Parte 1: Configurazione delle subnet

Tabella delle subnet

LAN	NetID	Subnet Mask	Host disponibili	Gateway/Ultimo indirizzo
LAN1	10.108.54.0	/25 (128)	126	10.108.54.126 (R1)
LAN2	10.108.54.128	/25 (128)	126	10.108.54.254 (R2)
LAN3	10.108.55.0	/29 (8)	6	10.108.55.6 (R1)
LAN4	10.108.55.8	/29 (8)	6	10.108.55.14 (GW)
LAN5	10.108.55.16	/29 (8)	6	10.108.55.22 (GW)

Configurazione degli indirizzi IP

Router R1

```
ip addr add 10.108.54.126/25 dev eth0  # LAN1
ip addr add 10.108.55.6/29 dev eth1    # LAN3
ip addr add 10.108.55.14/29 dev eth2   # LAN4
ip link set eth0 up
ip link set eth1 up
ip link set eth2 up
```

Router R2

```
ip addr add 10.108.54.254/25 dev eth0  # LAN2
ip addr add 10.108.55.6/29 dev eth1    # LAN3
ip addr add 10.108.55.22/29 dev eth2   # LAN5
ip link set eth0 up
ip link set eth1 up
ip link set eth2 up
```

Gateway (GW)

```
ip addr add 10.108.55.14/29 dev eth0   # LAN4
ip addr add 10.108.55.22/29 dev eth1   # LAN5
ip addr add 3.3.3.3/32 dev eth2        # Esterno
ip link set eth0 up
```

```
ip link set eth1 up
ip link set eth2 up
```

Host H1

```
ip addr add 10.108.54.1/25 dev eth0
ip route add default via 10.108.54.126
ip link set eth0 up
```

Host H2

```
ip addr add 10.108.54.129/25 dev eth0
ip route add default via 10.108.54.254
ip link set eth0 up
```

Server S1

```
ip addr add 10.108.54.2/25 dev eth0
ip route add default via 10.108.54.126
ip link set eth0 up
```

Server S2

```
ip addr add 10.108.54.130/25 dev eth0
ip route add default via 10.108.54.254
ip link set eth0 up
```

Parte 2: Configurazione della rete

Parte 2a: Isolamento dei domini di broadcast con VLAN

Configurazione VLAN sugli switch

Esegui i seguenti comandi su ogni switch:

```
vlan/create 10  # Crea VLAN 10 (LAN1)
vlan/create 20  # Crea VLAN 20 (LAN2)
vlan/create 30  # Crea VLAN 30 (LAN3)
```

```
vlan/create 40  # Crea VLAN 40 (LAN4)
vlan/create 50  # Crea VLAN 50 (LAN5)

port/setvlan eth0 10  # Assegna eth0 a VLAN 10
port/setvlan eth1 20  # Assegna eth1 a VLAN 20
port/setvlan eth2 30  # Assegna eth2 a VLAN 30
port/setvlan eth3 40  # Assegna eth3 a VLAN 40
port/setvlan eth4 50  # Assegna eth4 a VLAN 50
```

Subinterfacce sui router

Esempio per R1:

```
ip addr add 10.108.54.126/25 dev eth0  # VLAN10
ip addr add 10.108.55.6/29 dev eth1    # VLAN30
ip addr add 10.108.55.14/29 dev eth2   # VLAN40
```

Ripeti per R2 e GW.

Parte 2b: Configurazione delle interfacce e routing

Abilitare il forwarding IP

Su ogni router:

```
sysctl -w net.ipv4.ip_forward=1
```

Configurazione delle rotte statiche

Su R1:

```
ip route add 10.108.54.128/25 via 10.108.55.6  # LAN2 tramite R2
```

Su R2:

```
ip route add 10.108.54.0/25 via 10.108.55.6  # LAN1 tramite R1
```

Parte 2c: Evitare il passaggio tramite GW

1. **Aggiungere rotte dirette tra R1 e R2** per LAN1 e LAN2.
   - Su R1:

     ```
     ip route add 10.108.54.128/25 via 10.108.55.6
     ```

   - Su R2:

     ```
     ip route add 10.108.54.0/25 via 10.108.55.6
     ```

Parte 3: Configurazioni aggiuntive

NAT sul Gateway

Esegui i seguenti comandi su GW:

```
iptables -t nat -A POSTROUTING -s 10.108.54.0/25 -o eth2 -j SNAT --to-source
4.3.2.1
iptables -t nat -A POSTROUTING -s 10.108.54.128/25 -o eth2 -j SNAT --to-
source 1.2.3.4
iptables -t nat -A PREROUTING -d 4.3.2.1 -p tcp --dport 80 -j DNAT --to-
destination 10.108.54.2
iptables -t nat -A PREROUTING -d 1.2.3.4 -p tcp --dport 25 -j DNAT --to-
destination 10.108.54.130
```

Regole Firewall

1. Blocca tutti i servizi tranne HTTP e SMTP:

   ```
   iptables -A INPUT -p tcp --dport 80 -j ACCEPT
   iptables -A INPUT -p tcp --dport 25 -j ACCEPT
   iptables -A INPUT -j DROP
   ```

2. Consenti accesso HTTP/HTTPS da LAN1 e LAN2:

   ```
   iptables -A FORWARD -s 10.108.54.0/25 -p tcp --dport 80 -j ACCEPT
   iptables -A FORWARD -s 10.108.54.0/25 -p tcp --dport 443 -j ACCEPT
   ```

```
iptables -A FORWARD -s 10.108.54.128/25 -p tcp --dport 80 -j ACCEPT
iptables -A FORWARD -s 10.108.54.128/25 -p tcp --dport 443 -j ACCEPT
```

3. Blocca l'accesso a Internet per reti diverse da LAN1 e LAN2:

```
iptables -A FORWARD -s 10.108.55.0/29 -j DROP
iptables -A FORWARD -s 10.108.55.8/29 -j DROP
iptables -A FORWARD -s 10.108.55.16/29 -j DROP
```

Nota: Testa ogni configurazione con comandi come `ping`, `traceroute` e `curl` per verificare la connettività e il rispetto delle regole di rete.