ROSE-HULMAN
INSTITUTE OF TECHNOLOGY

# CSSE 490
# Network Security

Day 6: Layer 2 attacks and Defenses

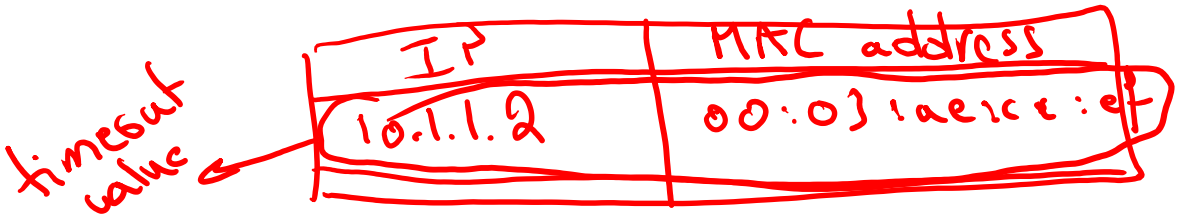
# Outline

- Recap: Address Resolution Protocol (ARP)
- The ARP Cache
- ARP Cache Poisoning
- ARP Defenses

# ARP Demo

- Use packet captures from the GitHub repo

# The ARP Cache




- Hosts cache IP to MAC mapping in ARP cache
- Checkout `arp -n`
- Each entry will timeout and will be removed

# ARP Cache Refresh

reset the timeout value

## The ARP Cache can be refreshed upon 3 events:

1. Receiving an **ARP Request**

2. Receiving an **ARP Reply** ✓

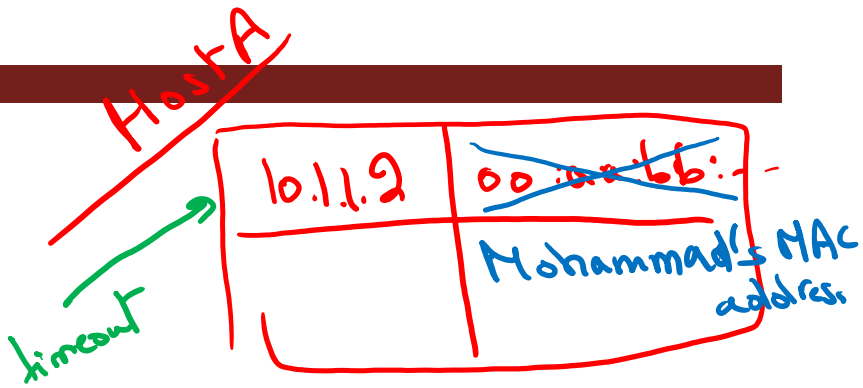
3. Receiving an **ARP gratuitous message** — same as ARP request. Same Source & destination IP/MAC mapping

# Challenges

- ARP is **stateless**
  - No correlation between an ARP request and an ARP reply
- **No authentication**
  - Cannot really verify who is sending the messages
- Designed for **performance** first

- Before any communication happens

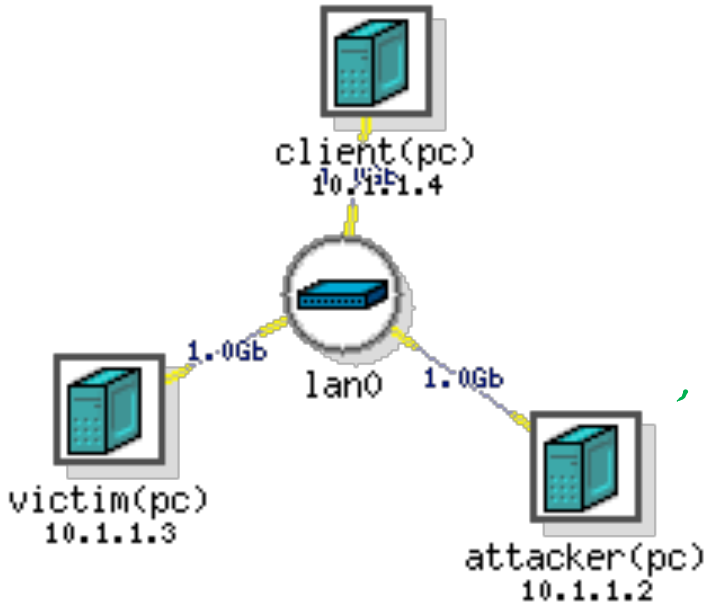
# ARP Cache Poisoning




- Modify the victim's ARP cache
- Create an invalid mapping in the cache
- Keep sending forged packets to refresh the cache

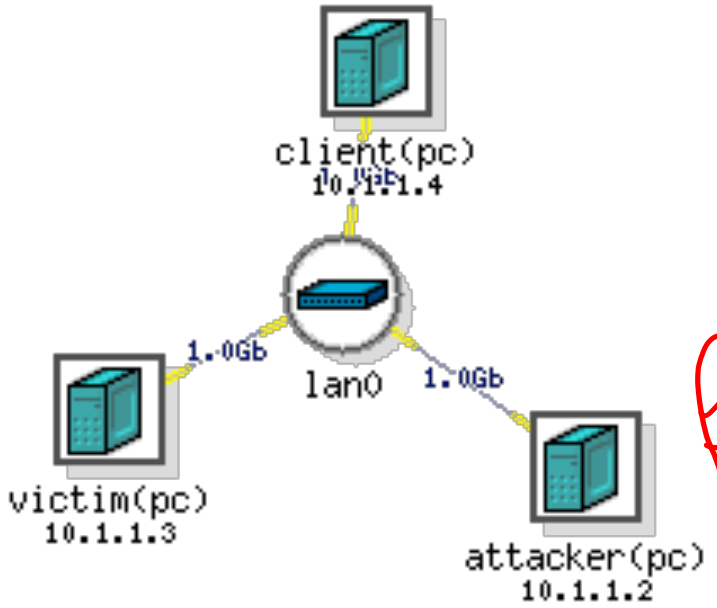
# Poisoning with a Request

- Send an ARP request with forged **source** IP and MAC address



# Poisoning with a Request

- Send an ARP reply with forged **destination** IP and MAC address

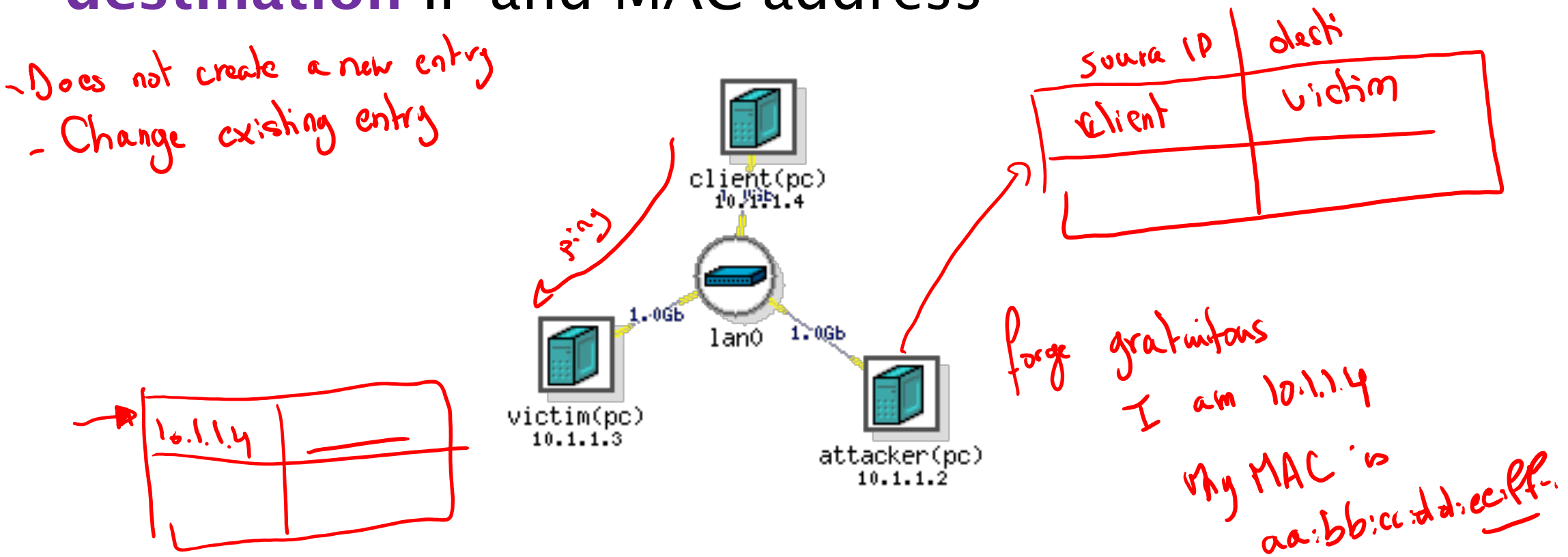



forged ARP request

10.1.1.4
aa:bb:cc:dd:ee:ff

# Poisoning with a Gratuitous Packet

- Send an ARP gratuitous with forged **source and destination** IP and MAC address



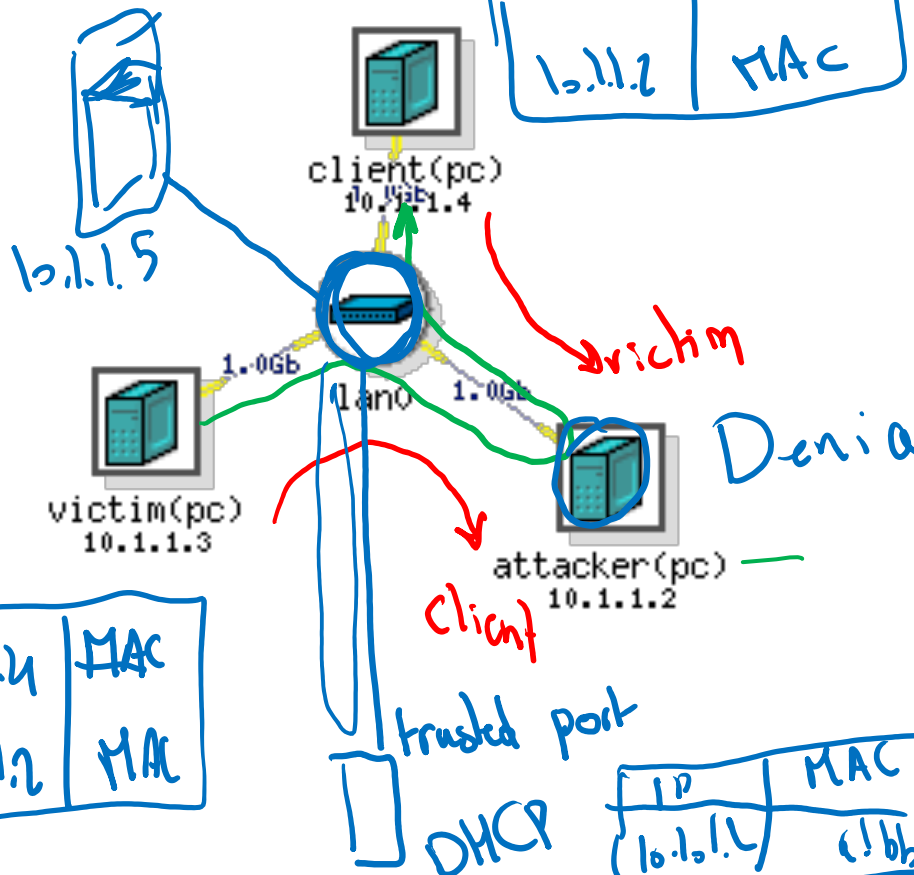
# Man-In-The-Middle (MITM) Attack

Layer 2
↓
inside the OS

Countermeasures

① Static ARP tables

② Authentication
(Public/Private key pairs)
S. ARP
≥ lox shutdown




| 10.1.1.3 | MAC |
|---|---|
| 10.1.1.2 | MAC |

| 10.1.1.4 | MAC |
|---|---|
| 10.1.1.2 | MAC |

| IP | MAC |
|---|---|
| 10.1.1.4 | 0:1b:1c:... |

Database

Denial of Service
(Availability).

# ARP Defenses

- Encryption to prevent MITM
- Static ARP tables
- Dynamic ARP Inspection (DAI)

DHCP

Cisco Routers/Switches