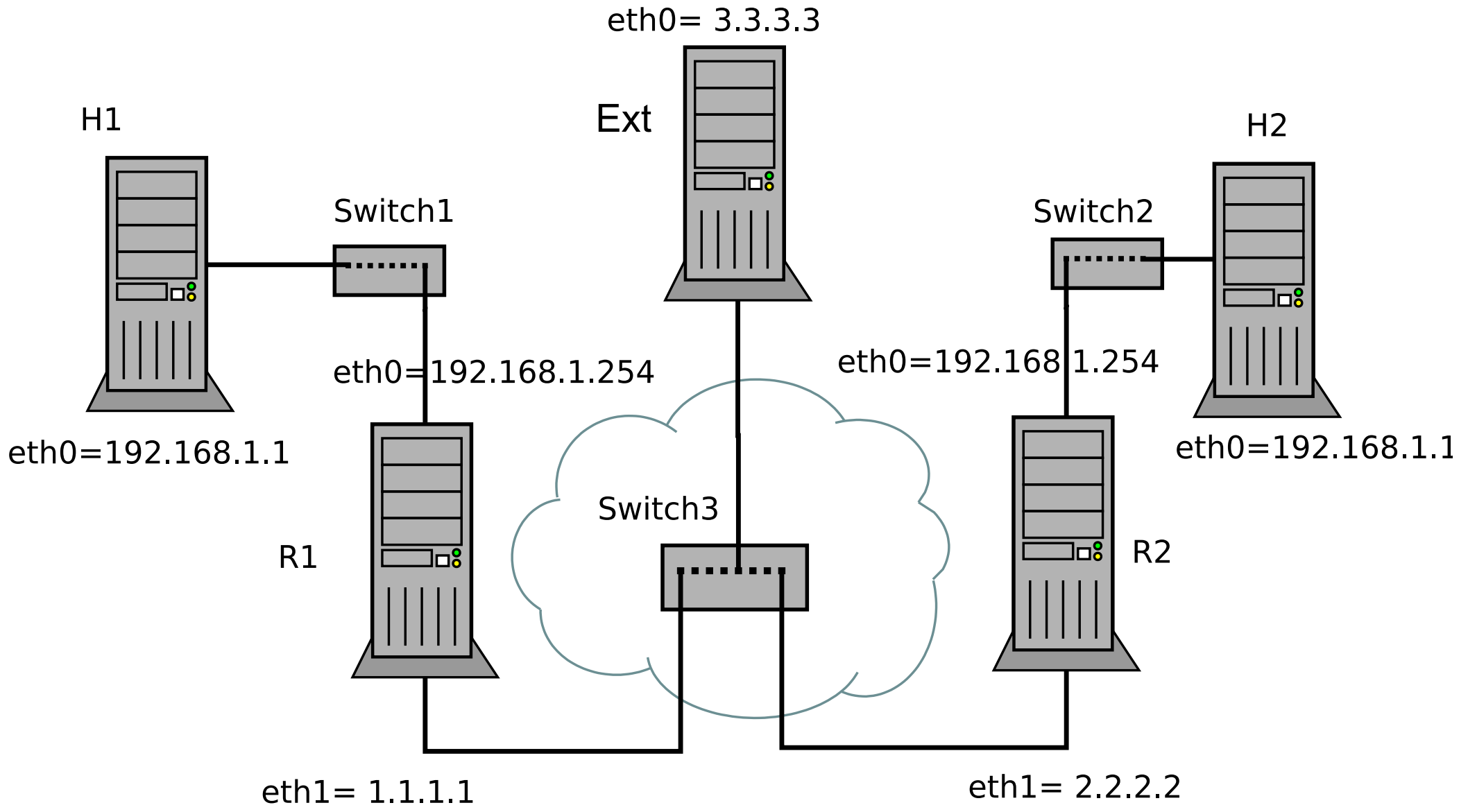
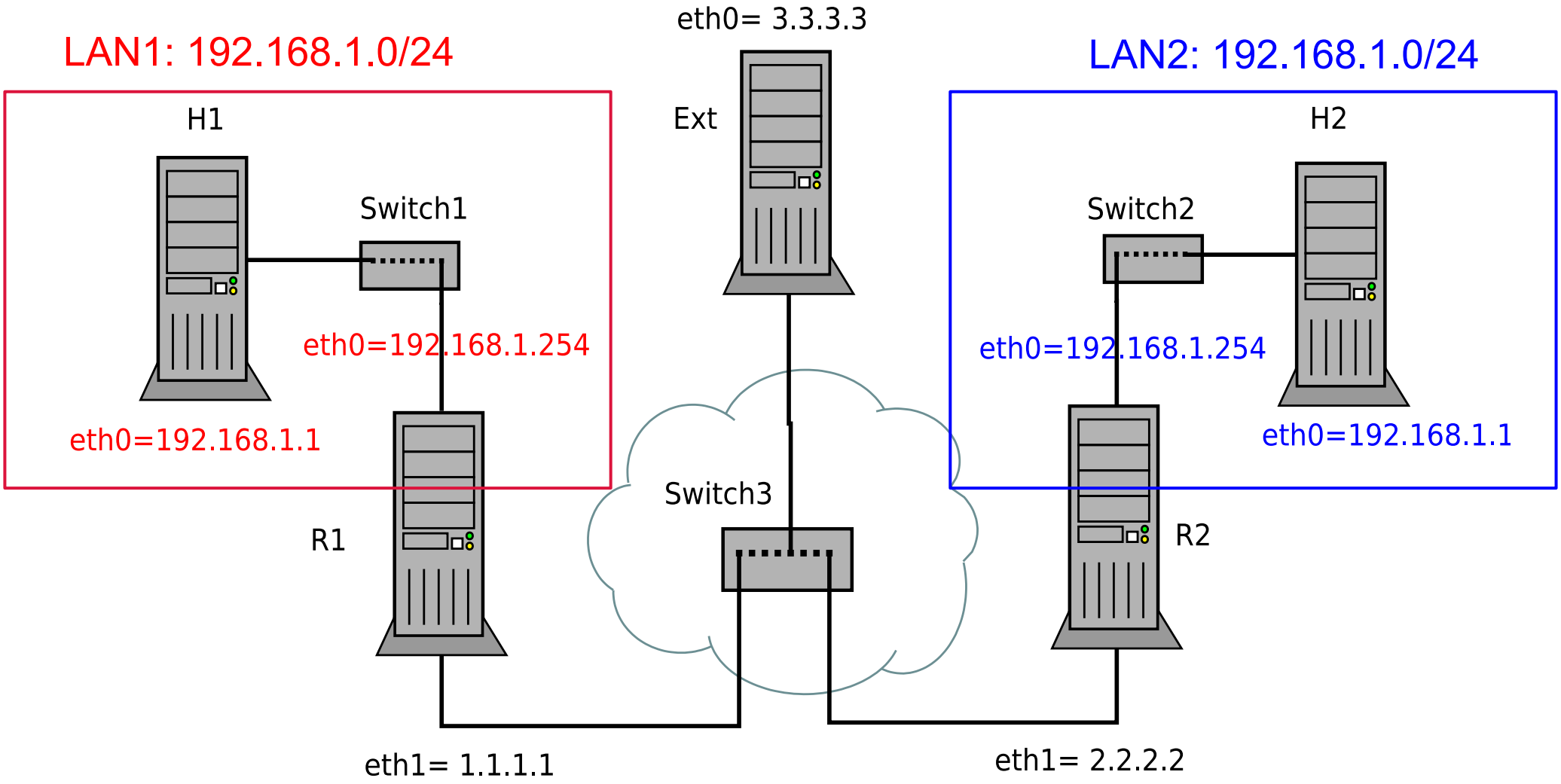
Esercitazione 1 [1]



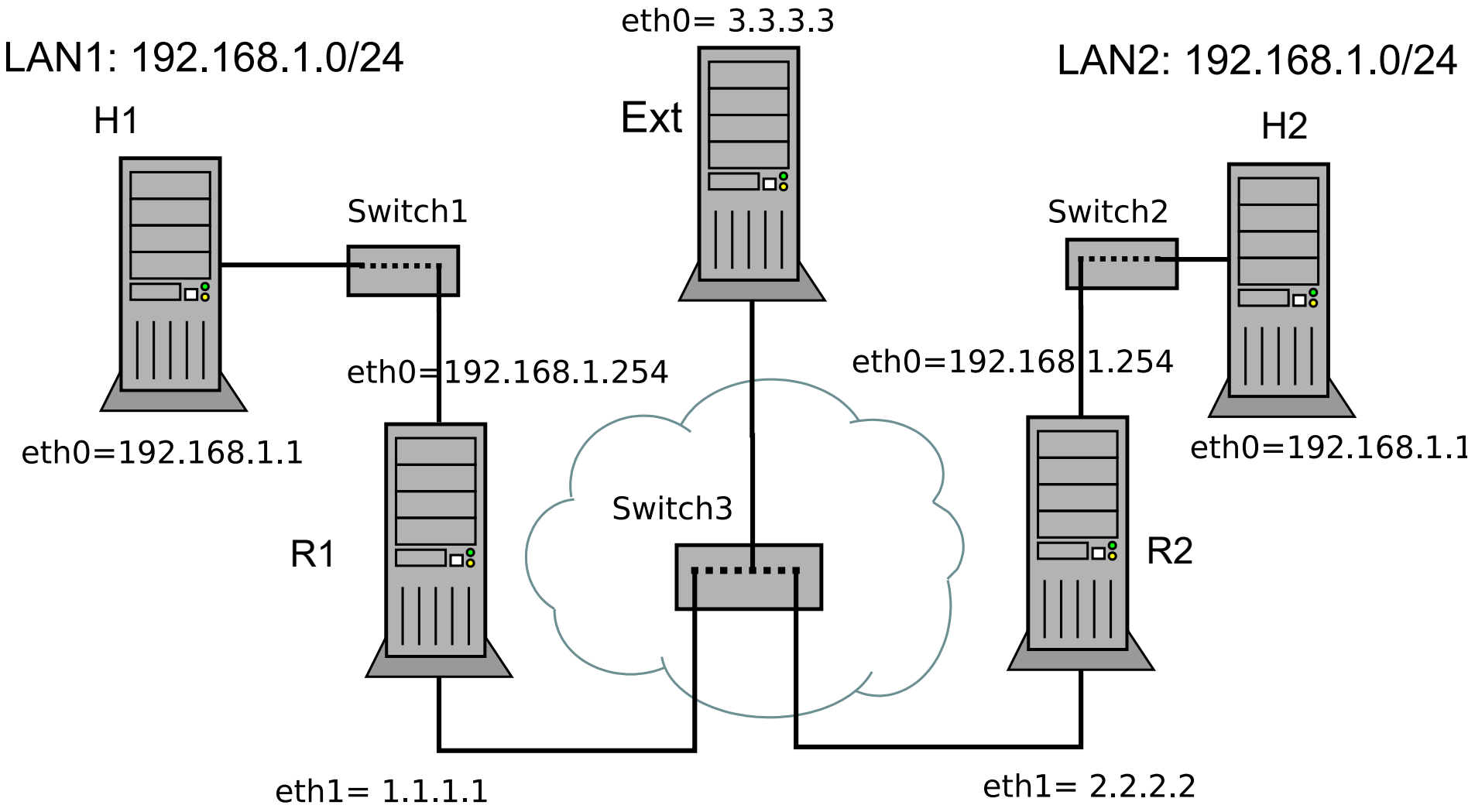
Esercitazione 1 [2]

Indirizzi IP Internet duplicati? **NO**, le tre reti impiegano tre spazi di indirizzamento IP separati, si impiega il **"NATting"** per farle comunicare



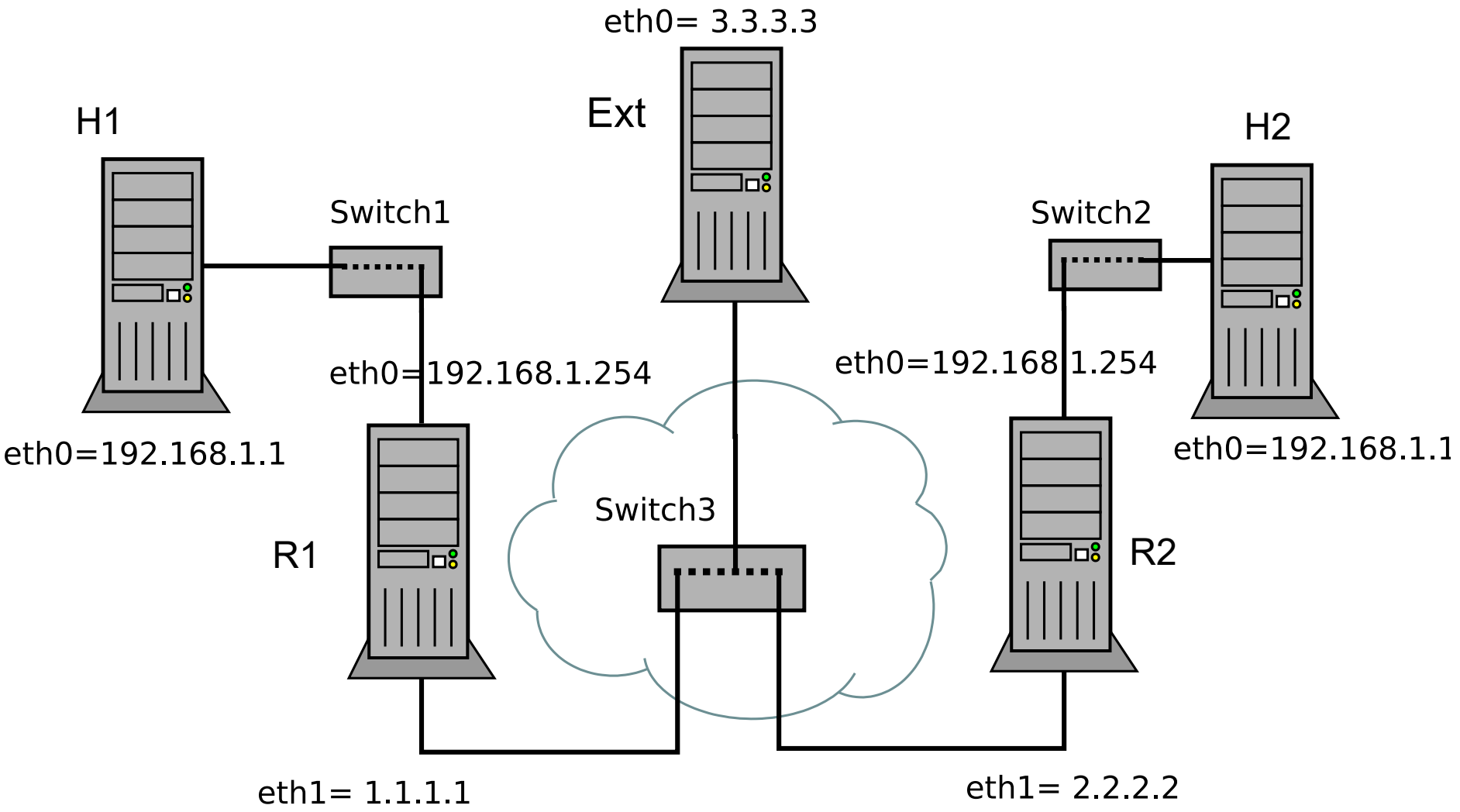
Esercitazione 1a [3]

Configurare la rete iniziale per permettere la comunicazione fra i nodi, considerando che S3 simula la rete Internet e i gateway R1 ed R2 devono applicare **Source Natting** sul traffico in uscita dalle rispettive reti.



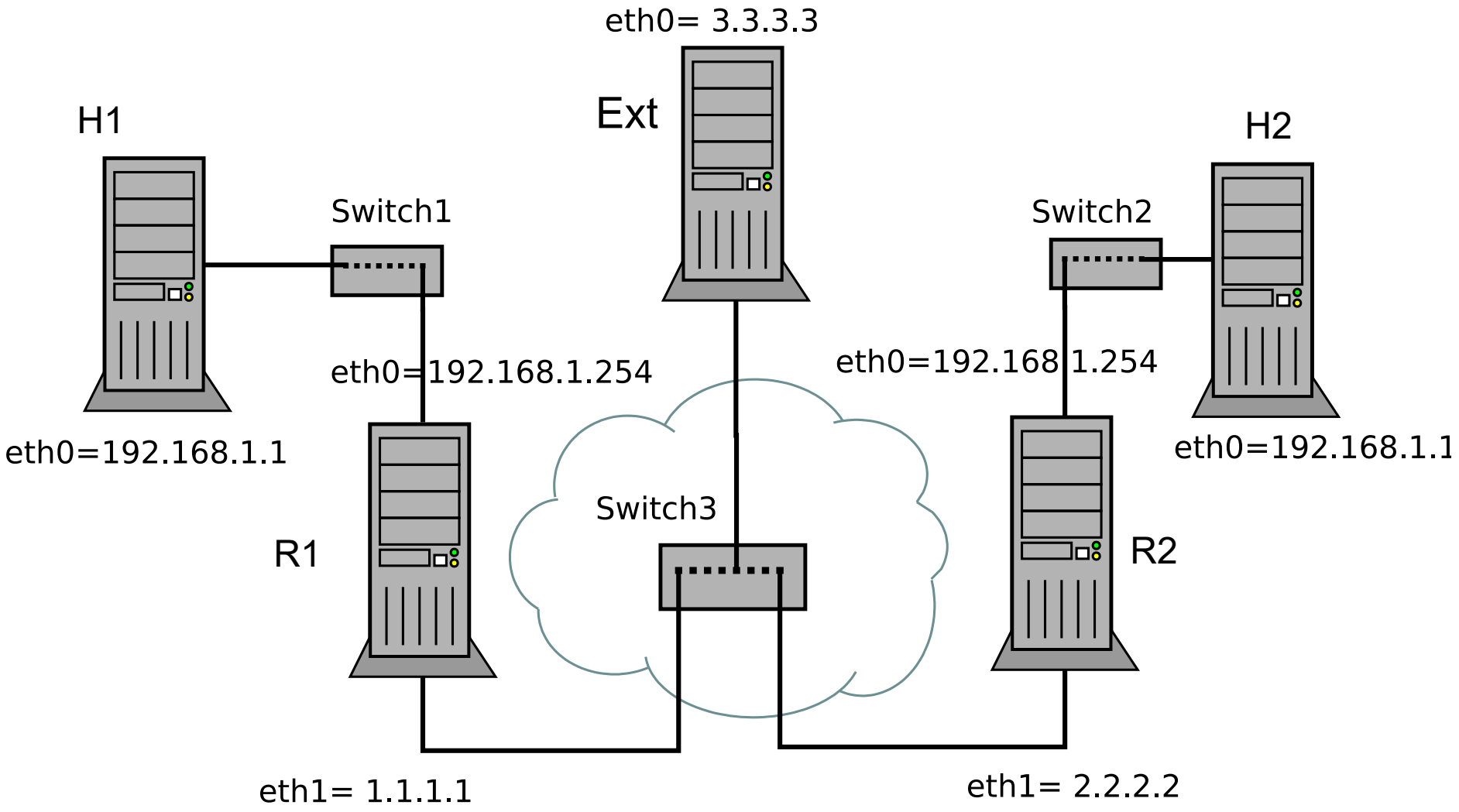
Esercitazione 1b [4]

Configurare R2 per permettere di utilizzare un servizio TCP in ascolto sulla porta 8080 di H2 utilizzando l'indirizzo IP 2.2.2.2 di R2.



Esercitazione 1c [5]

Configurare R1 per permettere di utilizzare un servizio TCP in ascolto sulla porta 22 di H1 utilizzando un indirizzo aggiuntivo 1.1.1.2 disponibile su R1 e sulla porta pubblica 2222



Soluzione esercitazione (1)

Assumiamo di aver configurato correttamente gli indirizzi IP e le regole di routing per la simulazione di Internet e per le due reti private

- **Fondamentale:** le reti private non sono “visibili” a chi non ne fa parte!

```
root@ext:~# ip r
1.1.1.1 dev eth0  scope link
2.2.2.2 dev eth0  scope link

root@r1:~# ip r
2.2.2.2 dev eth1  scope link
3.3.3.3 dev eth1  scope link
192.168.1.0/24 dev eth0 proto kernel scope link src 192.168.1.254

root@r2:~# ip r
1.1.1.1 dev eth1  scope link
3.3.3.3 dev eth1  scope link
192.168.1.0/24 dev eth0 proto kernel scope link src 192.168.1.254
```

Soluzione esercitazione (2)

a) SNAT

```
root@r1:~# iptables -t nat -A POSTROUTING -s 192.168.1.0/24 \
                -o eth1 -j MASQUERADE
root@r2:~# iptables -t nat -A POSTROUTING -s 192.168.1.0/24 \
                -o eth1 -j MASQUERADE
```

b) DNAT

```
root@r2:~# iptables -t nat -A PREROUTING -i eth1 -d 2.2.2.2
            -p tcp --dport 80 -j DNAT --to-destination 192.168.1.1
```

c) DNAT (soluzione senza alias, r1 diventa "referente" per 1.1.1.2)

```
root@r2:~# route add -host 1.1.1.2 gw 1.1.1.1
root@ext:~# route add -host 1.1.1.2 gw 1.1.1.1
root@r1:~# iptables -t nat -A PREROUTING -i eth1 -d 1.1.1.2
            -p tcp --dport 2222 \
            -j DNAT --to-destination 192.168.1.1:22
```

Nota: *possiamo testare con netcat, ma possiamo anche verificare con* `ss` *che c'è già un servizio ssh in ascolto sugli host virtuali. Possiamo chiuderlo con il comando* `systemctl stop ssh`