Firewall Project

JLJL Team

이성근 이창훈

장기헌 진이현

대우직업능력개발원
Daewoo Development Institute for Vocational ability

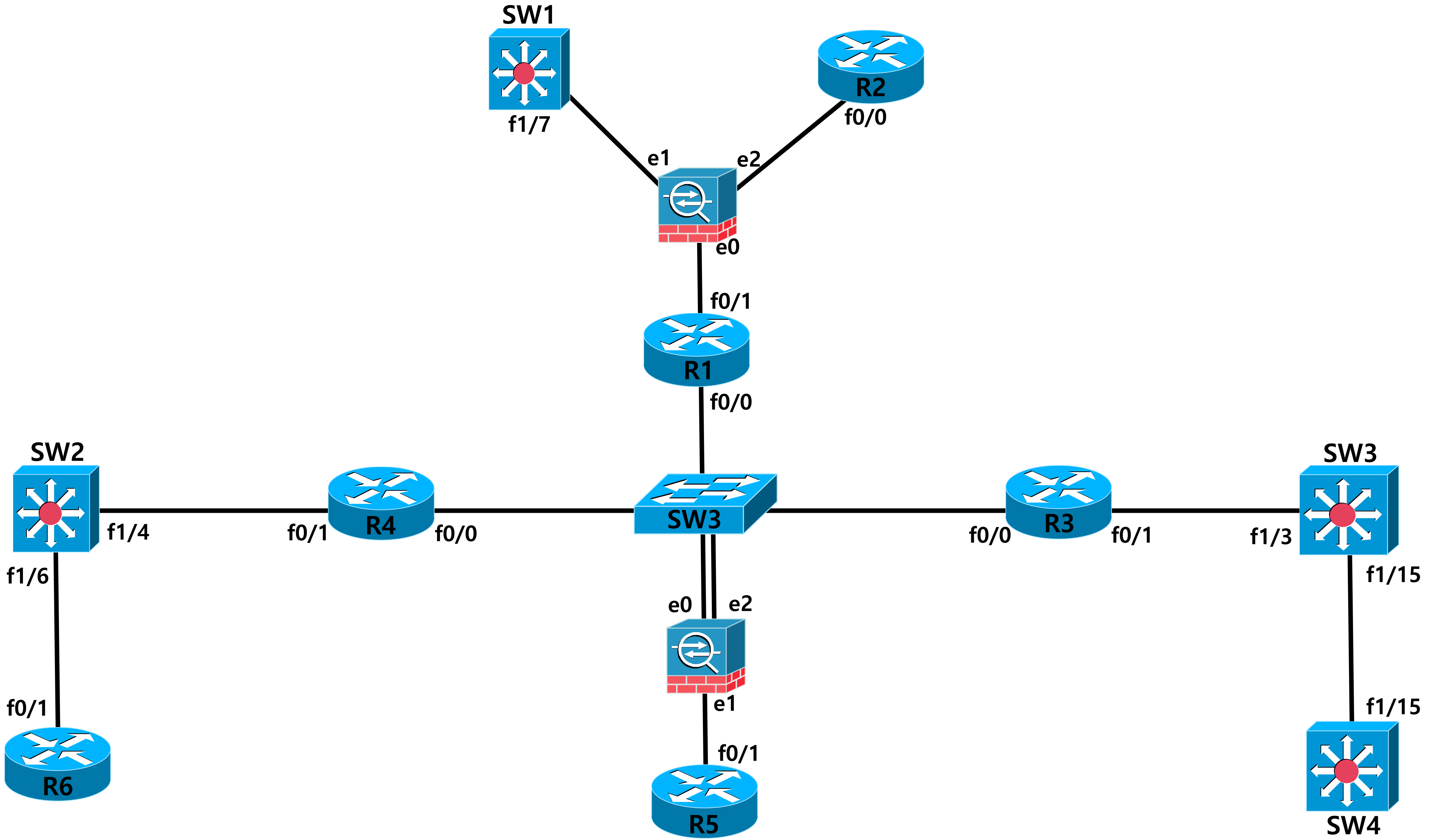
INDEX

1. 방화벽 구성도
    - 1-1. 논리적 구성
    - 1-2. 물리적 구성
    - 1-3. IGP 구성

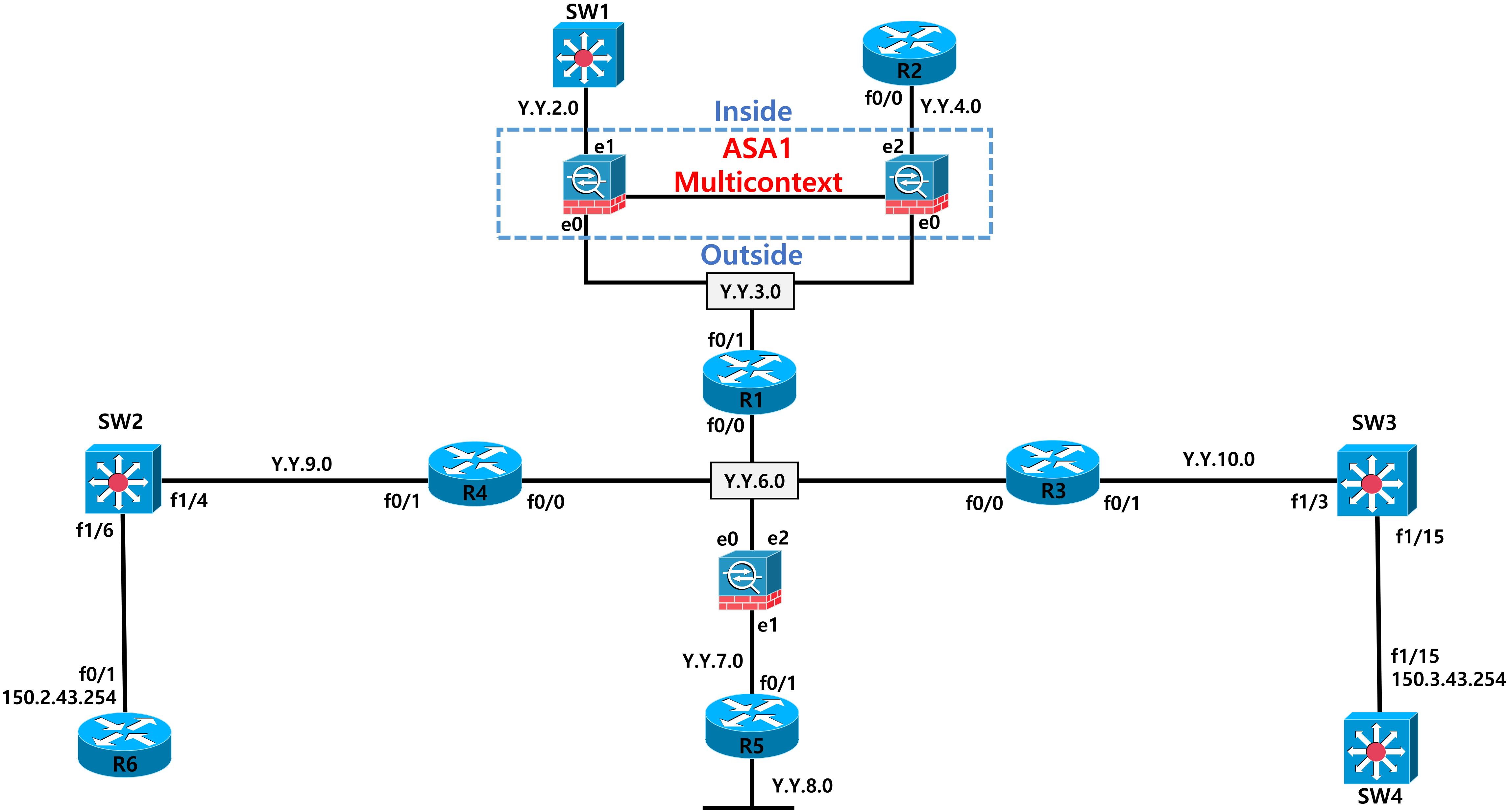
2. 장비 설정
    - 2-1. Router Setting
    - 2-2. Switch Setting
    - 2-3. Firewall Setting
    - 2-4. Firewall (NAT)
    - 2-5. Routing Table

1. 방화벽 구성도

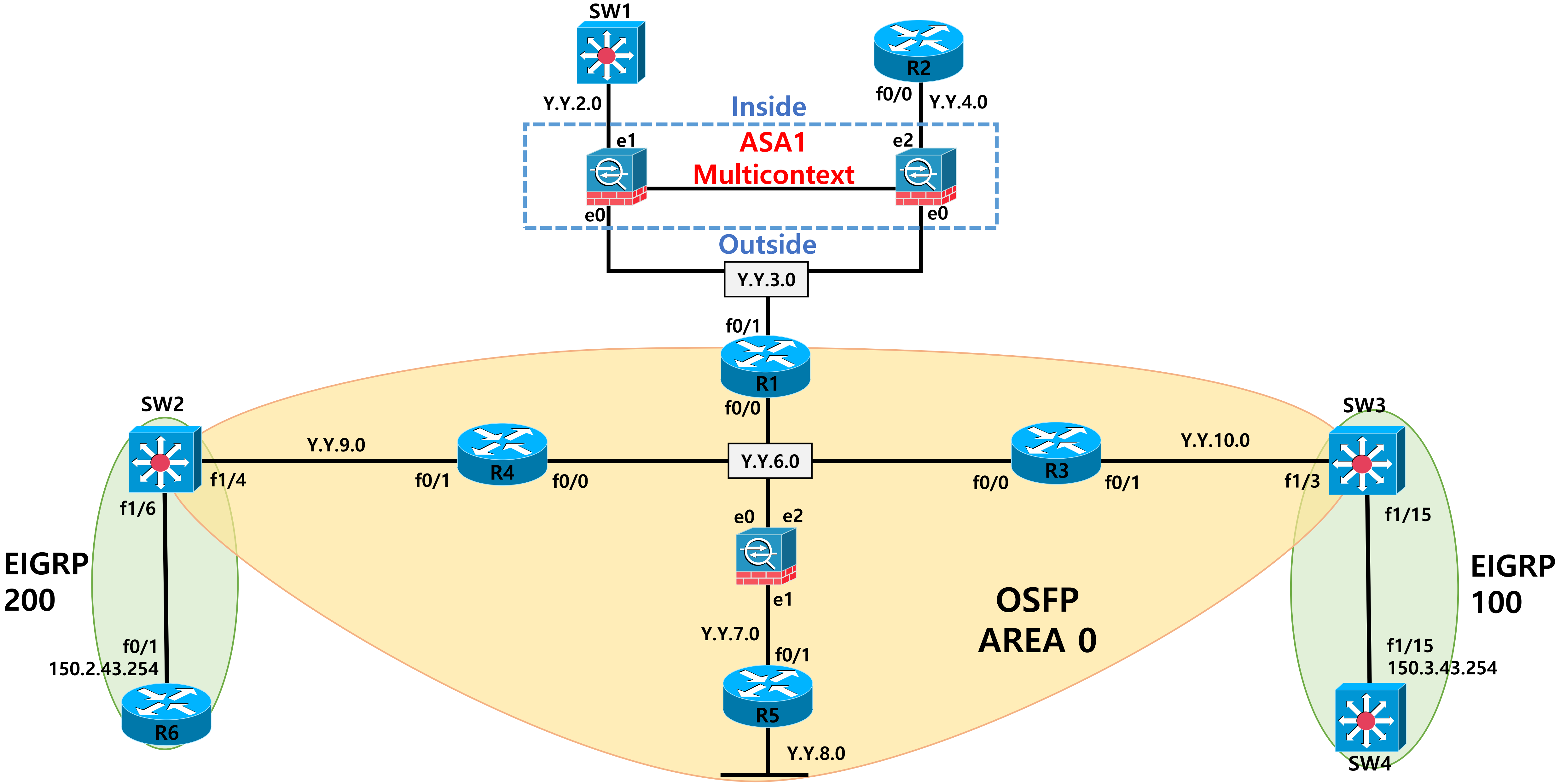
1-1. 물리적 구성


SW1
f1/7
R2
f0/0
e1
e2
e0
f0/1
R1
f0/0
SW2
f1/4
f1/6
f0/1
R4
f0/0
SW3
e0
e2
e1
f0/1
R5
f0/1
R6
f0/0
R3
f0/1
SW3
f1/3
f1/15
f1/15
SW4

1-2. 논리적 구성


SW1
R2
Y.Y.2.0
Inside
f0/0
Y.Y.4.0
e1
ASA1
e2
Multicontext
e0
e0
Outside
Y.Y.3.0
f0/1
R1
f0/0
SW2
SW3
Y.Y.9.0
Y.Y.10.0
R4
Y.Y.6.0
R3
f1/4
f0/1
f0/0
f0/0
f0/1
f1/3
f1/6
e0
e2
f1/15
e1
Y.Y.7.0
f0/1
f0/1
150.2.43.254
f1/15
150.3.43.254
R6
R5
Y.Y.8.0
SW4

1-3. IGP 구성


SW1
R2
Y.Y.2.0
Inside
f0/0
Y.Y.4.0
e1
ASA1
e2
Multicontext
e0
e0
Outside
Y.Y.3.0
f0/1
R1
f0/0
SW2
Y.Y.9.0
R4
Y.Y.6.0
R3
Y.Y.10.0
SW3
f1/4
f0/1
f0/0
f0/0
f0/1
f1/3
f1/6
e0
e2
f1/15
EIGRP
200
e1
OSFP
AREA 0
EIGRP
100
Y.Y.7.0
f0/1
f0/1
150.2.43.254
f1/15
150.3.43.254
R5
R6
Y.Y.8.0
SW4

2-1. Router Setting

Interface Setting

R1

```
int lo0
ip add 192.168.1.1 255.255.255.255

int lo2
ip add 43.43.51.1 255.255.255.255

int f0/0
no sh
ip add 43.43.6.1 255.255.255.0

int f0/1
no sh
ip add 43.43.3.1 255.255.255.0
```

R2

```
int lo0
ip add 192.168.2.2 255.255.255.255

int lo1
ip add 192.168.22.22 255.255.255.255

int f0/0
no sh
ip add 43.43.4.2 255.255.255.0
```

Interface Setting

R3

```
int lo0
ip add 192.168.3.3 255.255.255.255

int lo1
ip add 192.168.33.3 255.255.255.255

int f0/0
no sh
ip add 43.43.6.3 255.255.255.0

int f0/1
no sh
ip add 43.43.10.3 255.255.255.0
```

R4

```
int lo0
ip add 192.168.4.4
255.255.255.255

int f0/0
no sh
ip add 43.43.6.4 255.255.255.0

int f0/1
no sh
ip add 43.43.9.4 255.255.255.0
```

Interface Setting

R5

```
int lo0
ip add 192.168.5.5
255.255.255.255

int lo2
ip add 43.43.52.5 255.255.255.255

int f0/1
no sh
ip add 43.43.7.5 255.255.255.0

int f0/0
no sh
ip add 43.43.8.5 255.255.255.0
```

R6

```
int lo0
ip add 192.168.6.6
255.255.255.255

int f0/1
no sh
ip add 150.2.43.254 255.255.255.0
```

Routing

R1 Routing

```
ip route 0.0.0.0 0.0.0.0 43.43.3.10
ip route 43.43.4.0 255.255.255.0 43.43.3.12

router os 1
router-id 1.1.1.1
net 43.43.51.1 0.0.0.0 ar 0
net 43.43.6.1 0.0.0.0 ar 0
default-inf ori alway
```

R2 Routing

```
ip route 0.0.0.0 0.0.0.0 43.43.4.12
```

R3 Routing

```
router os 1
router-id 3.3.3.3
net 43.43.6.3 0.0.0.0 ar 0
net 43.43.10.3 0.0.0.0 ar 0
```

R4 Routing

```
router os 1
router-id 4.4.4.4
net 43.43.9.4 0.0.0.0 ar 0
net 43.43.6.4 0.0.0.0 ar 0
```

Routing

R5 Routing

```
router os 1
router-id 5.5.5.5
net 43.43.7.5 0.0.0.0 ar 0
net 43.43.8.5 0.0.0.0 ar 0
net 43.43.52.5 0.0.0.0 ar 0
```

R6 Routing

```
router ei 200
no au
net 150.2.43.254 0.0.0.0
```

2-2. Switch Setting

Switch

SW1

```
int lo150
ip add 150.1.43.1 255.255.255.0

int f1/7
no sw
ip add 43.43.2.1 255.255.255.0

ip route 43.43.0.0 255.255.0.0 43.43.2.10
```

SW2

```
int f1/4
no sw
ip add 43.43.9.1 255.255.255.0

int f1/6
no sw
ip add 150.2.43.1 255.255.255.0

router os 1
net 43.43.9.1 0.0.0.0 ar 0
redi ei 200 sub

router ei 200
no au
net 150.2.43.1 0.0.0.0
redi os 1 met 1 1 1 1 1
```

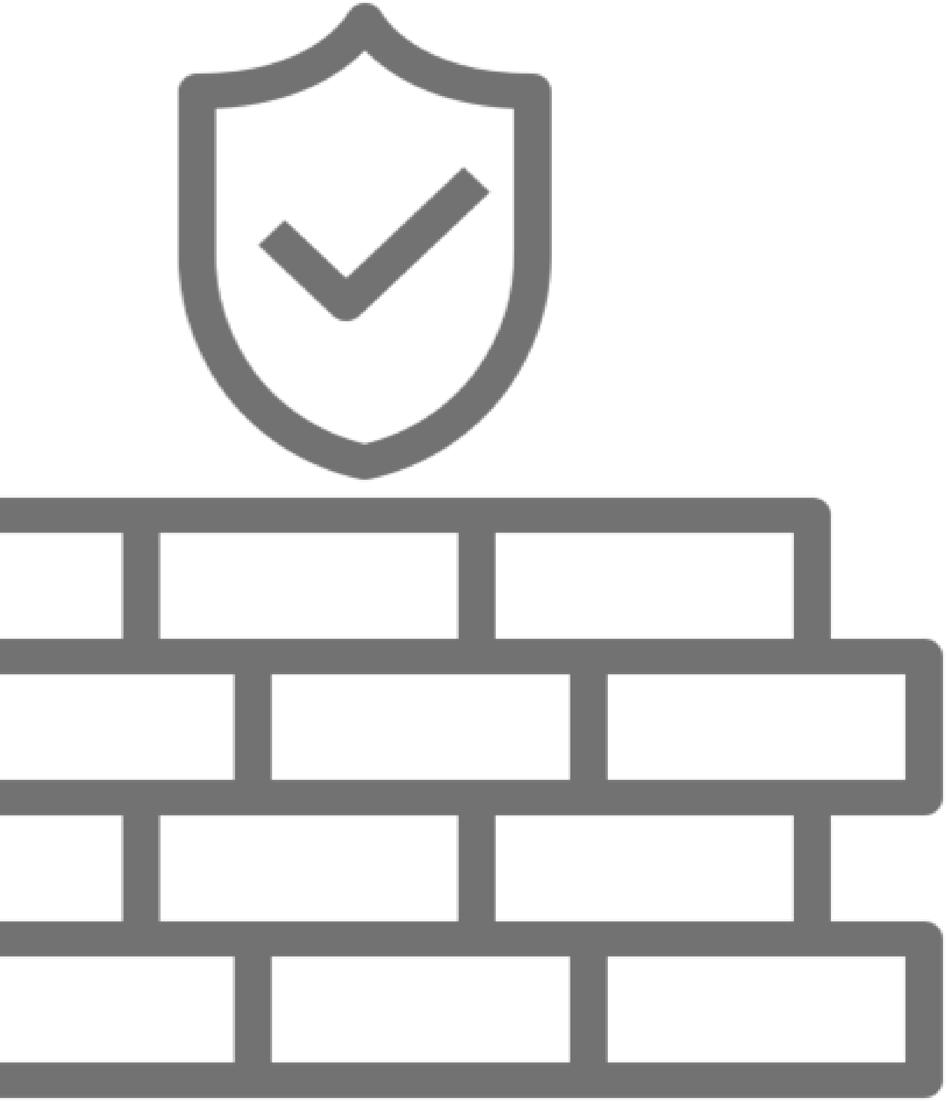
Switch

SW3

```
int f1/3
no sw
ip add 43.43.10.1 255.255.255.0

int f1/15
no sw
ip add 150.3.43.1 255.255.255.0

router os 1
net 43.43.10.1 0.0.0.0 ar 0
redi ei 100 sub

router ei 100
no au
net 150.3.43.1 0.0.0.0
redi os 1 met 1 1 1 1 1
```

SW4

```
int f1/15
no sw
ip add 150.3.43.254 255.255.255.0

router ei 100
no au
net 150.3.43.254 0.0.0.0
```



2-3. Firewall Setting

ASA1

ASA1

```
int g0
no sh

int g1
no sh

int g2
no sh

admin-context admin
context admin
config-u admin.cfg
```

Context 생성

```
context c1
config-u c1.cfg
allocate-int g0
allocate-int g1

context c2
config-u c2.cfg
allocate-int g0
allocate-int g2

mac-address auto
```

ASA1 (Context)

ASA1(Context c1)

```
nameif inside
ip add 43.43.2.10 255.255.255.0

int g0
nameif outside
ip add 43.43.3.10 255.255.255.0

route outside 0 0 43.43.3.1
route inside 150.1.0.0 255.255.0.0 43.43.2.1

access-l acl_oi per icmp a a
access-g acl_oi in int outside
```

ASA1(Context c2)

```
int g2
nameif inside
ip add 43.43.4.12 255.255.255.0

int g0
nameif outside
ip add 43.43.3.12 255.255.255.0

route outside 0 0 43.43.3.1
route inside 192.168.2.0
255.255.255.0 43.43.4.2

access-l acl_oi per icmp a a
access-g acl_oi in int outside
```

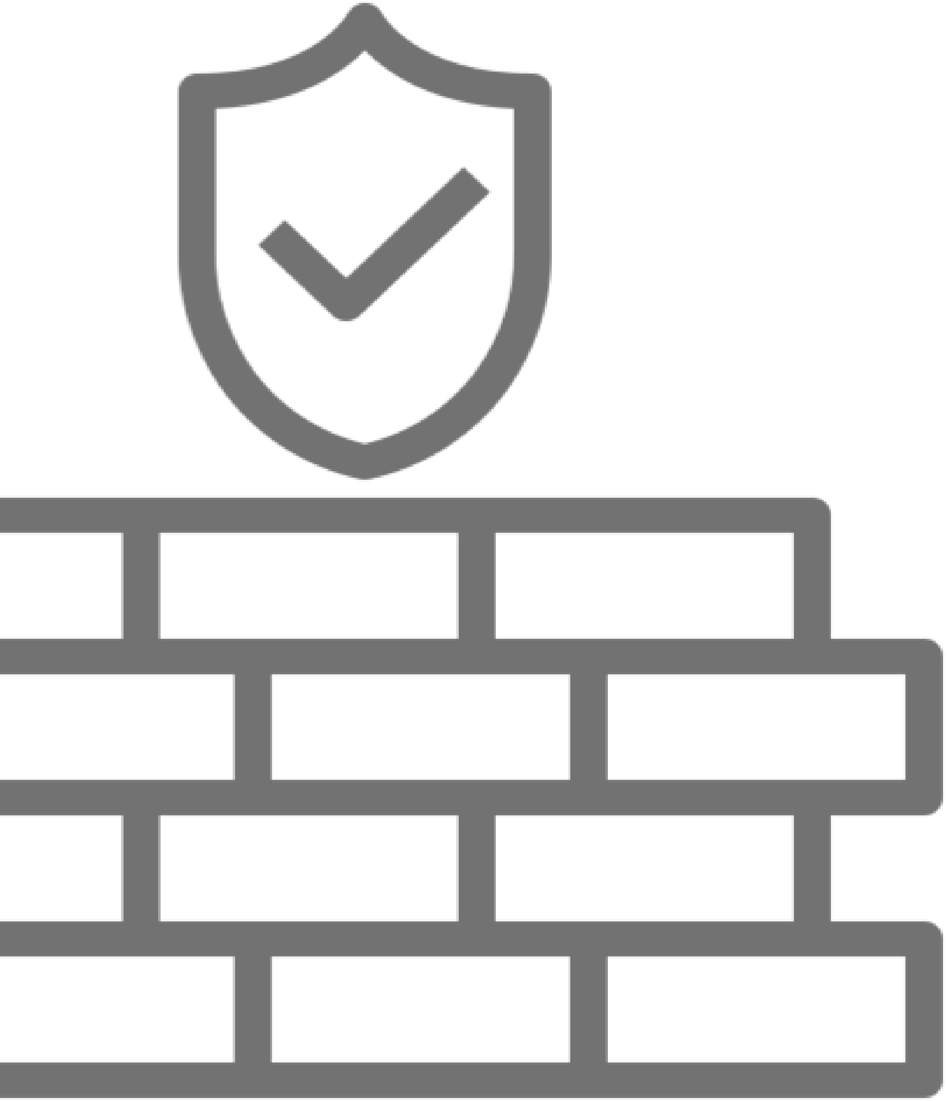
ASA2

ASA2

```
int g0
no sh

int g1
no sh

int g2
no sh

access-l acl_oi per icmp a a
access-g acl_oi in int outside

router os 1
net 43.43.6.0 255.255.255.0 a 0
net 43.43.7.0 255.255.255.0 a 0
```

ASA2 Redundant 기술

```
int re1
member-int g0
member-int g2
nameif outside
ip add 43.43.6.10 255.255.255.0

int g1
nameif inside
ip add 43.43.7.10 255.255.255.0

redundant-int re1 active-mem g0
```



2-4. Firewall (NAT)

Firewall(NAT)

정적 NAT

```
object network L2_Server
host 43.43.52.5
nat (inside,outside) static 43.43.6.52
```

정적 PAT

```
object network F1_Server
host 43.43.8.5
nat (inside,outside) static 43.43.6.8
service tcp http 8080
```

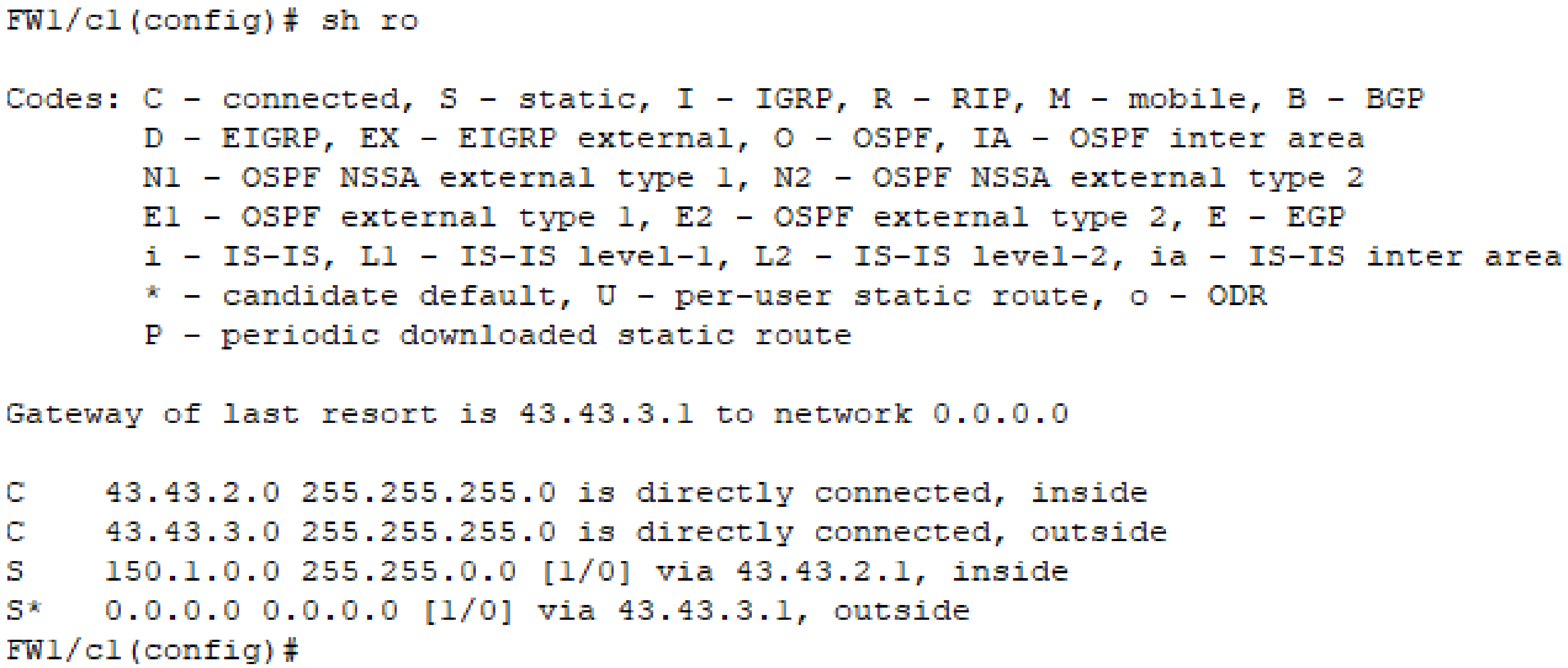
동적 PAT

```
object network Inside_PAT
subnet 43.43.7.0 255.255.255.0
nat (inside,outside) dynamic interface
```

2. 장비 설정

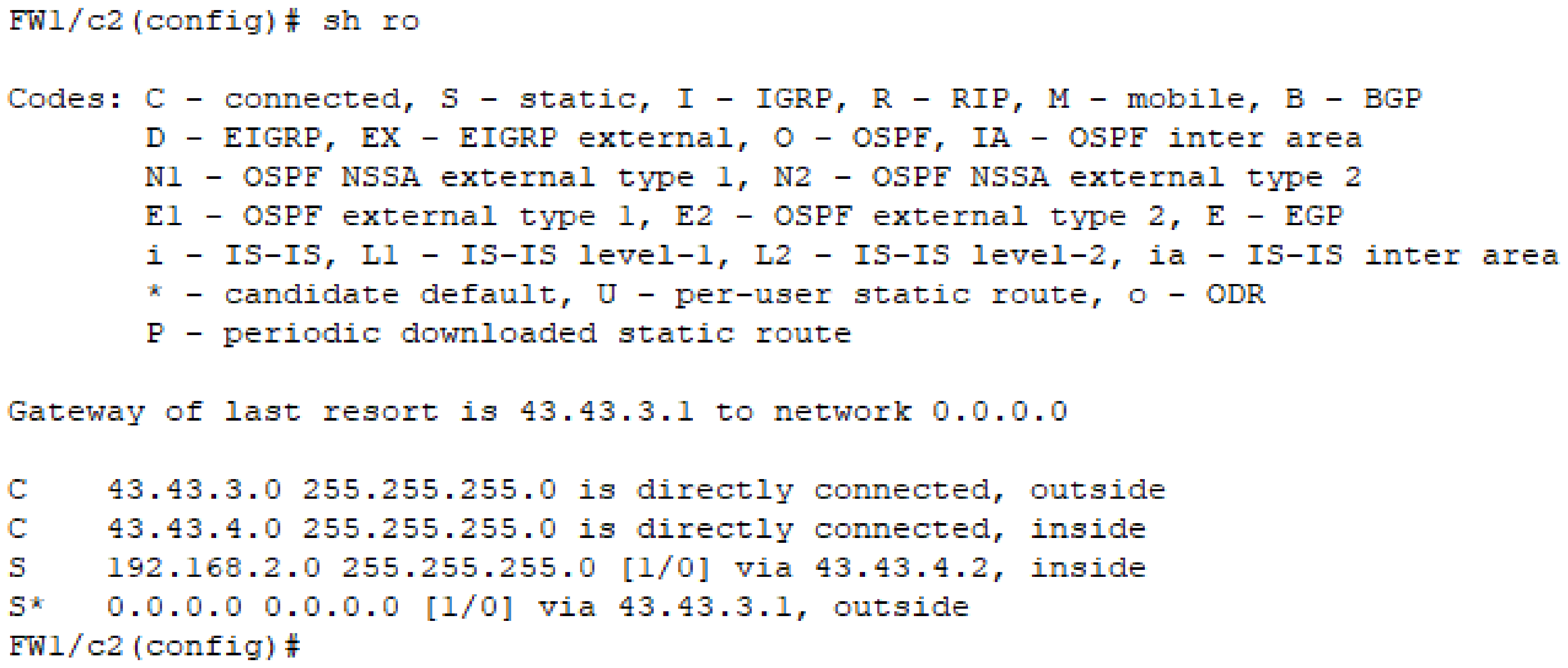
2-5. Routing Table

Context c1 Routing Table



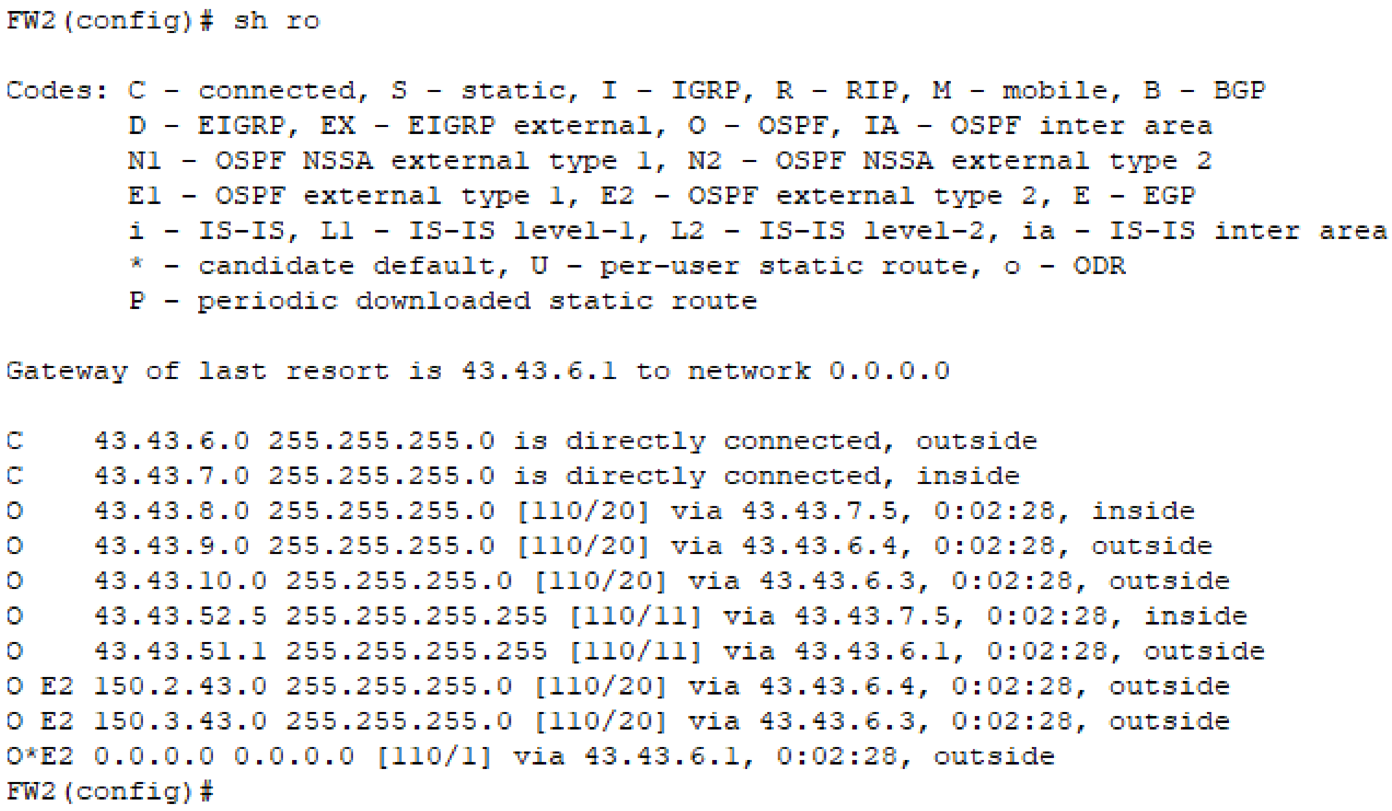
```
FW1/c1(config)# sh ro

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 43.43.3.1 to network 0.0.0.0

C    43.43.2.0 255.255.255.0 is directly connected, inside
C    43.43.3.0 255.255.255.0 is directly connected, outside
S    150.1.0.0 255.255.0.0 [1/0] via 43.43.2.1, inside
S*   0.0.0.0 0.0.0.0 [1/0] via 43.43.3.1, outside
FW1/c1(config)#
```

Context c2 Routing Table



```
FW1/c2(config)# sh ro

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 43.43.3.1 to network 0.0.0.0

C    43.43.3.0 255.255.255.0 is directly connected, outside
C    43.43.4.0 255.255.255.0 is directly connected, inside
S    192.168.2.0 255.255.255.0 [1/0] via 43.43.4.2, inside
S*   0.0.0.0 0.0.0.0 [1/0] via 43.43.3.1, outside
FW1/c2(config)#
```

ASA2 Routing Table



```
FW2(config)# sh ro

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 43.43.6.1 to network 0.0.0.0

C    43.43.6.0 255.255.255.0 is directly connected, outside
C    43.43.7.0 255.255.255.0 is directly connected, inside
O    43.43.8.0 255.255.255.0 [110/20] via 43.43.7.5, 0:02:28, inside
O    43.43.9.0 255.255.255.0 [110/20] via 43.43.6.4, 0:02:28, outside
O    43.43.10.0 255.255.255.0 [110/20] via 43.43.6.3, 0:02:28, outside
O    43.43.52.5 255.255.255.255 [110/11] via 43.43.7.5, 0:02:28, inside
O    43.43.51.1 255.255.255.255 [110/11] via 43.43.6.1, 0:02:28, outside
O E2 150.2.43.0 255.255.255.0 [110/20] via 43.43.6.4, 0:02:28, outside
O E2 150.3.43.0 255.255.255.0 [110/20] via 43.43.6.3, 0:02:28, outside
O*E2 0.0.0.0 0.0.0.0 [110/1] via 43.43.6.1, 0:02:28, outside
FW2(config)#
```

대우직업능력개발원

www.dwit.or.kr

대우직업능력개발원

Daewoo Development Institute for Vocational ability