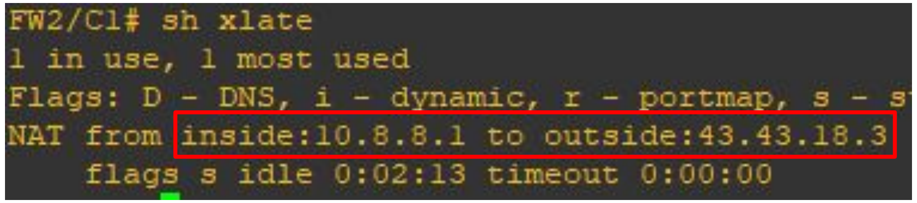


```
R5#ping 10.8.8.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.8.8.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 48/58/64 ms
R5#
```

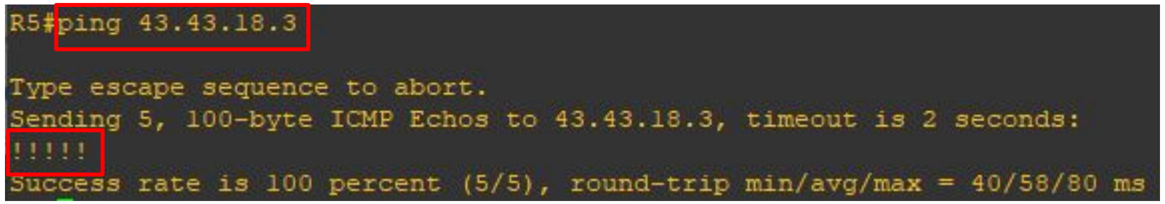
Static NAT 설정 후



```
R5#ping 10.8.8.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.8.8.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```



```
FW2/C1# sh xlate
1 in use, 1 most used
Flags: D - DNS, i - dynamic, r - portmap, s - s
NAT from inside:10.8.8.1 to outside:43.43.18.3
    flags s idle 0:02:13 timeout 0:00:00
```



```
R5#ping 43.43.18.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 43.43.18.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 40/58/80 ms
```

감사합니다.