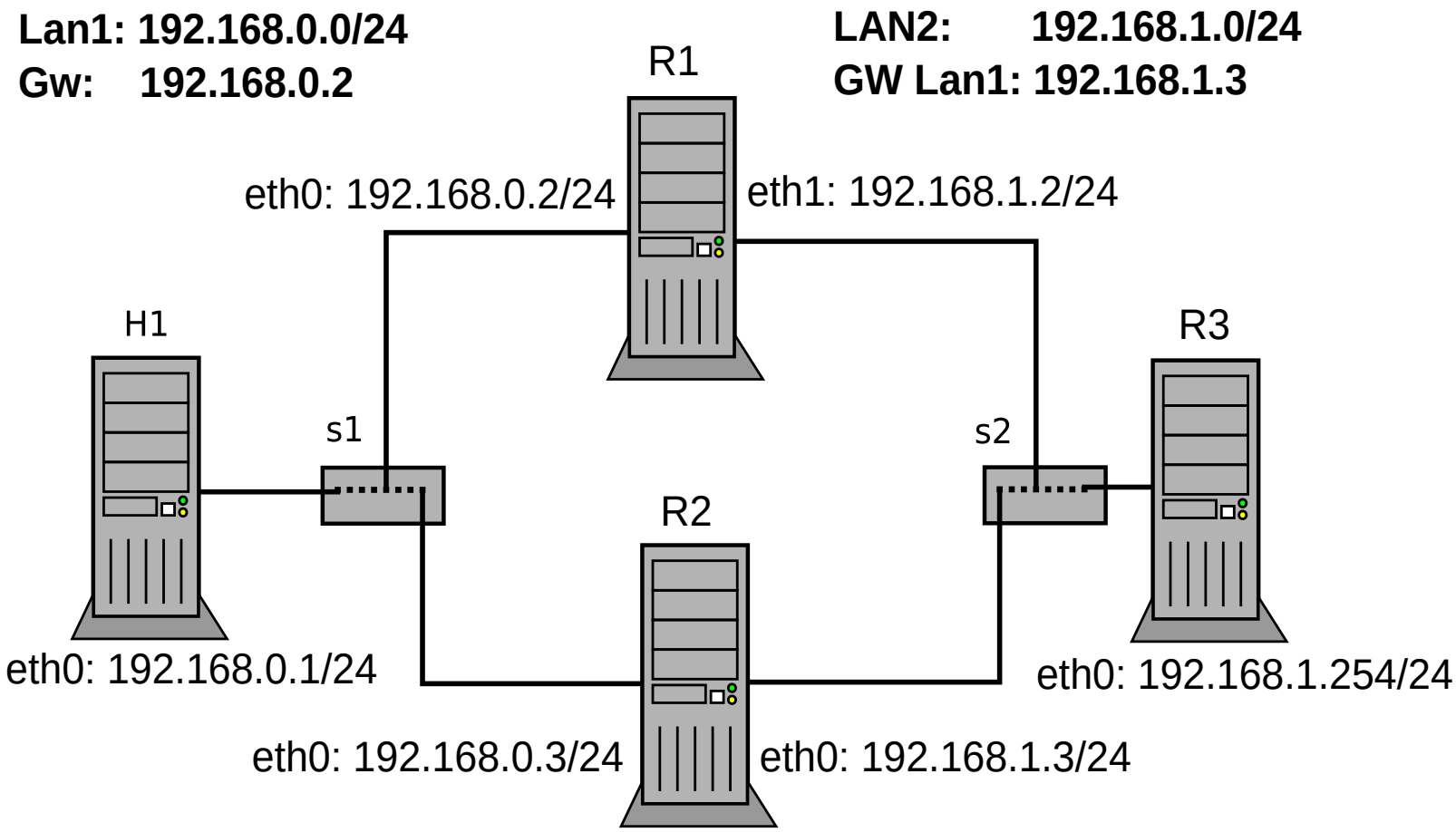
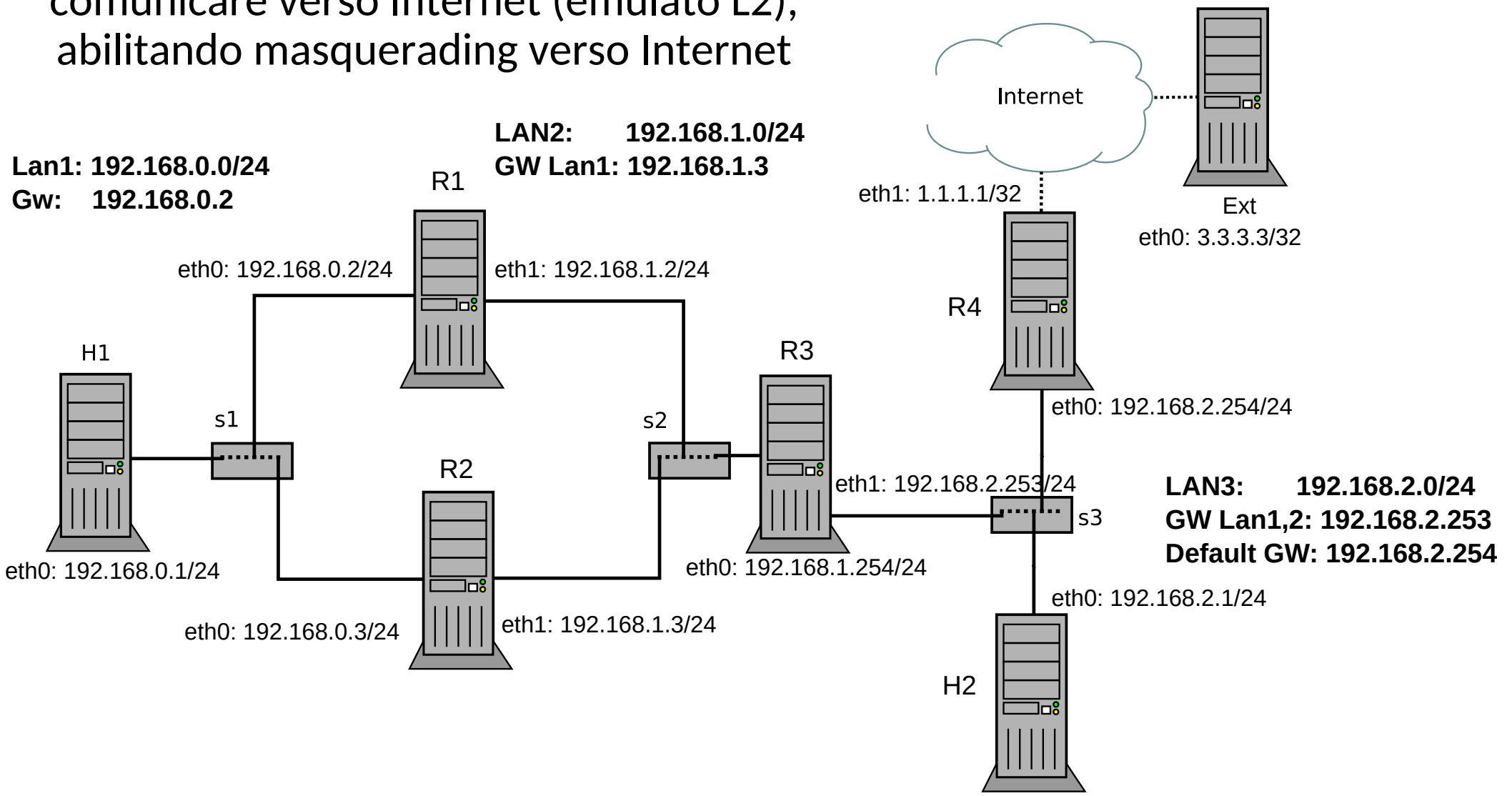
# Checkpoint 1




Configurare la rete in modo che tutti gli host possano comunicare fra di loro nei termini definiti (*prestare particolare attenzione ai gateway*)

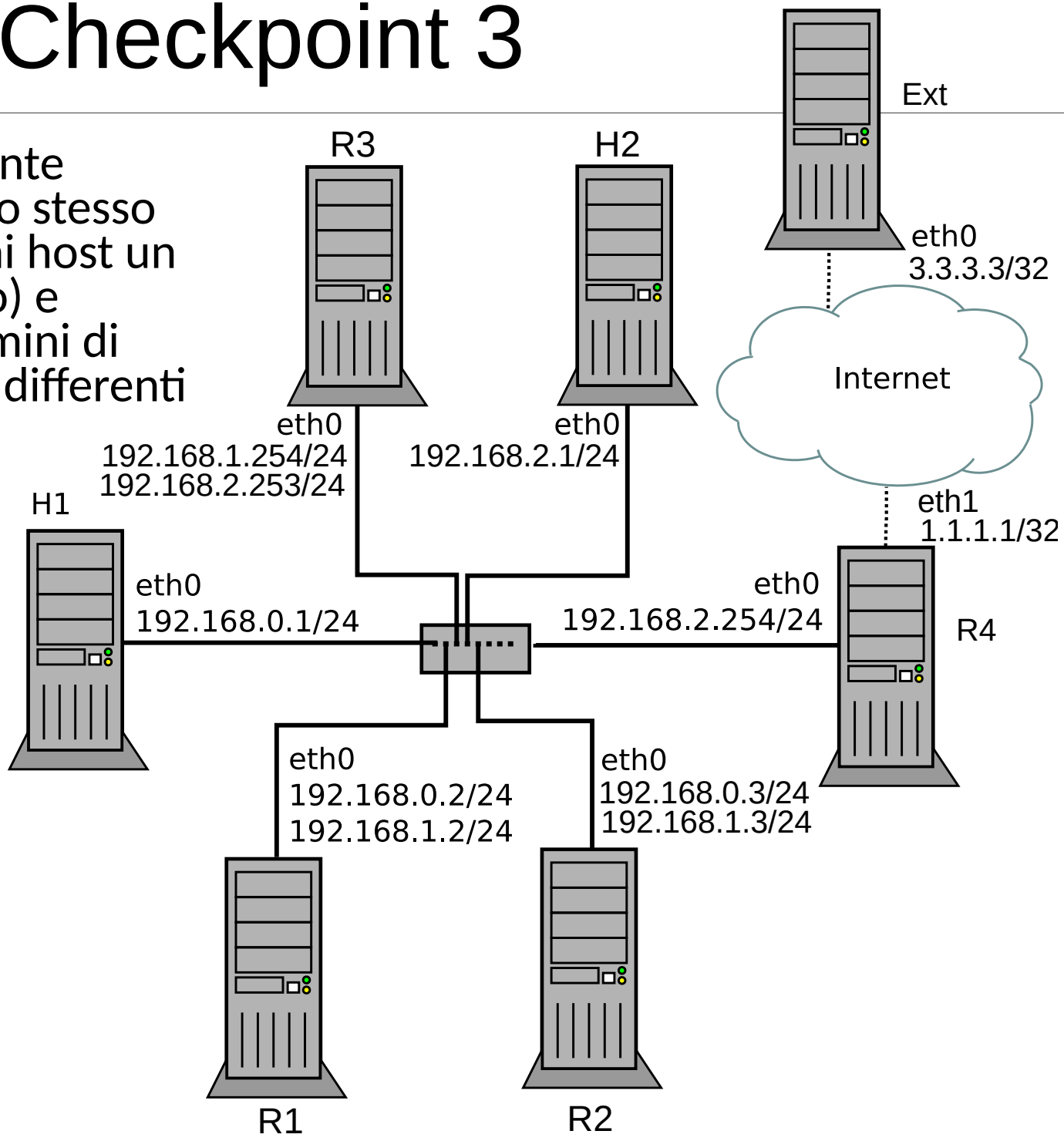
# Checkpoint 2

Estendere la rete per permettere agli host di comunicare verso Internet (emulato L2), abilitando masquerading verso Internet



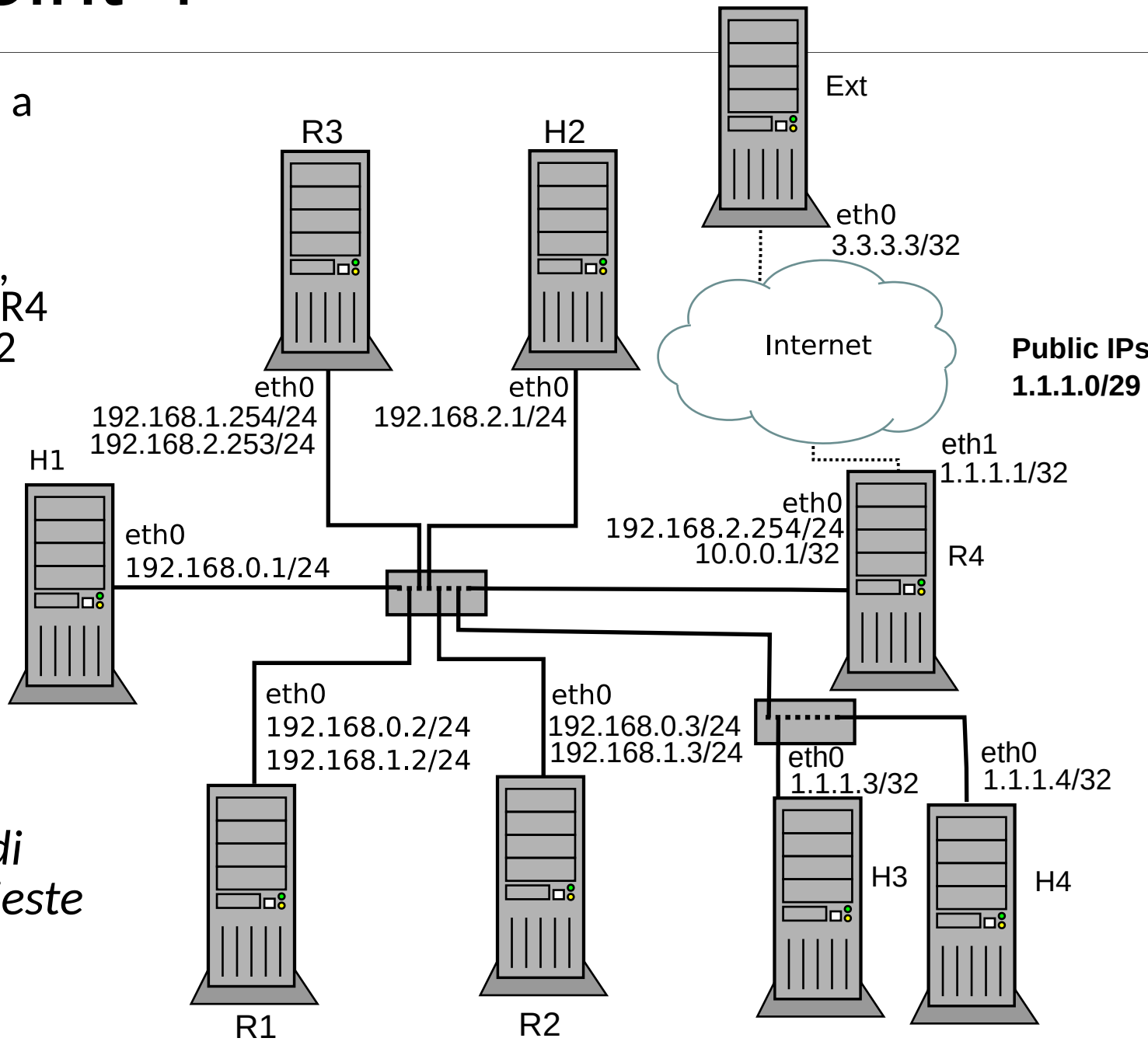
# Checkpoint 3

Modificare la rete precedente collegando tutti gli host allo stesso switch (utilizzando per ogni host un singolo collegamento fisico) e mantenendo separati i domini di broadcast Ethernet di LAN differenti tramite l'uso di VLAN.



# Checkpoint 4

La rete aziendale ha ora a disposizione il range pubblico 1.1.1.0/29, e configura due host H3 e H4 con indirizzi pubblici, collegati a livello H2N a R4 con indirizzo 10.0.0.1/32 in una rete dedicata




*Configurare le policy di natting e firewall richieste nella seguente slide*

# Checkpoint 4 - Policy

Source natting

- Lan1 può contattare Internet e i servizi pubblici della rete con IP 1.1.1.2
- Lan2 può contattare i servizi pubblici su H3 e H4 con IP 1.1.1.5

Destination natting

- Consentire la raggiungibilità dei servizi SSH su H1 e H2 su porte pubbliche “alte” a scelta, mantenendo la raggiungibilità del servizio SSH su R4

Firewall

- Su R4
  - Applicare policy DROP di default per il forward del traffico
  - Consentire la raggiungibilità di servizi HTTP[s] (porte TCP 80 e 443) su H3
  - Consentire la raggiungibilità di DNS (porte UDP 53) su H4
  - Consentire il traffico legato alle regole di source e destination natting
  - Consentire traffico ICMP di tipo ‘too big’ relativo a richieste da Lan1 e Lan2
- Su R3, consentire il traffico *originato* da Lan3 verso Lan1 e Lan2, ma non viceversa (attenzione a consentire comunque la comunicazione verso Internet)
- Configurare R1 e R2 per fare in modo che non possa essere possibile “eludere” le policy di routing “unidirezionali” espresse al checkpoint 1