방화벽 프로젝트

Team. C2K2
김동완, 김도욱, 차호영, 최태정

목차

1. 구성도
2. 스위치 설정
3. 라우터 설정
4. 방화벽-1 설정
5. 방화벽-2 설정

1

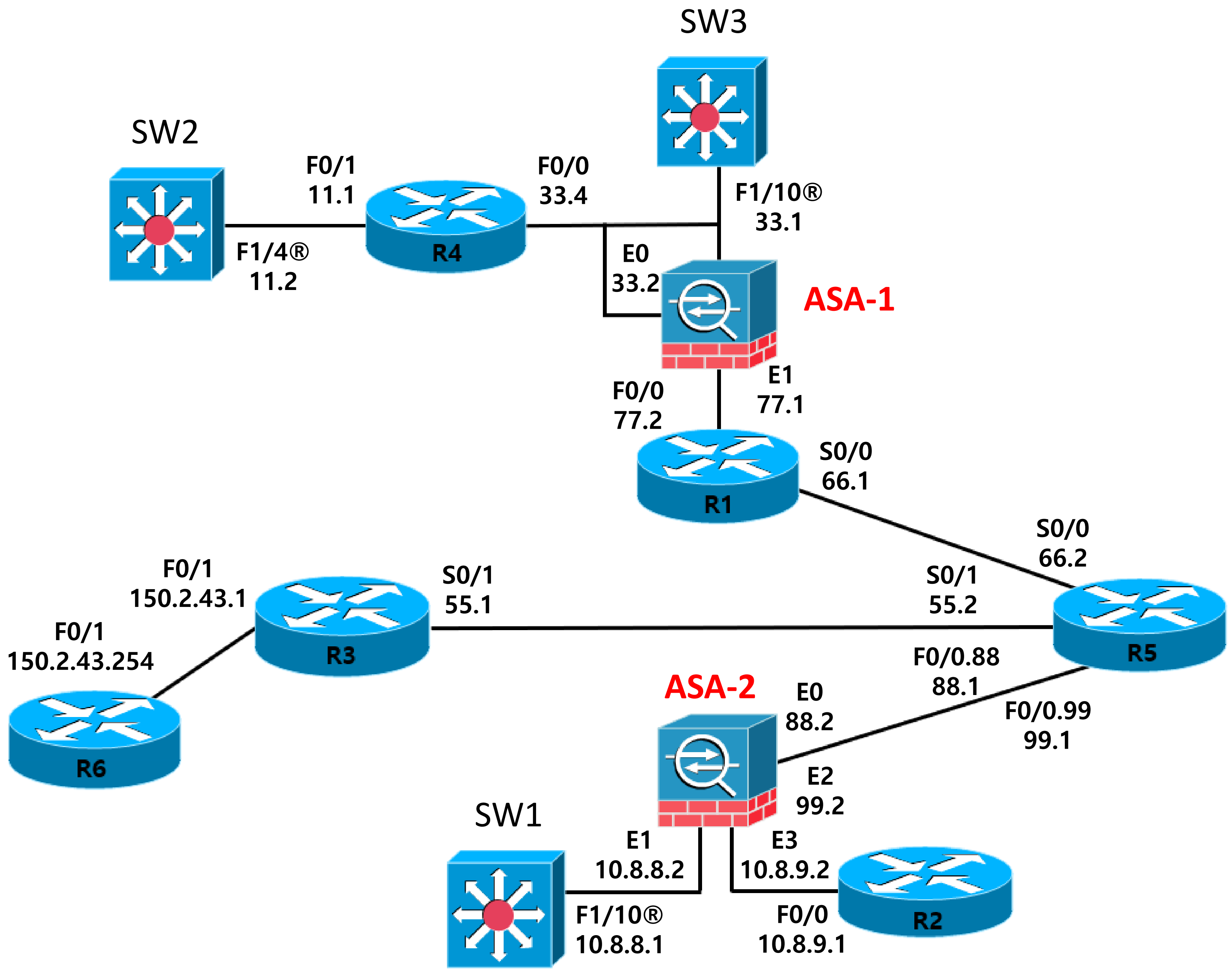
1. 구성도

1-1. 물리적 구성도

1-2. 논리적 구성도

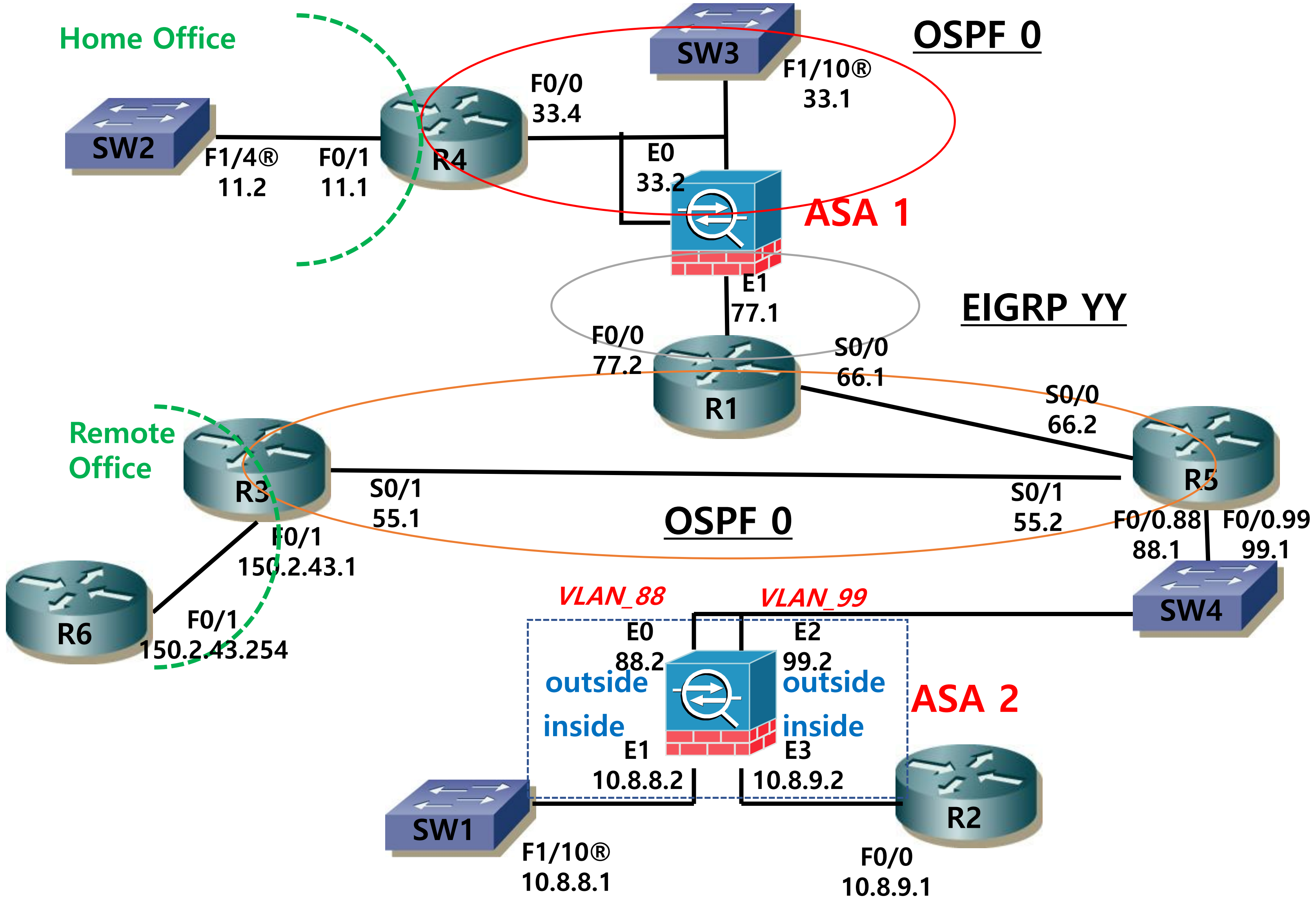
1. 구성도

1-1. 물리적 구성도



1. 구성도

1-2. 논리적 구성도



2

2. 스위치 설정

2-1. SW1

2-2. SW2

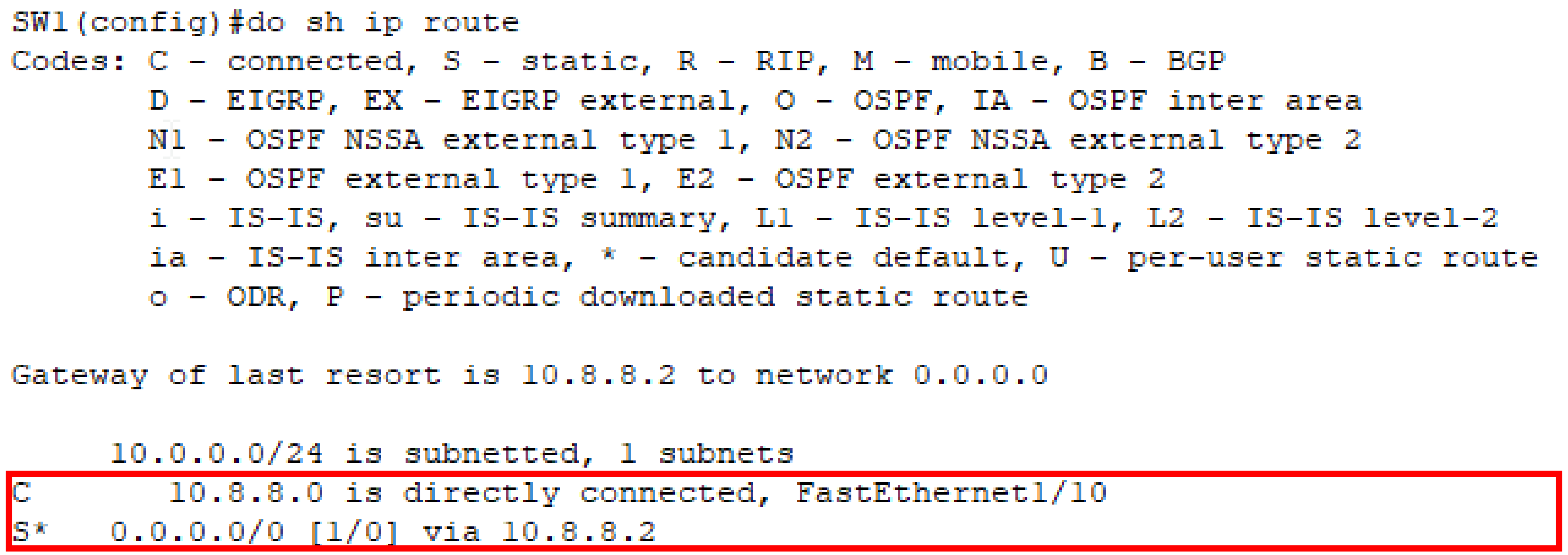
2-3. SW3

2-4. SW4

2. 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
```

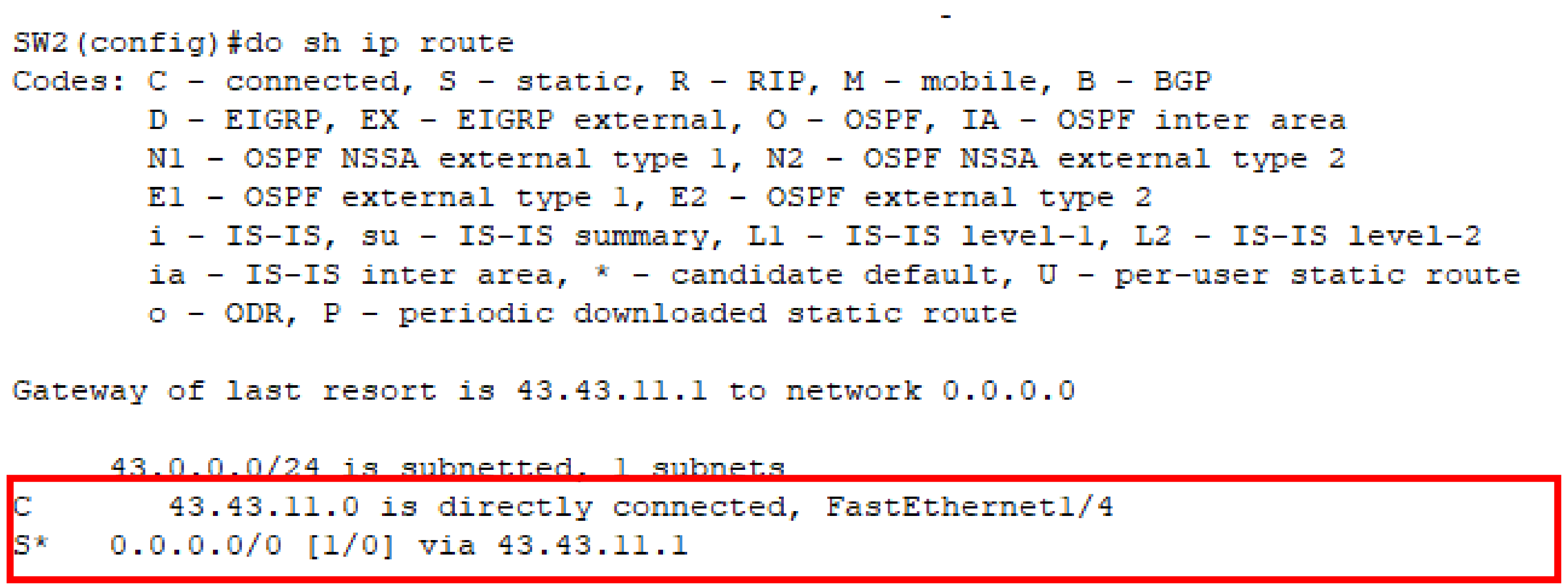


```
SW1(config)#do sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       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. 스위치 설정

2-2. SW2

```
int f1/4
no sw
ip add 43.43.11.2 255.255.255.0
!
ip route 0.0.0.0 0.0.0.0 43.43.11.1
```

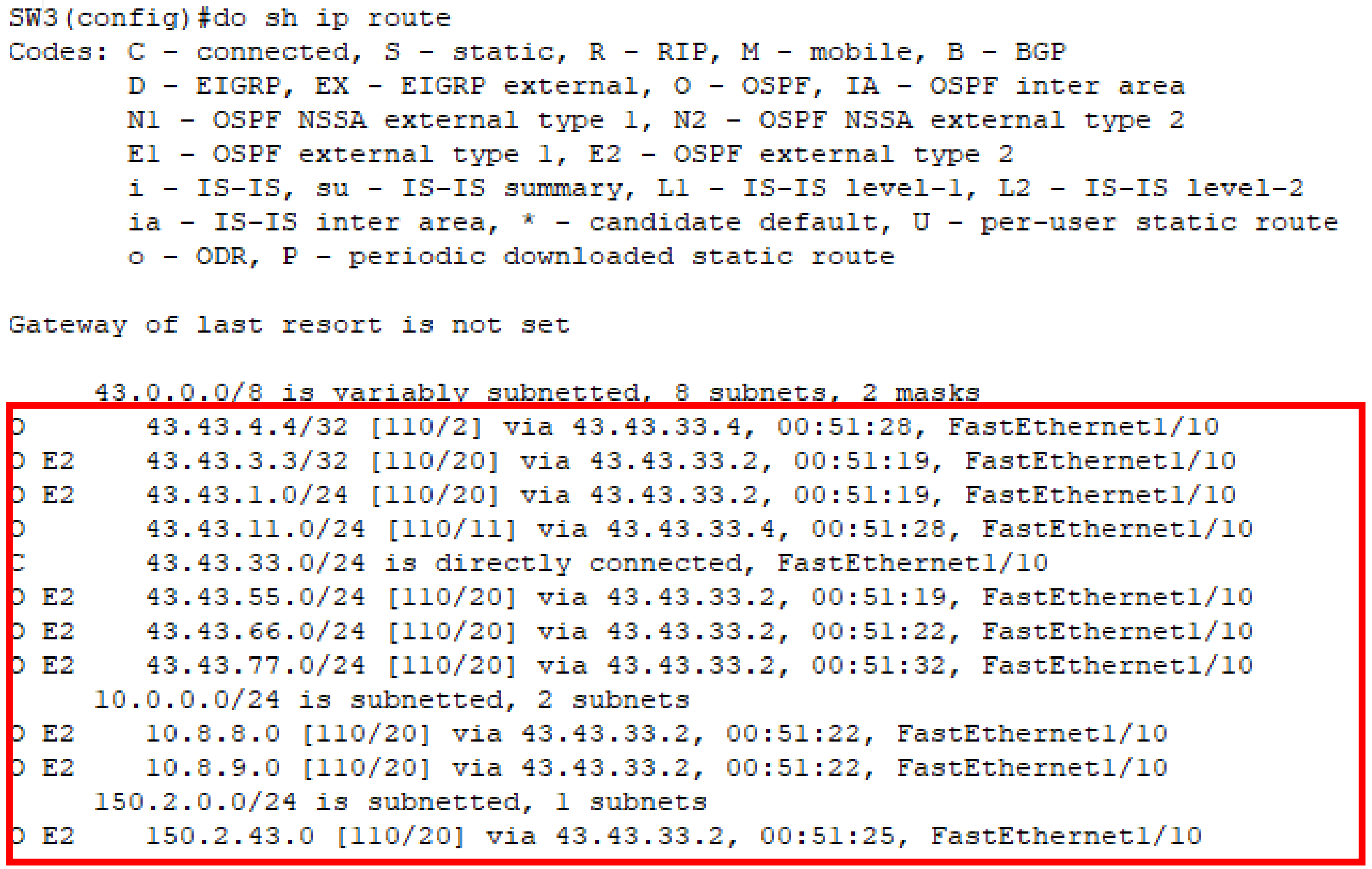


```
SW2(config)#do sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       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 43.43.11.1 to network 0.0.0.0

     43.0.0.0/24 is subnetted, 1 subnets
C       43.43.11.0 is directly connected, FastEthernet1/4
S*   0.0.0.0/0 [1/0] via 43.43.11.1
```

2. 스위치 설정

2-3. SW3

```
int f1/10
no sw
ip add 43.43.33.1 255.255.255.0
!
router os 1
net 43.43.33.1 0.0.0.0 a 0
```

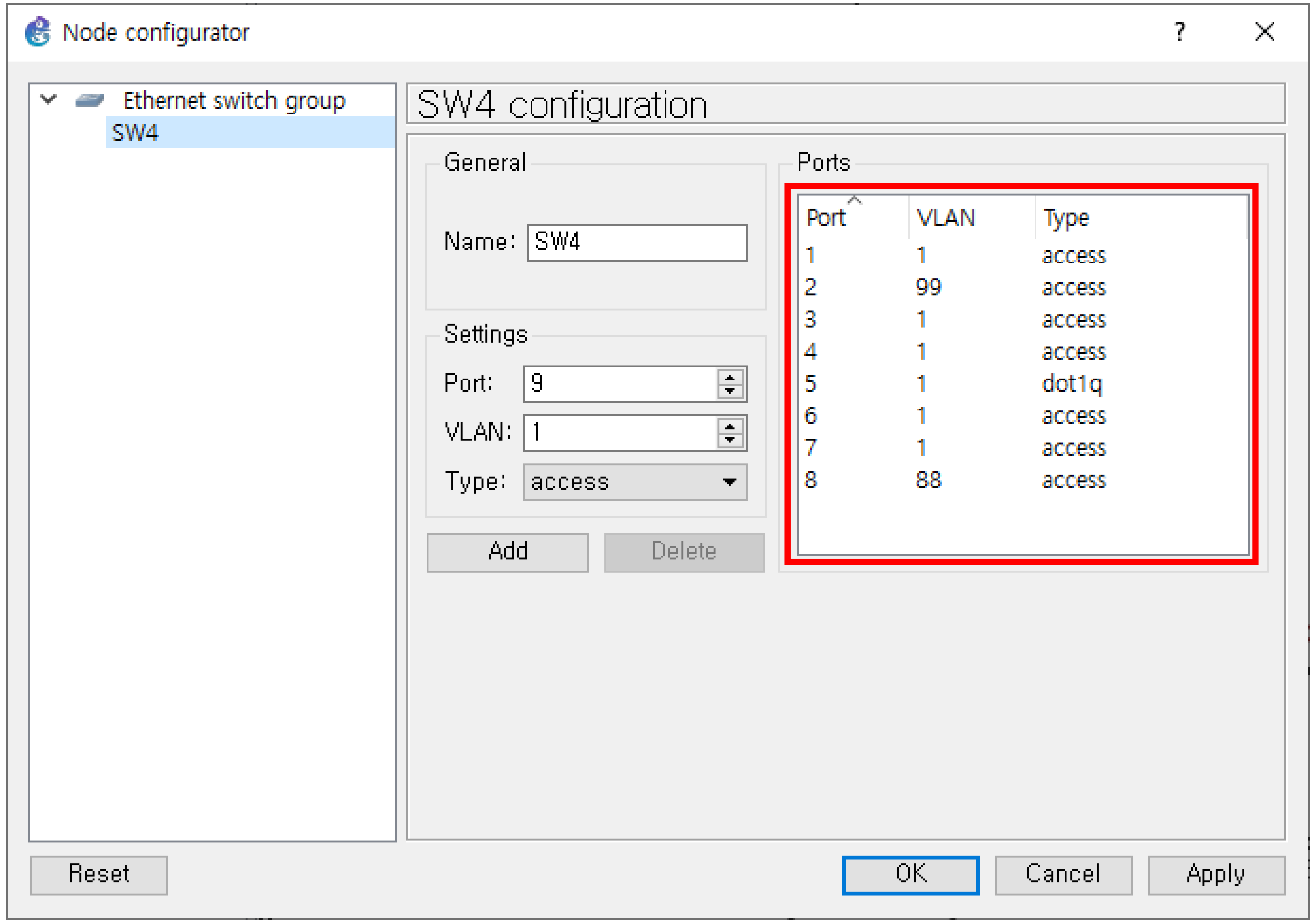


```
SW3(config)#do sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       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

     43.0.0.0/8 is variably subnetted, 8 subnets, 2 masks
O       43.43.4.4/32 [110/2] via 43.43.33.4, 00:51:28, FastEthernet1/10
O E2    43.43.3.3/32 [110/20] via 43.43.33.2, 00:51:19, FastEthernet1/10
O E2    43.43.1.0/24 [110/20] via 43.43.33.2, 00:51:19, FastEthernet1/10
O       43.43.11.0/24 [110/11] via 43.43.33.4, 00:51:28, FastEthernet1/10
C       43.43.33.0/24 is directly connected, FastEthernet1/10
O E2    43.43.55.0/24 [110/20] via 43.43.33.2, 00:51:19, FastEthernet1/10
O E2    43.43.66.0/24 [110/20] via 43.43.33.2, 00:51:22, FastEthernet1/10
O E2    43.43.77.0/24 [110/20] via 43.43.33.2, 00:51:32, FastEthernet1/10
     10.0.0.0/24 is subnetted, 2 subnets
O E2    10.8.8.0 [110/20] via 43.43.33.2, 00:51:22, FastEthernet1/10
O E2    10.8.9.0 [110/20] via 43.43.33.2, 00:51:22, FastEthernet1/10
     150.2.0.0/24 is subnetted, 1 subnets
O E2    150.2.43.0 [110/20] via 43.43.33.2, 00:51:25, FastEthernet1/10
```

2. 스위치 설정

2-4. SW4

```
vlan 88
vlan 99
!
5번 포트 인터페이스
switchport trunk encapsulation dot1q
switchport mode trunk
!
8번 포트 인터페이스
switchport mode access
switchport access vlan 88
!
2번 포트 인터페이스
switchport mode access
switchport access vlan 99
```



SW4 configuration

General

Name: SW4

Settings

Port: 9

VLAN: 1

Type: access

Ports

Port	VLAN	Type
1	1	access
2	99	access
3	1	access
4	1	access
5	1	dot1q
6	1	access
7	1	access
8	88	access

3

3. 라우터 설정

3-1. R1

3-2. R2

3-3. R3

3-4. R4

3-5. R5

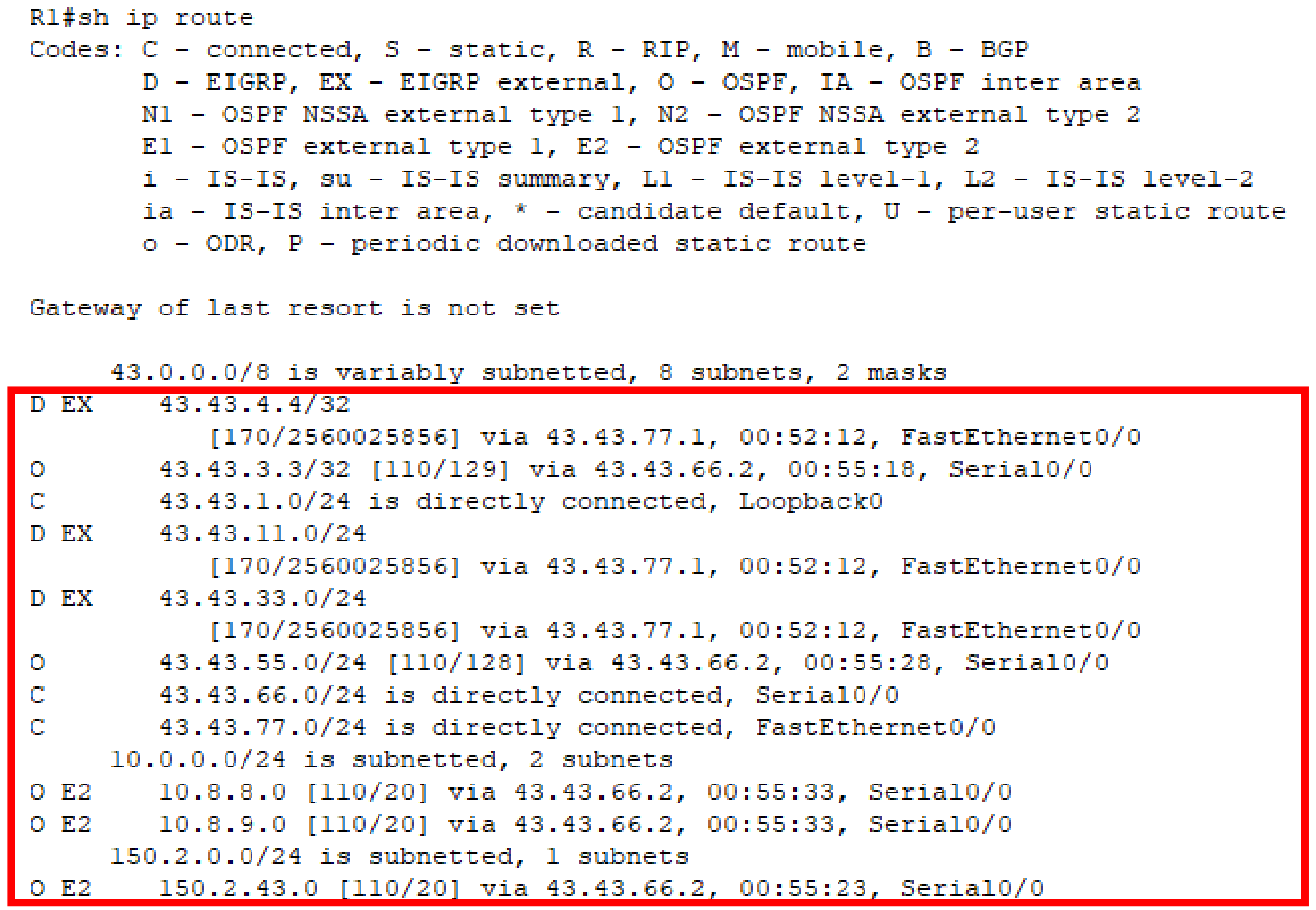
3-6. R6

3. 라우터 설정

3-1. R1

```
int lo0
ip add 43.43.1.1 255.255.255.0
!
int f0/0
no sh
ip add 43.43.77.2 255.255.255.0
!
int s0/0
no sh
ip add 43.43.66.1 255.255.255.0
```

```
router ei 43
no auto
net 43.43.1.1 0.0.0.0
net 43.43.77.2 0.0.0.0
redi os 1 met 1 1 1 1 1
!
router os 1
net 43.43.66.1 0.0.0.0 a 0
default-inf ori always
redi ei 43 sub
```

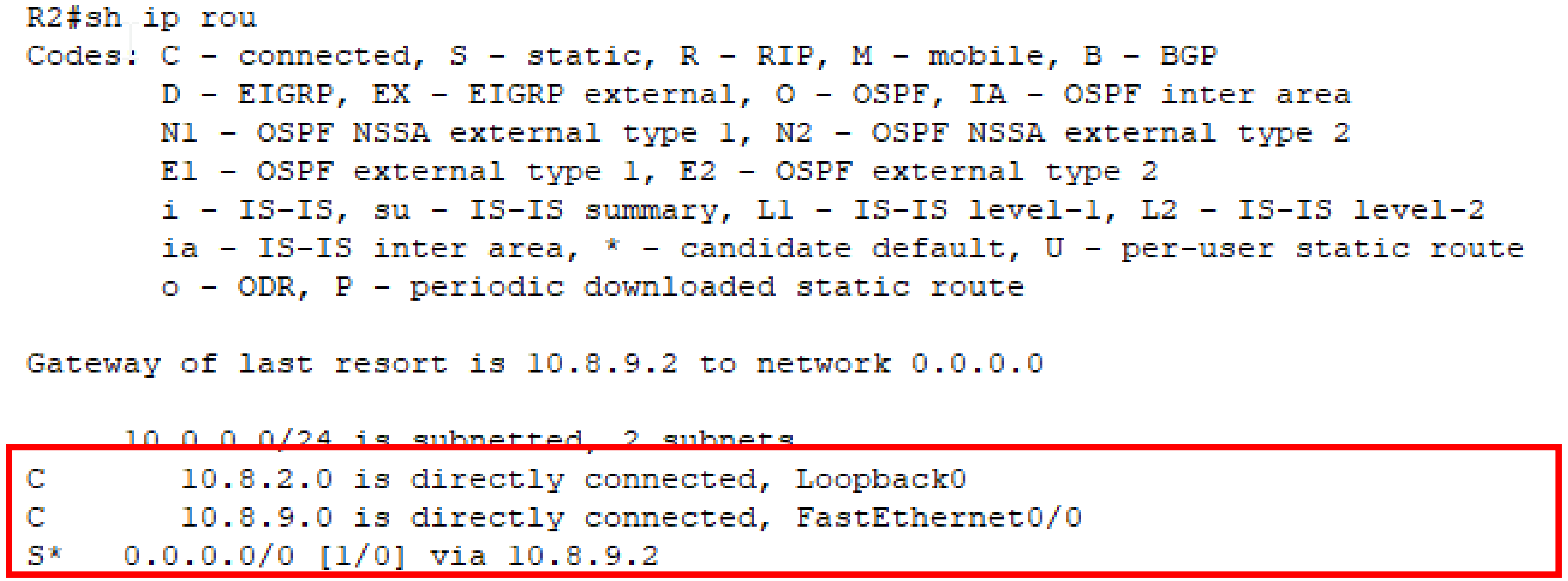


```
R1#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - 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

     43.0.0.0/8 is variably subnetted, 8 subnets, 2 masks
D EX    43.43.4.4/32
           [170/2560025856] via 43.43.77.1, 00:52:12, FastEthernet0/0
O       43.43.3.3/32 [110/129] via 43.43.66.2, 00:55:18, Serial0/0
C       43.43.1.0/24 is directly connected, Loopback0
D EX    43.43.11.0/24
           [170/2560025856] via 43.43.77.1, 00:52:12, FastEthernet0/0
D EX    43.43.33.0/24
           [170/2560025856] via 43.43.77.1, 00:52:12, FastEthernet0/0
O       43.43.55.0/24 [110/128] via 43.43.66.2, 00:55:28, Serial0/0
C       43.43.66.0/24 is directly connected, Serial0/0
C       43.43.77.0/24 is directly connected, FastEthernet0/0
     10.0.0.0/24 is subnetted, 2 subnets
O E2    10.8.8.0 [110/20] via 43.43.66.2, 00:55:33, Serial0/0
O E2    10.8.9.0 [110/20] via 43.43.66.2, 00:55:33, Serial0/0
     150.2.0.0/24 is subnetted, 1 subnets
O E2    150.2.43.0 [110/20] via 43.43.66.2, 00:55:23, Serial0/0
```

3. 라우터 설정

3-2. R2

```
int lo0
ip add 10.8.2.2 255.255.255.0
!
int f0/0
no sh
ip add 10.8.9.1 255.255.255.0
!
ip route 0.0.0.0 0.0.0.0 10.8.9.2
```



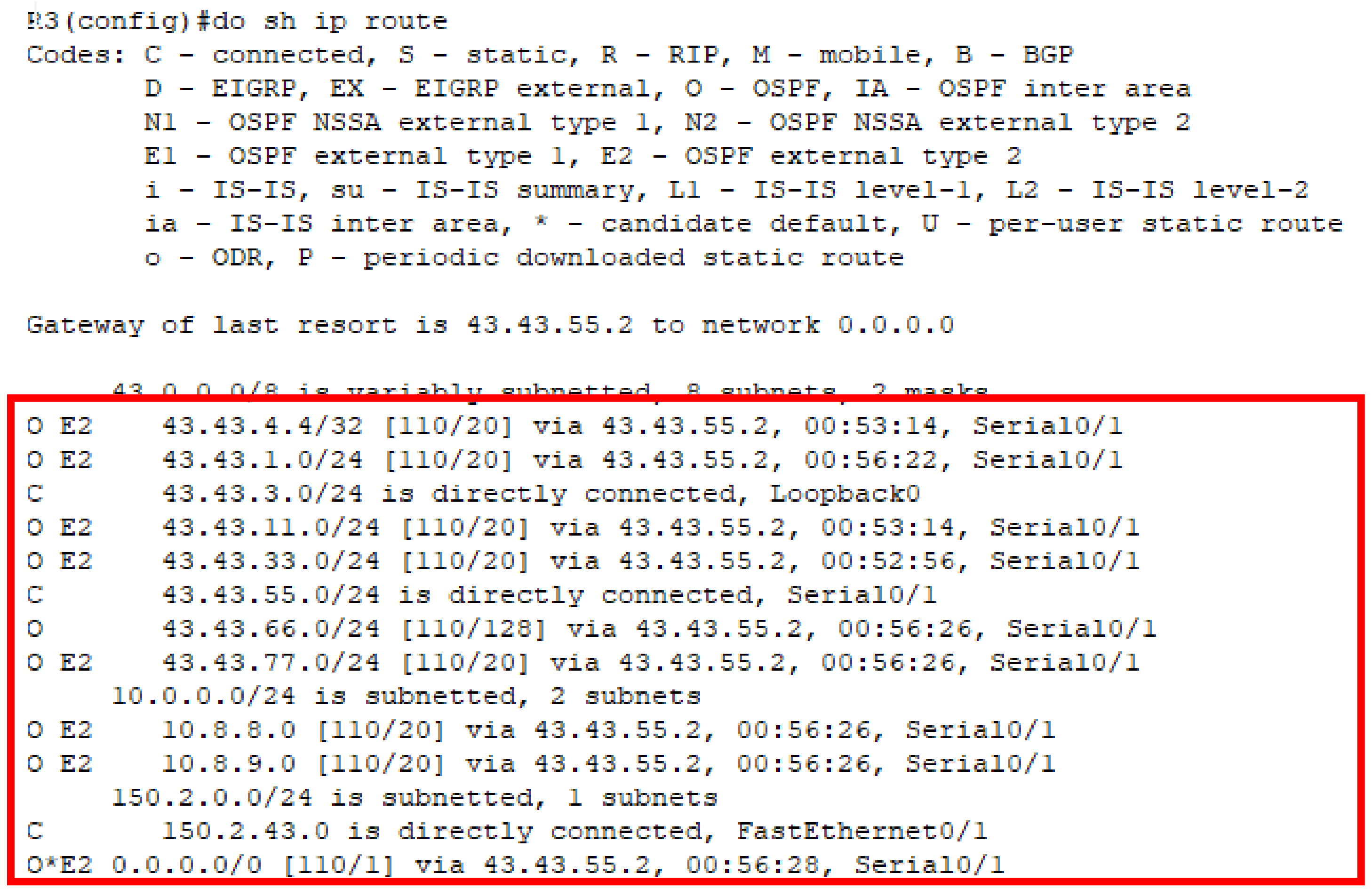
```
R2#sh ip rou
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - 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. 라우터 설정

3-3. R3

```
int lo0
ip add 43.43.3.3 255.255.255.0
!
int s0/1
no sh
ip add 43.43.55.1 255.255.255.0
!
int f0/1
no sh
ip add 150.2.43.1 255.255.255.0
```

```
router os 1
net 43.43.3.3 0.0.0.0 a 0
net 43.43.55.1 0.0.0.0 a 0
redi ei 254 sub
!
router ei 254
no auto
net 150.2.43.1 0.0.0.0
redi os 1 met 1 1 1 1 1
```

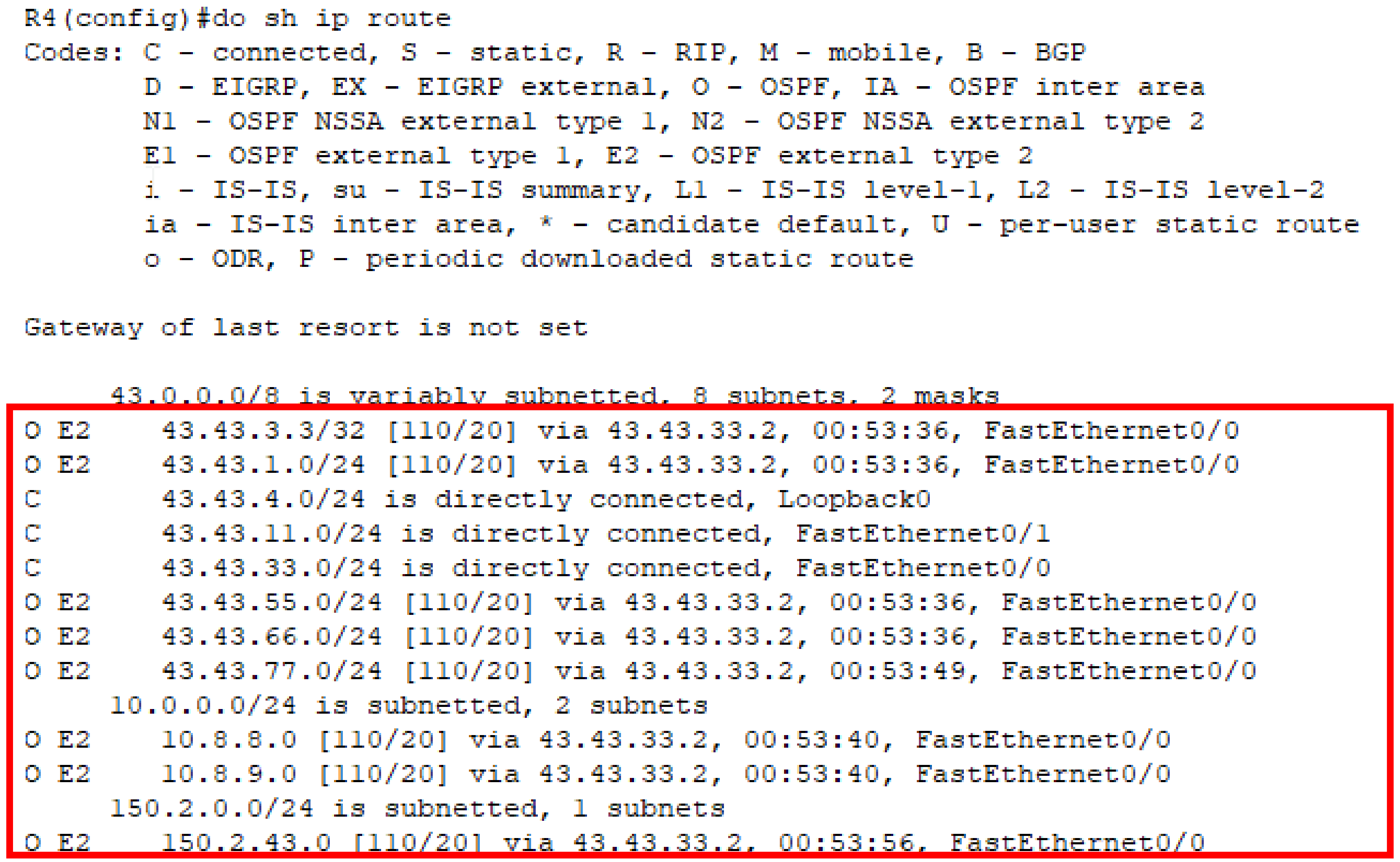


```
R3(config)#do sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - 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 43.43.55.2 to network 0.0.0.0

     43.0.0.0/8 is variably subnetted, 8 subnets, 2 masks
O E2    43.43.4.4/32 [110/20] via 43.43.55.2, 00:53:14, Serial0/1
O E2    43.43.1.0/24 [110/20] via 43.43.55.2, 00:56:22, Serial0/1
C       43.43.3.0/24 is directly connected, Loopback0
O E2    43.43.11.0/24 [110/20] via 43.43.55.2, 00:53:14, Serial0/1
O E2    43.43.33.0/24 [110/20] via 43.43.55.2, 00:52:56, Serial0/1
C       43.43.55.0/24 is directly connected, Serial0/1
O       43.43.66.0/24 [110/128] via 43.43.55.2, 00:56:26, Serial0/1
O E2    43.43.77.0/24 [110/20] via 43.43.55.2, 00:56:26, Serial0/1
     10.0.0.0/24 is subnetted, 2 subnets
O E2    10.8.8.0 [110/20] via 43.43.55.2, 00:56:26, Serial0/1
O E2    10.8.9.0 [110/20] via 43.43.55.2, 00:56:26, 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 43.43.55.2, 00:56:28, Serial0/1
```

3. 라우터 설정

3-4. R4

```
int lo0
ip add 43.43.4.4 255.255.255.0
!
int f0/0
no sh
ip add 43.43.33.4 255.255.255.0
!
int f0/1
no sh
ip add 43.43.11.1 255.255.255.0
!
router os 1
net 43.43.4.4 0.0.0.0 a 0
net 43.43.33.4 0.0.0.0 a 0
net 43.43.11.1 0.0.0.0 a 0
```



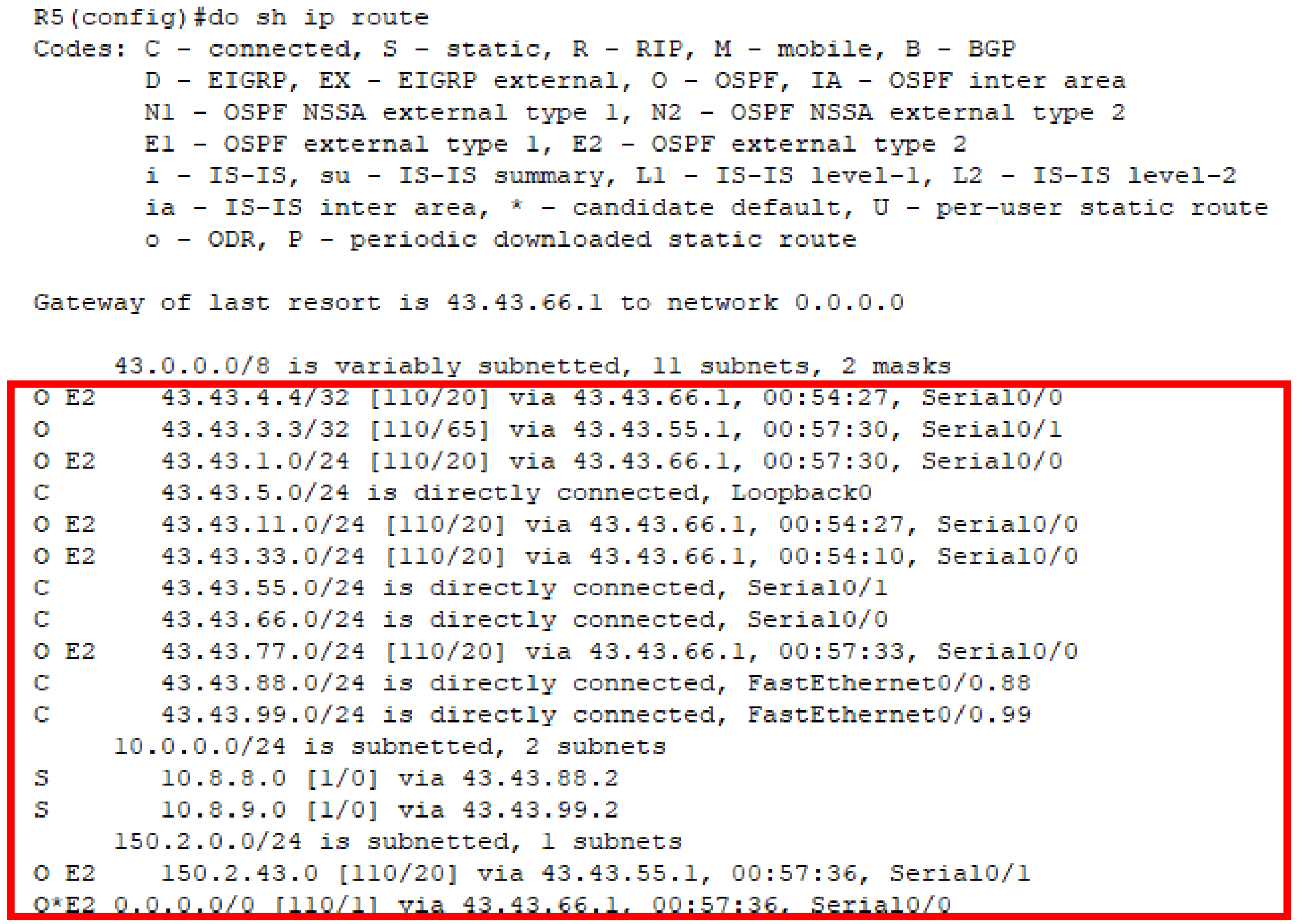
```
R4(config)#do sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - 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

     43.0.0.0/8 is variably subnetted, 8 subnets, 2 masks
O E2    43.43.3.3/32 [110/20] via 43.43.33.2, 00:53:36, FastEthernet0/0
O E2    43.43.1.0/24 [110/20] via 43.43.33.2, 00:53:36, FastEthernet0/0
C       43.43.4.0/24 is directly connected, Loopback0
C       43.43.11.0/24 is directly connected, FastEthernet0/1
C       43.43.33.0/24 is directly connected, FastEthernet0/0
O E2    43.43.55.0/24 [110/20] via 43.43.33.2, 00:53:36, FastEthernet0/0
O E2    43.43.66.0/24 [110/20] via 43.43.33.2, 00:53:36, FastEthernet0/0
O E2    43.43.77.0/24 [110/20] via 43.43.33.2, 00:53:49, FastEthernet0/0
     10.0.0.0/24 is subnetted, 2 subnets
O E2    10.8.8.0 [110/20] via 43.43.33.2, 00:53:40, FastEthernet0/0
O E2    10.8.9.0 [110/20] via 43.43.33.2, 00:53:40, FastEthernet0/0
     150.2.0.0/24 is subnetted, 1 subnets
O E2    150.2.43.0 [110/20] via 43.43.33.2, 00:53:56, FastEthernet0/0
```

3. 라우터 설정

3-5. R5

```
int lo0
ip add 43.43.5.5 255.255.255.0
!
int f0/0
no sh
!
int f0/0.99
en dot 99
ip add 43.43.99.1 255.255.255.0
!
int f0/0.88
en dot 88
ip add 43.43.88.1 255.255.255.0
```

```
int s0/0
no sh
ip add 43.43.66.2 255.255.255.0
!
int s0/1
no sh
ip add 43.43.55.2 255.255.255.0
!
router os 1
net 43.43.55.2 0.0.0.0 a 0
net 43.43.66.2 0.0.0.0 a 0
redi static sub
!
ip route 10.8.8.0 255.255.255.0 43.43.88.2
ip route 10.8.9.0 255.255.255.0 43.43.99.2
```

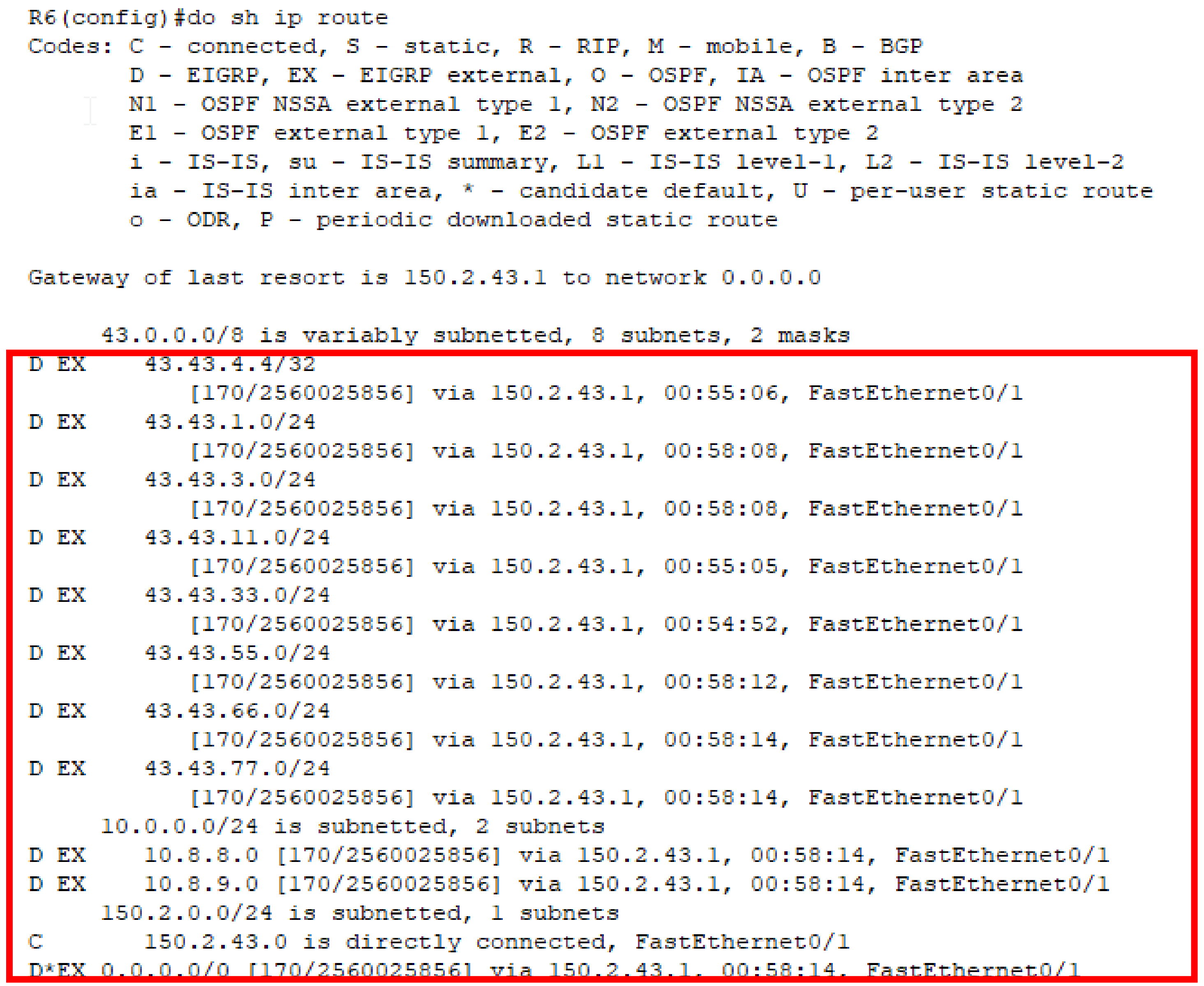


```
R5(config)#do sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - 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 43.43.66.1 to network 0.0.0.0

     43.0.0.0/8 is variably subnetted, 11 subnets, 2 masks
O E2    43.43.4.4/32 [110/20] via 43.43.66.1, 00:54:27, Serial0/0
O       43.43.3.3/32 [110/65] via 43.43.55.1, 00:57:30, Serial0/1
O E2    43.43.1.0/24 [110/20] via 43.43.66.1, 00:57:30, Serial0/0
C       43.43.5.0/24 is directly connected, Loopback0
O E2    43.43.11.0/24 [110/20] via 43.43.66.1, 00:54:27, Serial0/0
O E2    43.43.33.0/24 [110/20] via 43.43.66.1, 00:54:10, Serial0/0
C       43.43.55.0/24 is directly connected, Serial0/1
C       43.43.66.0/24 is directly connected, Serial0/0
O E2    43.43.77.0/24 [110/20] via 43.43.66.1, 00:57:33, Serial0/0
C       43.43.88.0/24 is directly connected, FastEthernet0/0.88
C       43.43.99.0/24 is directly connected, FastEthernet0/0.99
     10.0.0.0/24 is subnetted, 2 subnets
S       10.8.8.0 [1/0] via 43.43.88.2
S       10.8.9.0 [1/0] via 43.43.99.2
     150.2.0.0/24 is subnetted, 1 subnets
O E2    150.2.43.0 [110/20] via 43.43.55.1, 00:57:36, Serial0/1
O*E2 0.0.0.0/0 [110/1] via 43.43.66.1, 00:57:36, Serial0/0
```

3. 라우터 설정

3-6. R6

```
int f0/1
no sh
ip add 150.2.43.254 255.255.255.0
!
router ei 254
no auto
net 150.2.43.254 0.0.0.0
```



```
R6(config)#do 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 150.2.43.1 to network 0.0.0.0

     43.0.0.0/8 is variably subnetted, 8 subnets, 2 masks
D EX    43.43.4.4/32
           [170/2560025856] via 150.2.43.1, 00:55:06, FastEthernet0/1
D EX    43.43.1.0/24
           [170/2560025856] via 150.2.43.1, 00:58:08, FastEthernet0/1
D EX    43.43.3.0/24
           [170/2560025856] via 150.2.43.1, 00:58:08, FastEthernet0/1
D EX    43.43.11.0/24
           [170/2560025856] via 150.2.43.1, 00:55:05, FastEthernet0/1
D EX    43.43.33.0/24
           [170/2560025856] via 150.2.43.1, 00:54:52, FastEthernet0/1
D EX    43.43.55.0/24
           [170/2560025856] via 150.2.43.1, 00:58:12, FastEthernet0/1
D EX    43.43.66.0/24
           [170/2560025856] via 150.2.43.1, 00:58:14, FastEthernet0/1
D EX    43.43.77.0/24
           [170/2560025856] via 150.2.43.1, 00:58:14, FastEthernet0/1
     10.0.0.0/24 is subnetted, 2 subnets
D EX    10.8.8.0 [170/2560025856] via 150.2.43.1, 00:58:14, FastEthernet0/1
D EX    10.8.9.0 [170/2560025856] via 150.2.43.1, 00:58:14, 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, 00:58:14, FastEthernet0/1
```

4

4. 방화벽-1 설정

4-1. Redundant 1

4-2. 인터페이스 설정

4-3. 라우팅

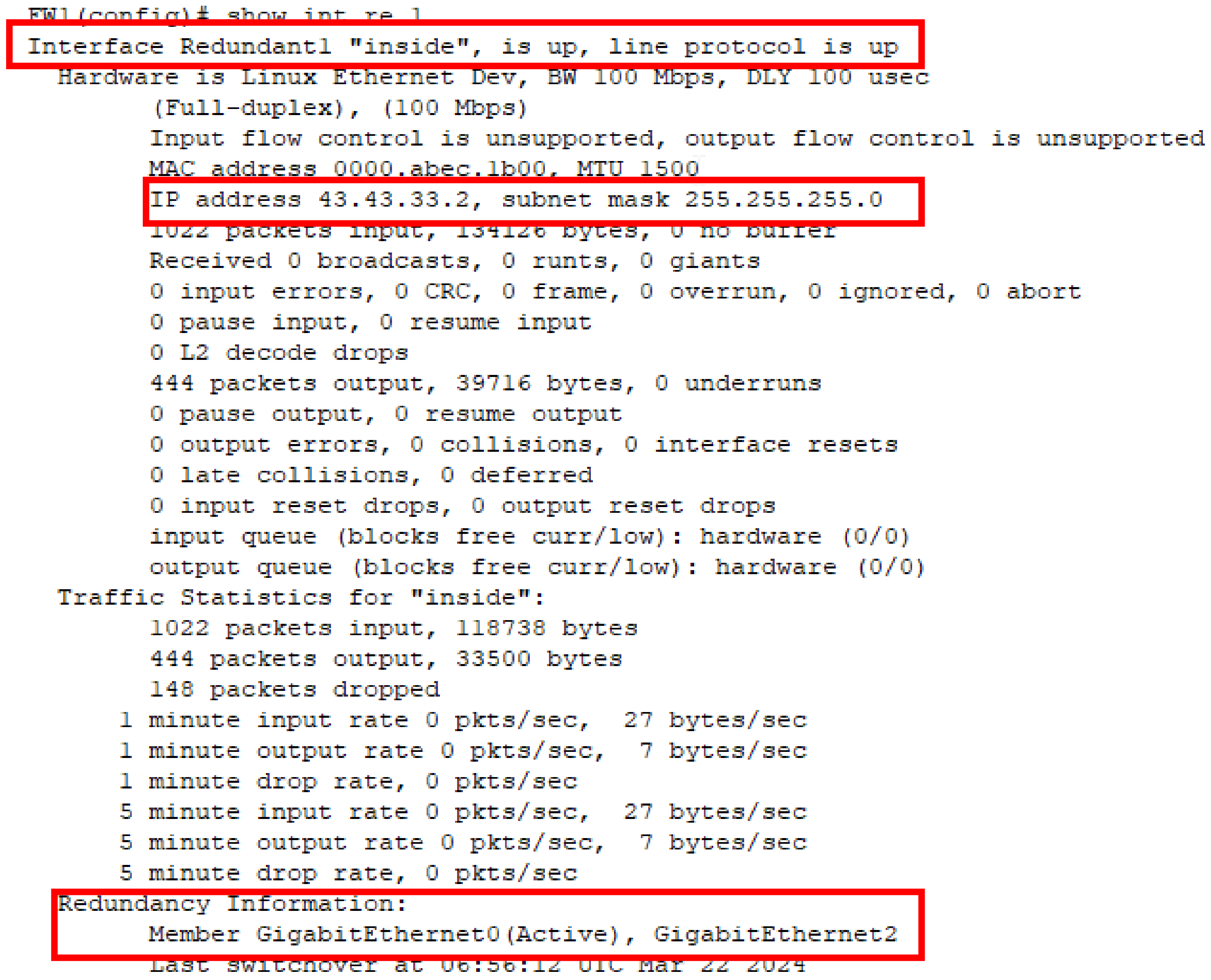
4-4. MPF

4. 방화벽-1 설정

4-1. Redundant 1

ASA redundant 구성은 Active/Standby 또는 Active/Active 구성으로 구현된다.
Active/Standby 구성에서는 하나의 ASA가 활성(active)으로 동작하고, 다른 하나는 대기(standby) 모드에 있다.
활성 ASA에 장애가 발생하면 대기 모드에 있는 ASA가 자동으로 활성화되어 서비스 중단을 방지한다.

```
int re 1
member-int g0
member-int g2
nameif inside
ip add 43.43.33.2 255.255.255.0
```



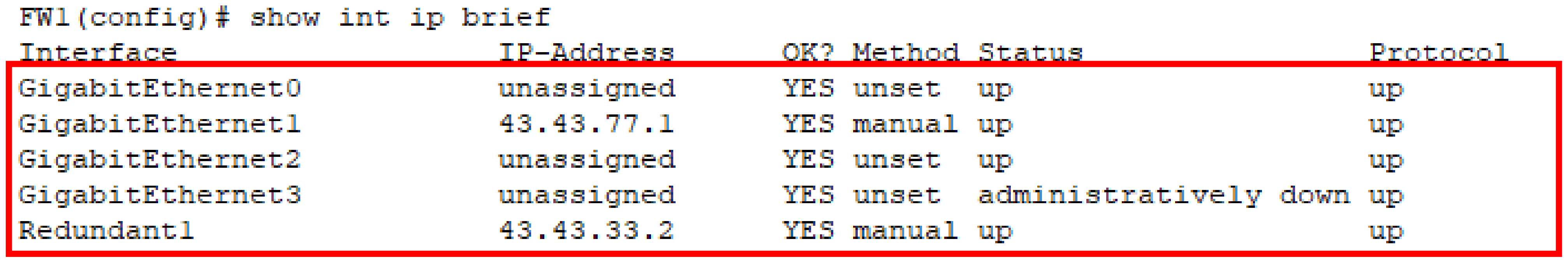
```
FW1(config)# show int re 1
Interface Redundant1 "inside", is up, line protocol is up
  Hardware is Linux Ethernet Dev, BW 100 Mbps, DLY 100 usec
        (Full-duplex), (100 Mbps)
        Input flow control is unsupported, output flow control is unsupported
        MAC address 0000.abec.1b00, MTU 1500
        IP address 43.43.33.2, subnet mask 255.255.255.0
        1022 packets input, 134126 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 pause input, 0 resume input
        0 L2 decode drops
        444 packets output, 39716 bytes, 0 underruns
        0 pause output, 0 resume output
        0 output errors, 0 collisions, 0 interface resets
        0 late collisions, 0 deferred
        0 input reset drops, 0 output reset drops
        input queue (blocks free curr/low): hardware (0/0)
        output queue (blocks free curr/low): hardware (0/0)
  Traffic Statistics for "inside":
        1022 packets input, 118738 bytes
        444 packets output, 33500 bytes
        148 packets dropped
      1 minute input rate 0 pkts/sec,  27 bytes/sec
      1 minute output rate 0 pkts/sec,  7 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  27 bytes/sec
      5 minute output rate 0 pkts/sec,  7 bytes/sec
      5 minute drop rate, 0 pkts/sec
  Redundancy Information:
        Member GigabitEthernet0(Active), GigabitEthernet2
        Last switchover at 06:56:12 UTC Mar 22 2024
```

4. 방화벽-1 설정

4-2. 인터페이스 설정

```
int g0
no sh
!
int g1
no sh
!
int g2
no sh
!
```

```
int re 1
member-int g0
member-int g2
nameif inside
ip add 43.43.33.2 255.255.255.0
!
int g1
nameif outside
ip add 43.43.77.1 255.255.255.0
```

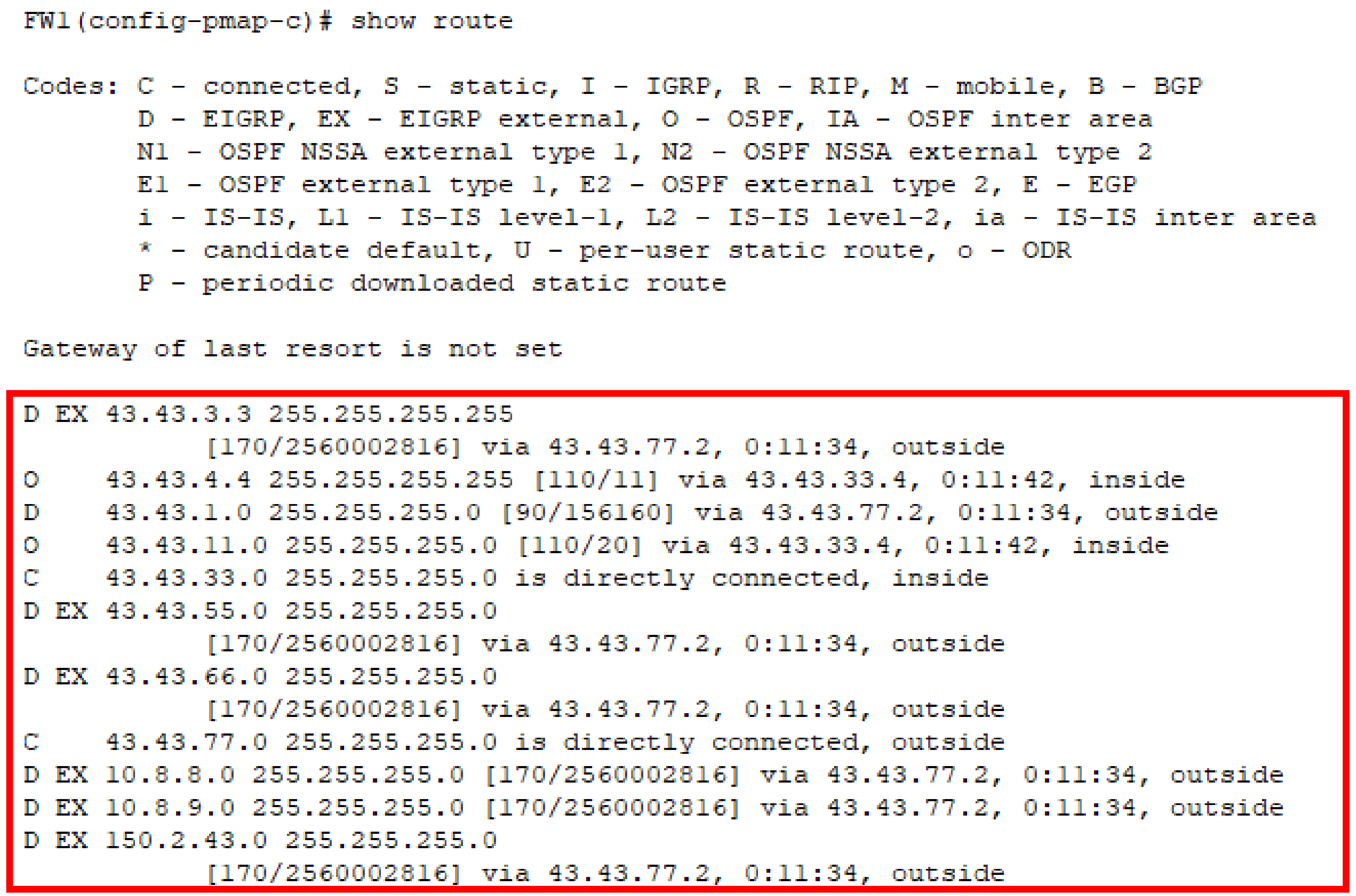


```
FW1(config)# show int ip brief
Interface                  IP-Address      OK? Method Status                Protocol
GigabitEthernet0           unassigned      YES unset  up                    up
GigabitEthernet1           43.43.77.1      YES manual up                    up
GigabitEthernet2           unassigned      YES unset  up                    up
GigabitEthernet3           unassigned      YES unset  administratively down up
Redundant1                 43.43.33.2      YES manual up                    up
```

4. 방화벽-1 설정

4-3. 라우팅

```
router os 1
net 43.43.33.2 255.255.255.255 a 0
redi ei 43 sub
!
router ei 43
no auto
net 43.43.77.1 255.255.255.255
redi os 1 met 1 1 1 1 1
```



```
FW1(config-pmap-c)# show 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

D EX 43.43.3.3 255.255.255.255
           [170/2560002816] via 43.43.77.2, 0:11:34, outside
O    43.43.4.4 255.255.255.255 [110/11] via 43.43.33.4, 0:11:42, inside
D    43.43.1.0 255.255.255.0 [90/156160] via 43.43.77.2, 0:11:34, outside
O    43.43.11.0 255.255.255.0 [110/20] via 43.43.33.4, 0:11:42, inside
C    43.43.33.0 255.255.255.0 is directly connected, inside
D EX 43.43.55.0 255.255.255.0
           [170/2560002816] via 43.43.77.2, 0:11:34, outside
D EX 43.43.66.0 255.255.255.0
           [170/2560002816] via 43.43.77.2, 0:11:34, outside
C    43.43.77.0 255.255.255.0 is directly connected, outside
D EX 10.8.8.0 255.255.255.0 [170/2560002816] via 43.43.77.2, 0:11:34, outside
D EX 10.8.9.0 255.255.255.0 [170/2560002816] via 43.43.77.2, 0:11:34, outside
D EX 150.2.43.0 255.255.255.0
           [170/2560002816] via 43.43.77.2, 0:11:34, outside
```

4. 방화벽-1 설정

4-4. MPF

class-map inspection_default -> 클래스 맵 설정 (트래픽을 분류)

match default-inspection-traffic -> 기본적으로 정해진 트래픽을 지정한다.

policy-map global_policy -> 폴리시 맵 설정 (트래픽에 대한 보안 정책 설정)

class inspection_default

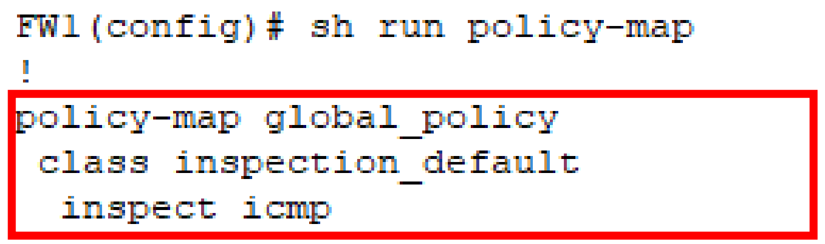
service-policy global_policy global -> 폴리시 맵 활성화

global 키워드를 사용하여 폴리시 맵을 활성화 하면, 해당 폴리시 맵이 글로벌 정책으로 동작한다.
글로벌 정책은 모든 인터페이스에 적용되며, 패킷을 수신할 때만 정책을 검사한다.

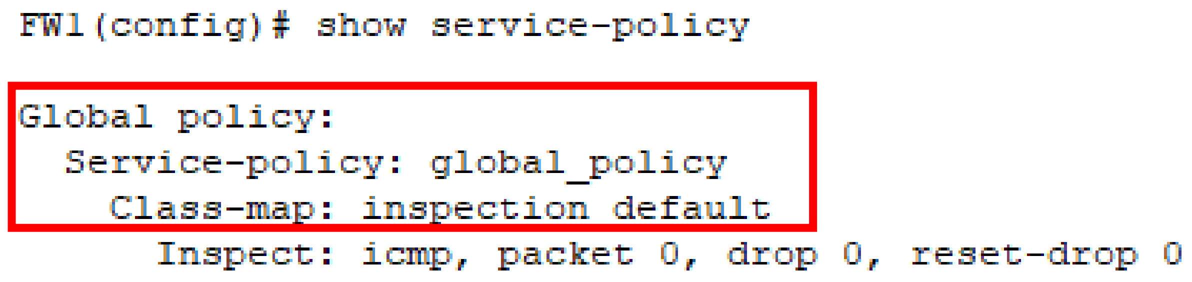
policy-map global_policy

class inspection_default

inspect icmp -> ICMP 패킷 검사



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



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

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

5

5. 방화벽-2 설정

5-1. Active Key 설정

5-2. Context 설정

5-3. ACL

5-4. 라우팅

5-5. Object NAT

5. 방화벽-2 설정

5-1. Active Key 설정

Activation-Key
: **activation-key 0x4a3ec071 0x0d86fbf6 0x7cb1bc48 0x8b48b8b0 0xf317c0b5**

Activation-key 입력 후,

reload 입력

재부팅 되면,

mode multiple 입력

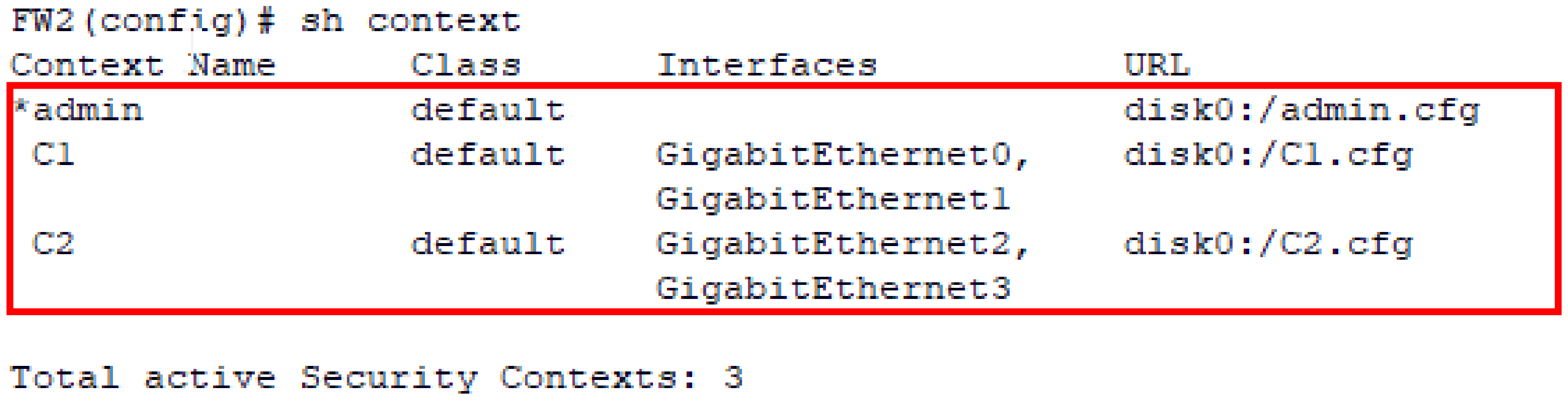
(자동 재부팅)

5. 방화벽-2 설정

5-2. Context 설정

```
int g0
no sh
!
int g1
no sh
!
int g2
no sh
!
int g3
no sh
```

```
admin-context admin
context admin
config-u admin.cfg
!
context C1
config-u C1.cfg
allocate-int g0 outside
allocate-int g1 inside
!
context C2
config-u C2.cfg
allocate-int g2 outside
allocate-int g3 inside
```



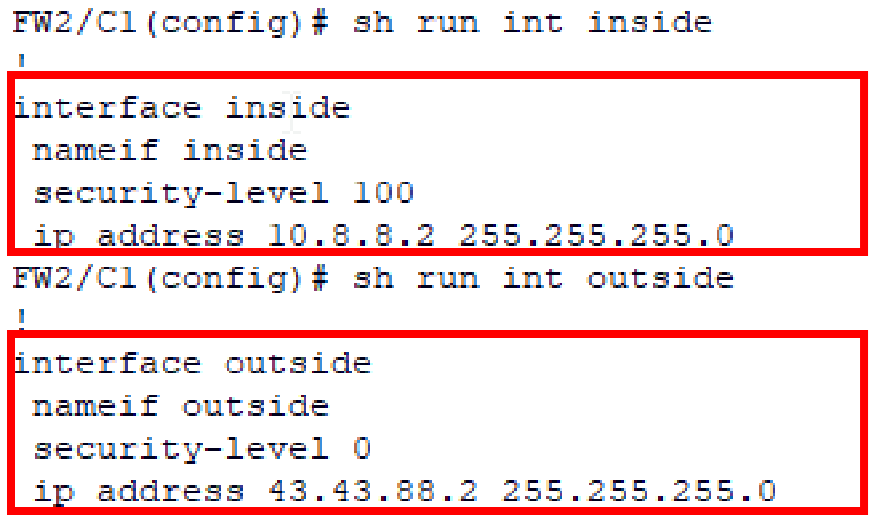
```
FW2(config)# sh context
Context Name      Class      Interfaces           URL
*admin            default                         disk0:/admin.cfg
 C1               default    GigabitEthernet0,    disk0:/C1.cfg
                             GigabitEthernet1
 C2               default    GigabitEthernet2,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

Total active Security Contexts: 3
```

5. 방화벽-2 설정

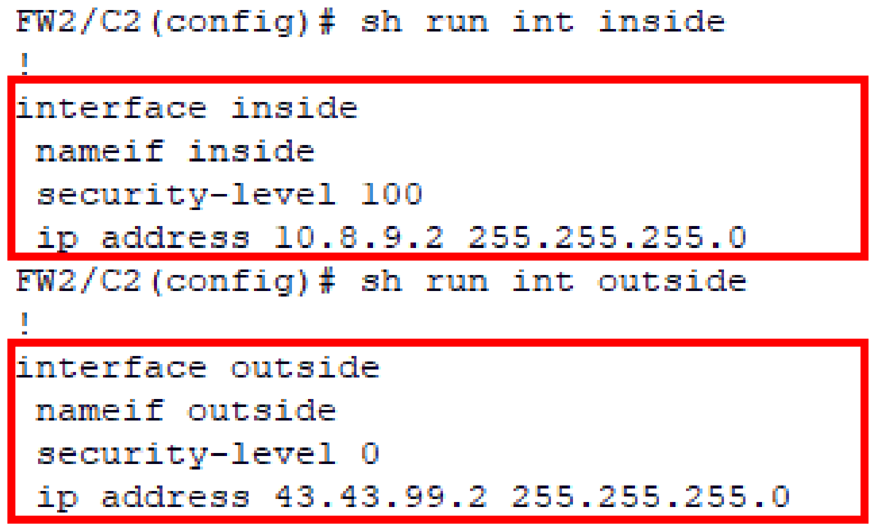
5-2. Context 설정

```
ch con C1
!
int outside
nameif outside
ip add 43.43.88.2 255.255.255.0
!
int inside
nameif inside
ip add 10.8.8.2 255.255.255.0
```

```
ch con C2
!
int outside
nameif outside
ip add 43.43.99.2 255.255.255.0
!
int inside
nameif inside
ip add 10.8.9.2 255.255.255.0
```



```
FW2/C1(config)# sh run int inside
!
interface inside
 nameif inside
 security-level 100
 ip address 10.8.8.2 255.255.255.0
FW2/C1(config)# sh run int outside
!
interface outside
 nameif outside
 security-level 0
 ip address 43.43.88.2 255.255.255.0
```



```
FW2/C2(config)# sh run int inside
!
interface inside
 nameif inside
 security-level 100
 ip address 10.8.9.2 255.255.255.0
FW2/C2(config)# sh run int outside
!
interface outside
 nameif outside
 security-level 0
 ip address 43.43.99.2 255.255.255.0
```

5. 방화벽-2 설정

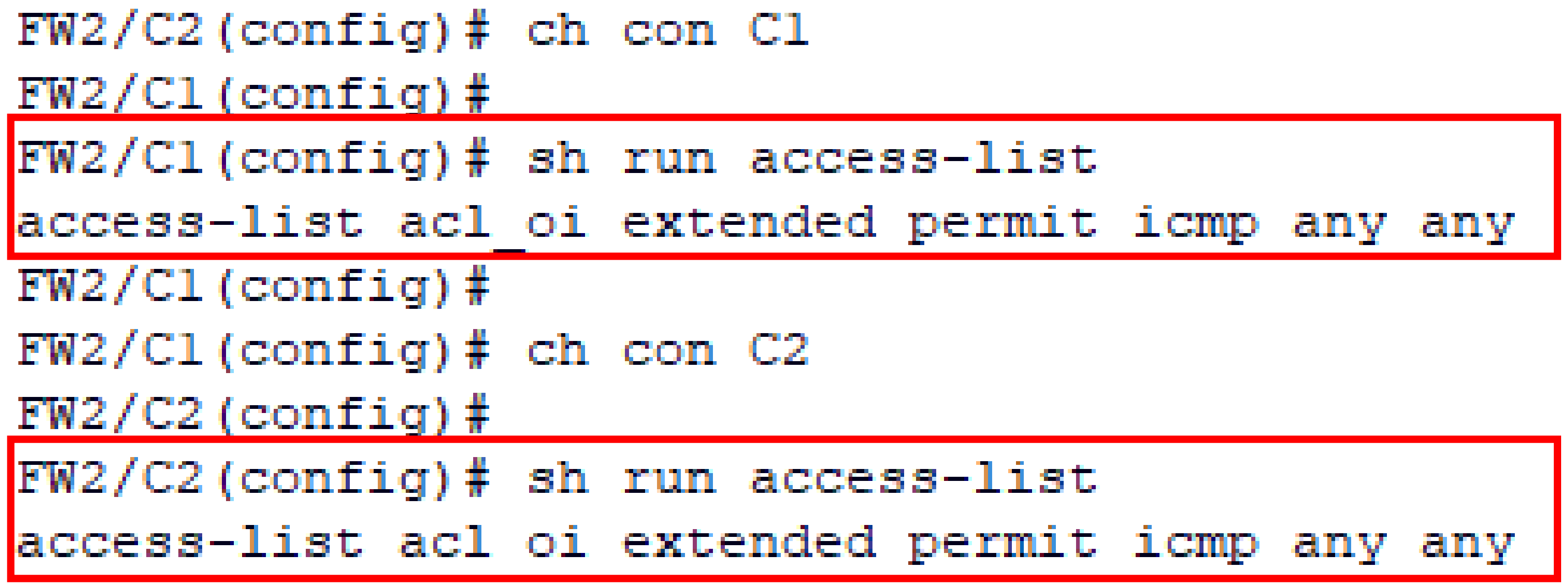
5-3. ACL

Context C1, C2의 외부에서 내부 - ICMP 패킷 허용

< C1, C2 >

access-l acl_oi per icmp a a

access-g acl_oi in int outside



```
FW2/C2(config)# ch con C1
FW2/C1(config)#
FW2/C1(config)# sh run access-list
access-list acl_oi extended permit icmp any any
FW2/C1(config)#
FW2/C1(config)# ch con C2
FW2/C2(config)#
FW2/C2(config)# sh run access-list
access-list acl oi extended permit icmp any any
```

5. 방화벽-2 설정

5-4. 라우팅

< C1 >

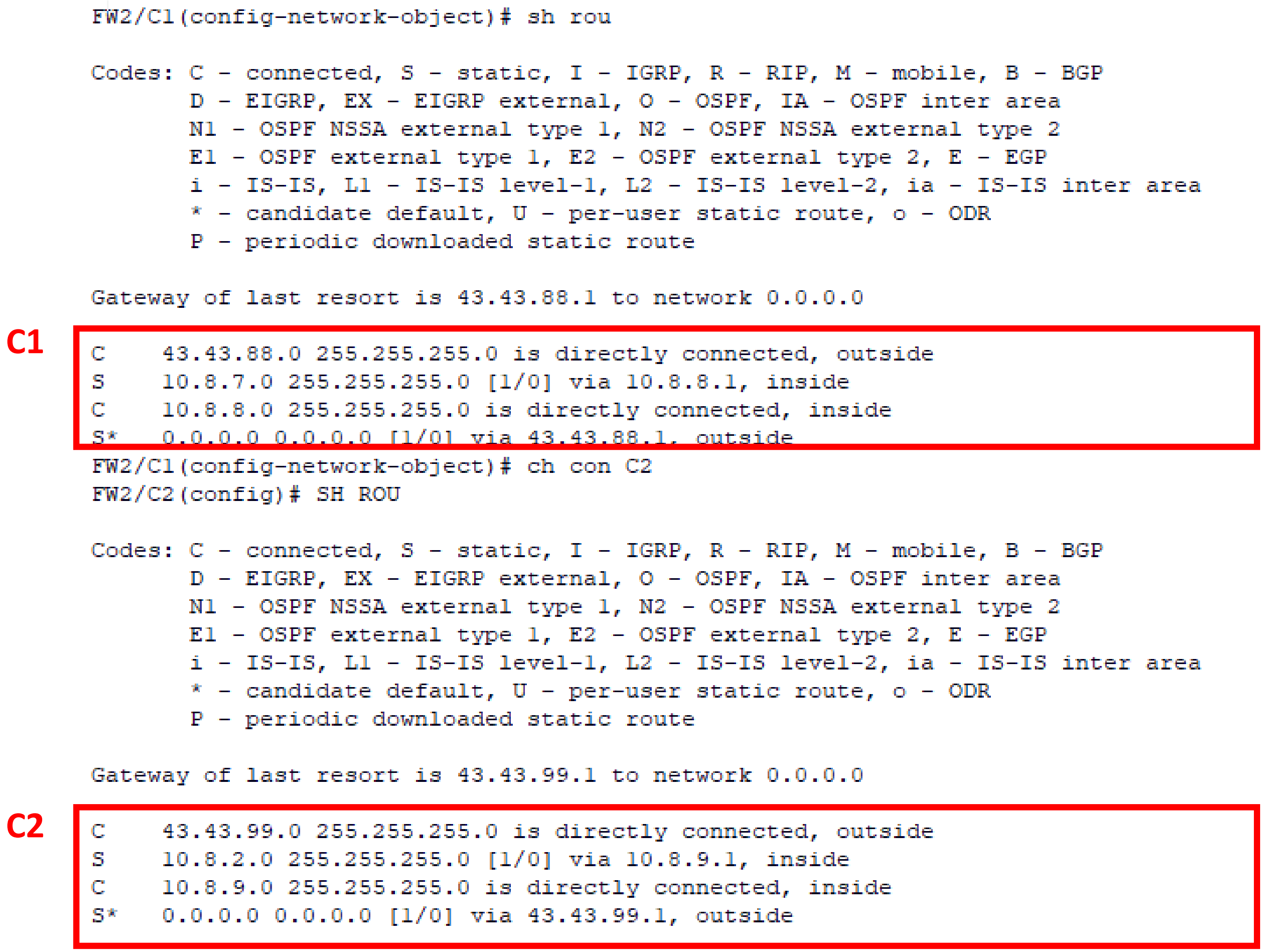
route outside 0 0 43.43.88.1

route inside 10.8.7.0 255.255.255.0 10.8.8.1

< C2 >

route outside 0 0 43.43.99.1

route inside 10.8.2.0 255.255.255.0 10.8.9.1



```
FW2/C1(config-network-object)# sh rou

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 43.43.88.1 to network 0.0.0.0

C    43.43.88.0 255.255.255.0 is directly connected, outside
S    10.8.7.0 255.255.255.0 [1/0] via 10.8.8.1, inside
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 43.43.88.1, outside
FW2/C1(config-network-object)# ch con C2
FW2/C2(config)# SH ROU

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 43.43.99.1 to network 0.0.0.0

C    43.43.99.0 255.255.255.0 is directly connected, outside
S    10.8.2.0 255.255.255.0 [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 43.43.99.1, outside
```

5. 방화벽-2 설정

5-5. Object NAT

Static Object NAT은 내부의 실제 IP(사설 IP) 주소를 외부에 있는 목적지까지 라우팅 가능한 IP(공인 IP) 주소로 변환시키거나, 외부에서 내부의 사설 IP 주소를 가진 서버와 통신할 수 있도록 해준다.
Dynamic Object NAT은 내부의 IP가 외부로 나갈 때 미리 설정된 IP Pool을 이용하여 주소를 변환해 통신한다.

< C1 >

object network inside_Server

host 10.8.7.7 (host는 특정 호스트를 지정)

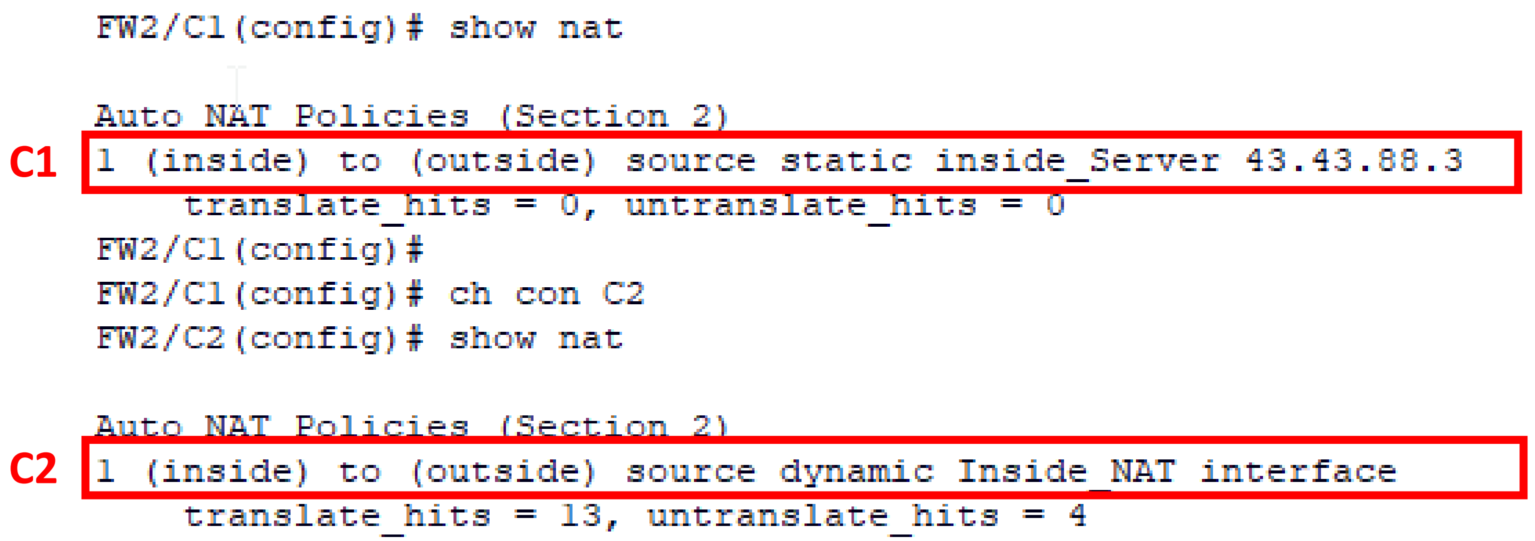
nat (inside,outside) static 43.43.88.3 (static = 정적)

< C2 >

object network Inside_NAT

subnet 10.8.0.0 255.255.0.0 (subnet은 IP 서브넷 마스크를 사용하여 IP 대역을 지정)

nat (inside,outside) dynamic interface (dynamic = 동적)



```
FW2/C1(config)# show nat

Auto NAT Policies (Section 2)
1 (inside) to (outside) source static inside_Server 43.43.88.3
    translate_hits = 0, untranslate_hits = 0
FW2/C1(config)#
FW2/C1(config)# ch con C2
FW2/C2(config)# show nat

Auto NAT Policies (Section 2)
1 (inside) to (outside) source dynamic Inside_NAT interface
    translate_hits = 13, untranslate_hits = 4
```

THANK YOU

대우능력개발원

DAEWOO DEVELOPMENT OP ABILITY