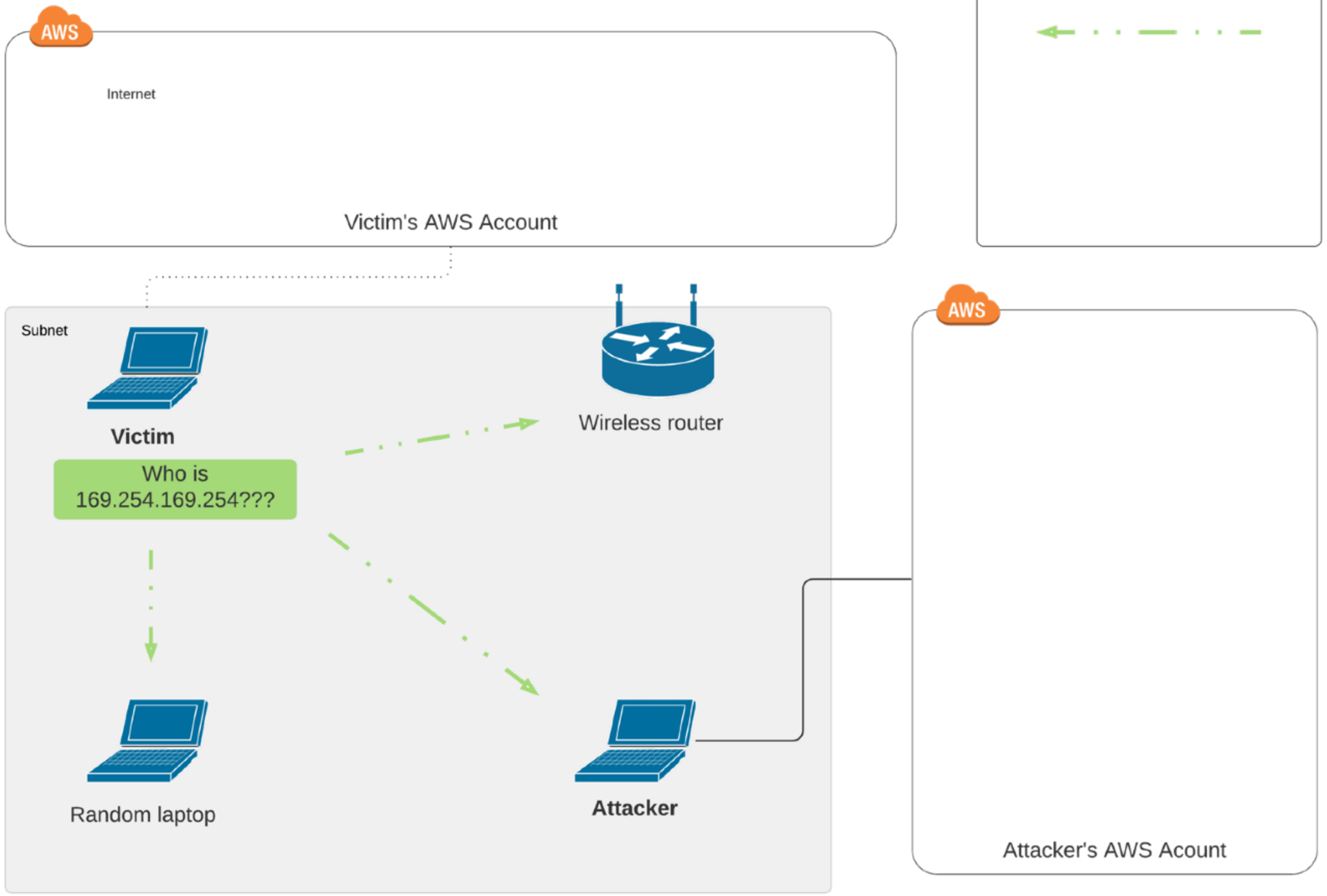
IMDS lookup

IMDS behavior + link-local routing

- What’s happening here
- Can this be abused?
- If so what’s the worst case scenario?

IMDS Request Hijacking

Ryan Gerstenkorn | November 30, 2020



Notes

1. *ARP happens when the IP is in a range the host considers link-local.*
2. *Generally 169.254.0.0/16 is treated as link-local.*
3. *ARP is sent on the broadcast IP which means any host in the subnet can recieve and respond to it.*