

# Redes de Computadores II

**Universidade do Algarve**

**Semana 5**

[https://github.com/ncatanoc/redes\\_algarve](https://github.com/ncatanoc/redes_algarve)

**Néstor Cataño**

[nestor.catano@gmail.com](mailto:nestor.catano@gmail.com)

# ARP and DHCP

## **Goal:**

To understand the basic functionality of ARP and DHCP.

# Roadmap

1. ARP

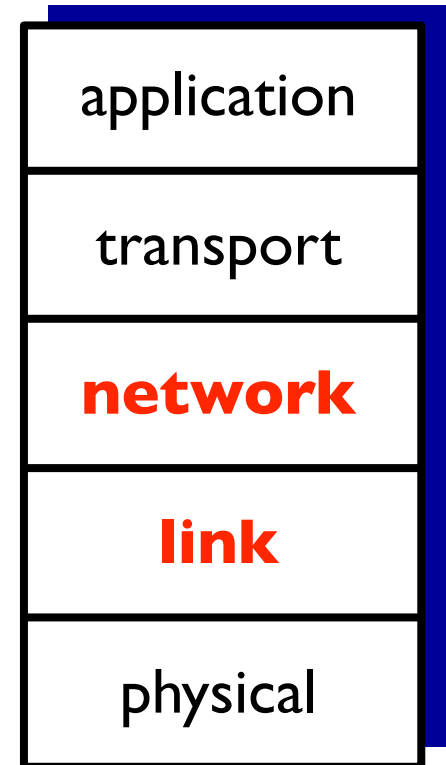
2. DHCP (Dynamic Host Control Protocol)

3. DHCP security

# introduction

- How do we connect the link layer to the network layer?
- How do we get MAC address `0C:0C:0B:14:CD:98` connected to IP address `192.0.2.1`?

**How to connect these two?**



# properties of MAC and IP addresses

## ● **MAC addresses**

- Consist of an OUI and NIC identifier
- Are associated with a network adapter, e.g., hardware

## ● **IP addresses**

- Not dependent on hardware
- Assigned by some authority
- Have a hierarchical structure
- Geographical location

# why do we need a MAC address at all?

- why not have an IP address per device?
- why not just have only an IP and no link-layer address(es)?
- having different addresses **keep the layers separate**
- each layer needs its own addressing scheme
- Whereas MAC addresses signify the **next hop**, IP addresses indicate the **final destination**

**ARP connects IP to MAC**

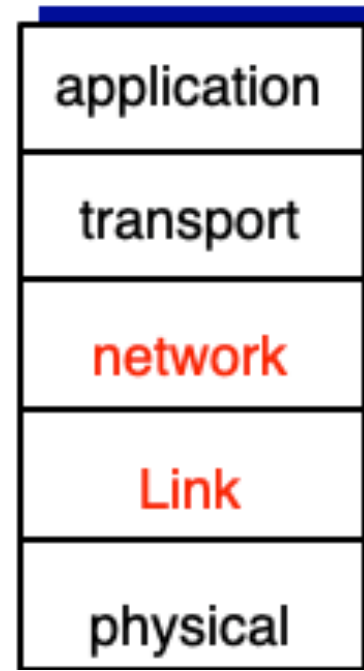
# ARP (address resolution protocol)

- when sending an IP packet to some IP address, the ethernet frame should contain the right MAC address for the next hop.
- However, we usually have the IP address but not the MAC address.

ARP goes from the network layer to the link layer

# how does ARP work?      Postcard example

- a postcard is sent to **Sergio** who lives at some residence building
- the **postman** knows the postcard is for **Sergio** and knows **his address**.
- **transport layer**: recipient's name (**Sergio**)
- **network layer**: **Sergio's** address
- **link layer**: andar 6, fracção Z





# how does ARP work?

## Postcard example

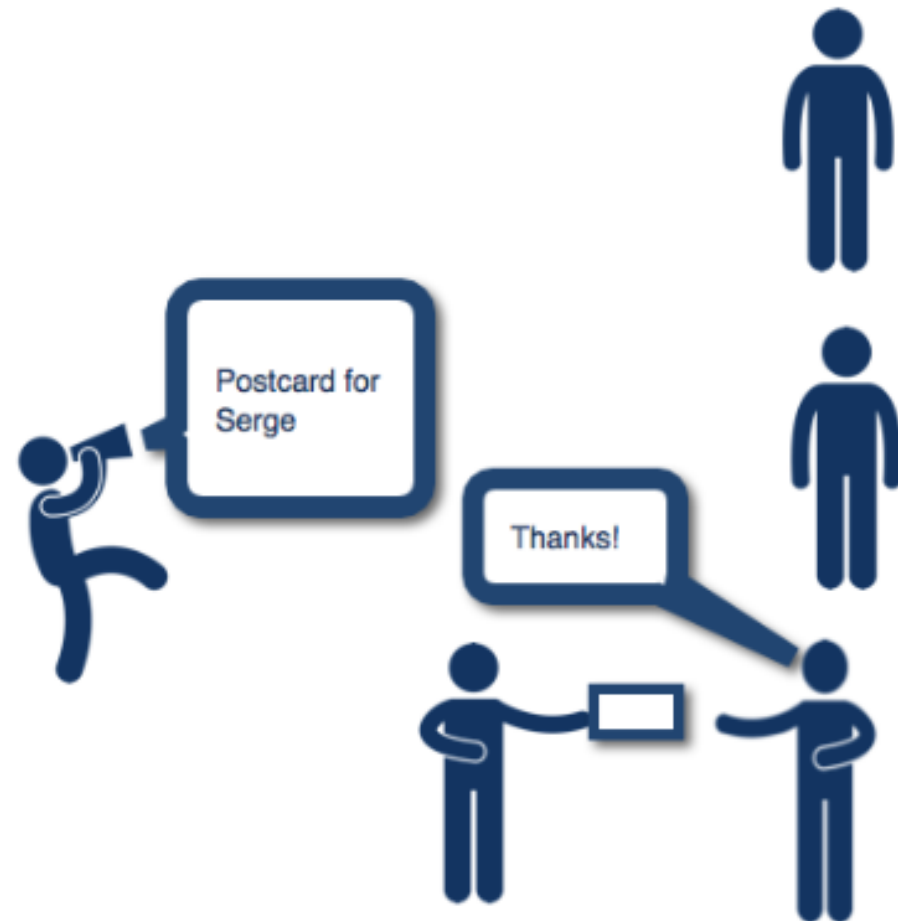
- Using **network routing** the packet has arrived at the final destination.
- The **postman broadcasts** “Where does Sergio live?”
- Everybody hears the **postman's** announcement, including **Sergio**



# how does ARP work?

## Postcard example

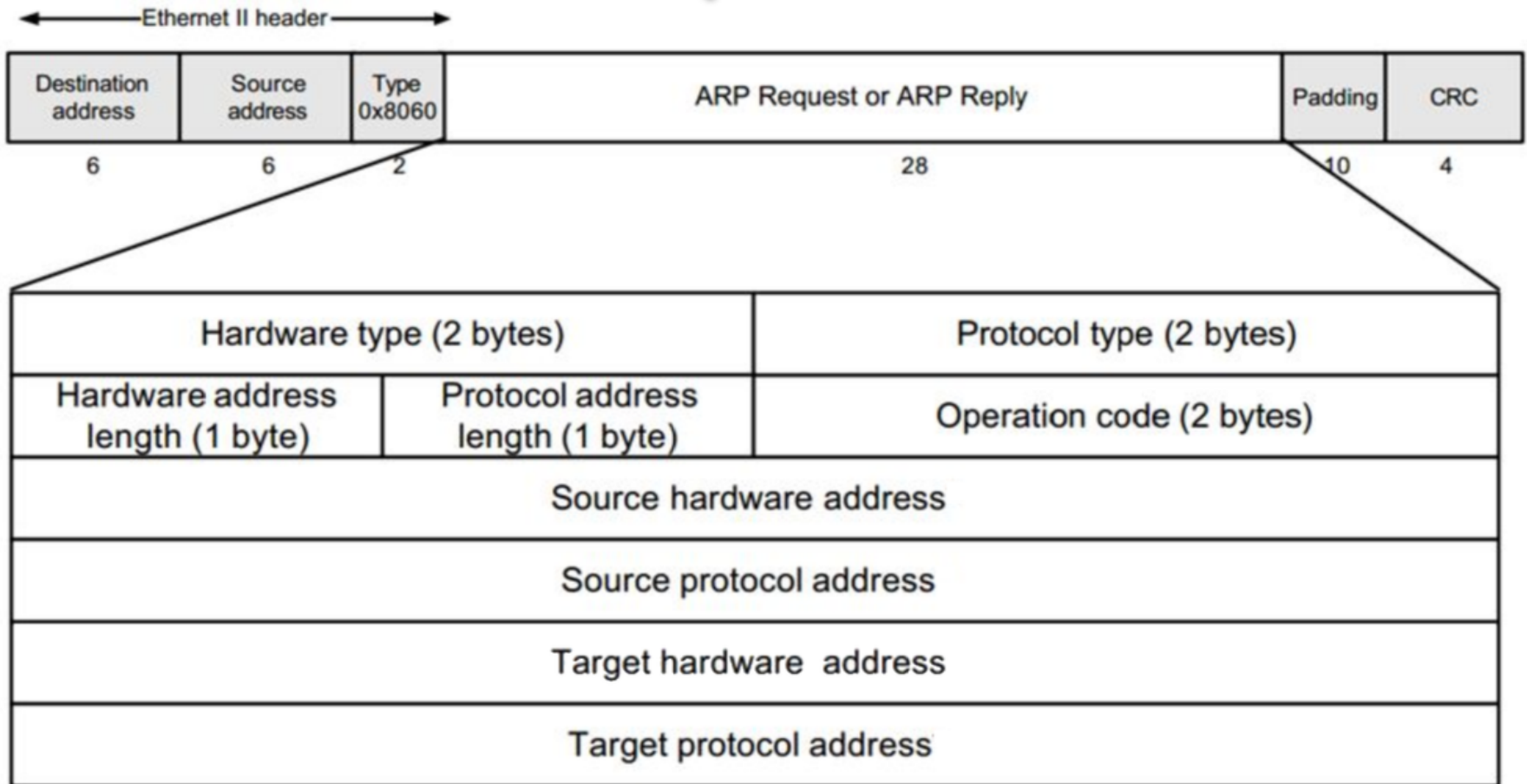
- Sergio would notice it and acknowledge it by shouting his location back ... “I live here”.
- The next time the postman wants to deliver a postcard to Sergio, he won't need to ask again.
  - He will know where and how to find Sergio



# how does ARP work?

1. ARP sends an ethernet **broadcast** query that states the intended destination IP address.
2. If the target device (**Sergio**) is on the network, it sends a message stating its MAC address.
3. ARP stores previous results in a **lookup table** to ensure this process is not repeated for every packet.

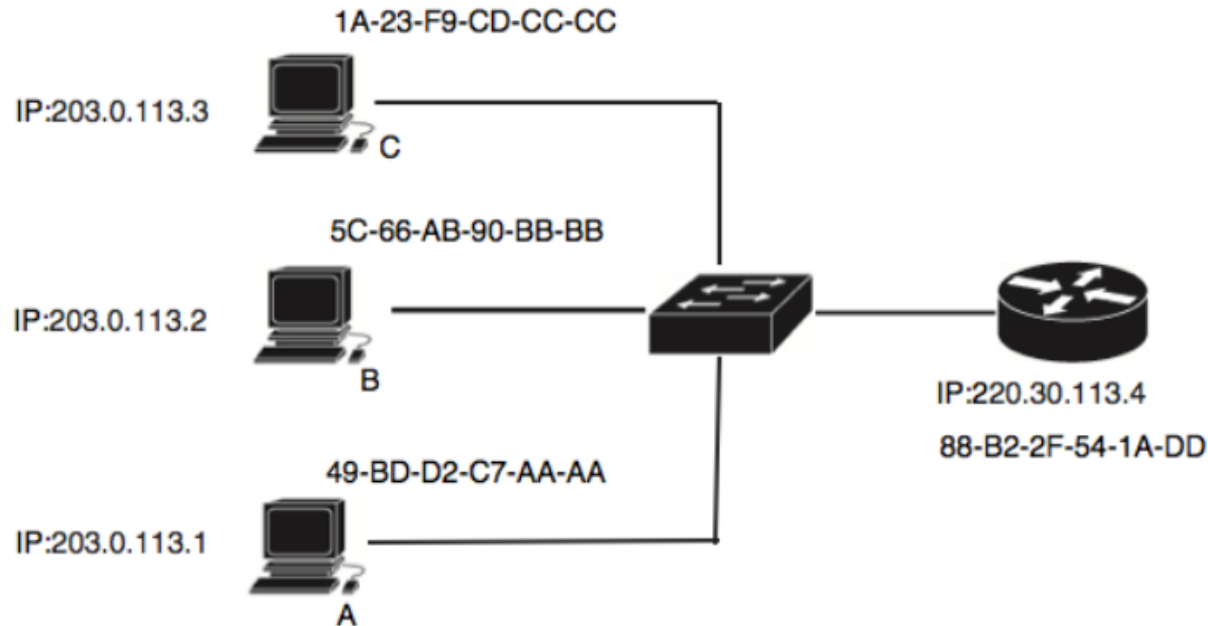
# ARP structure packet



**Type 0x8060 indicates ARP packet**

# how does ARP work?

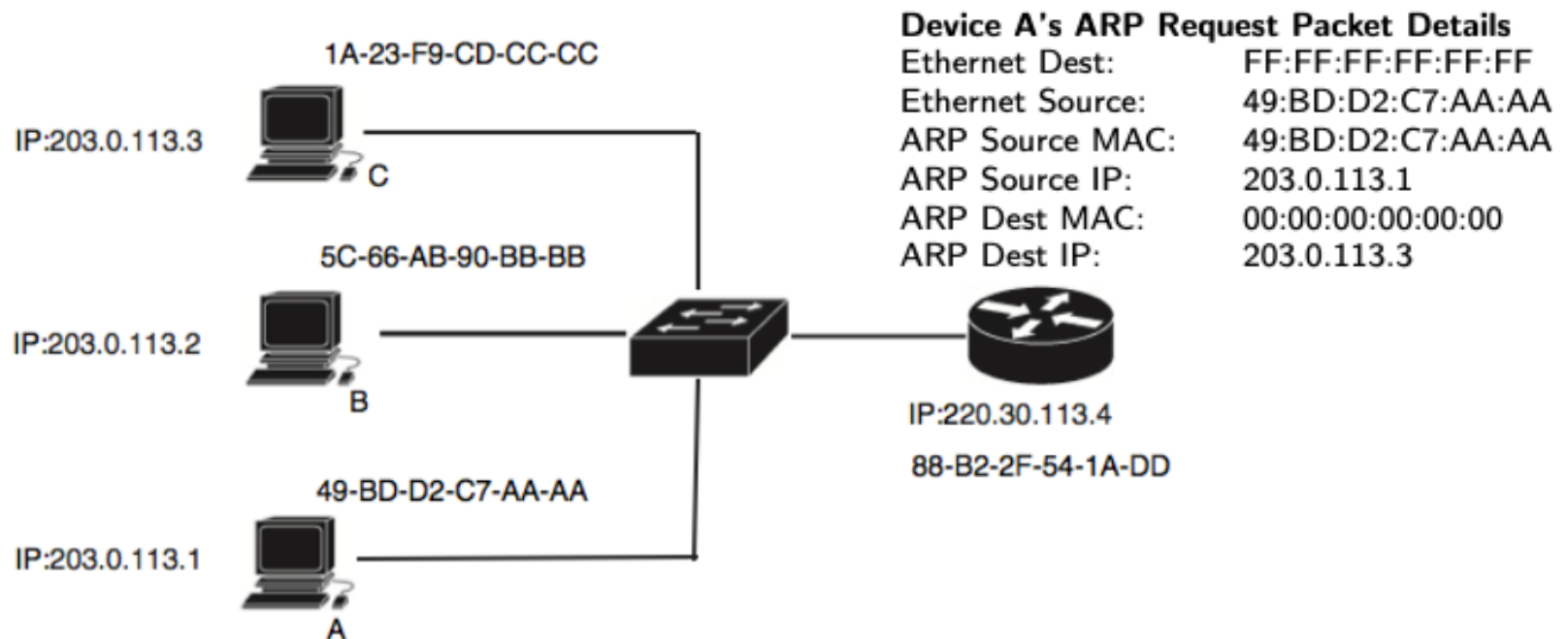
simple network -  
no routing



- A wants to send a message to C
- A knows C's IP address
- A does not know C's MAC address
- C is not in A's ARP table: 00:00:00:00:00:00

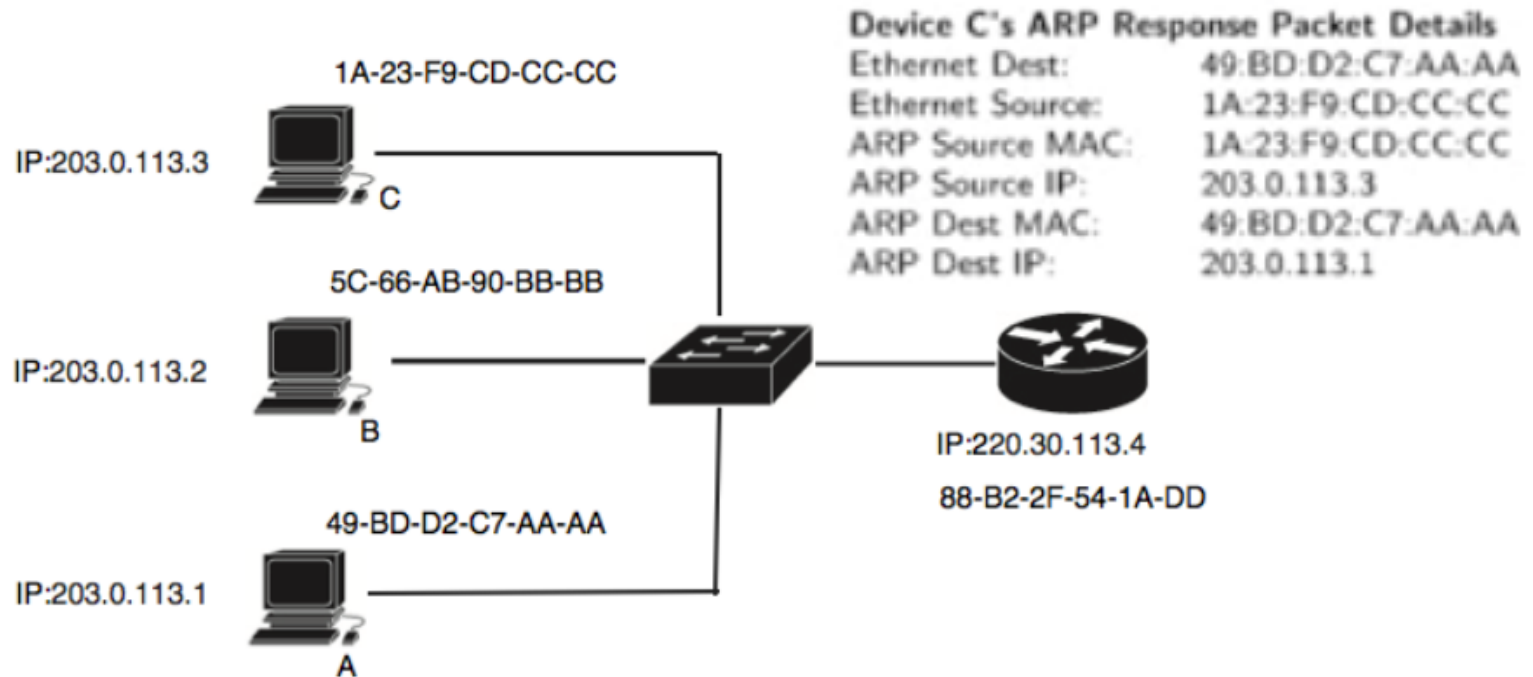
# how does ARP work?

from A to B, C



- A creates an **ARP packet** and **broadcasts** a **Discovery Request**
  - this request is inside an **ethernet frame** (Type = **ARP**)
  - ARP Source IP: A's IP
  - ARP Dest IP: C's IP
  - ARP Source MAC: A's MAC
  - ARP Dest MAC: broadcast address

# how does ARP work? from C to A



- C creates an **ARP packet** and sends a **Response** to A
  - ARP Source IP: C's IP
  - ARP Dest IP: A's IP
  - ARP Source MAC: C's MAC
  - ARP Dest MAC: A's MAC

A then update its ARP table

# Roadmap

1. ARP
2. DHCP (Dynamic Host Control Protocol)
3. DHCP security



# DHCP - Dynamic Host Control Protocol

## Why DHCP?

1. IP addresses can be static or dynamic
2. IP addresses are assigned on the fly
3. Reduce overhead for assigning IP addresses
4. Reduce overhead for managing IP addresses assigned

# DHCP - protocol for a newly added device

1. **DHCP** Server Discovery - finding the **DHCP** server.
2. **DHCP** CP Server Offer Message - providing the client with an IP address
3. **DHCP** Request Message - accepting and requesting the offered IP address.
4. **DHCP** ACK Message - confirming to the client that they are granted the IP address

# DHCP - protocol for a newly added device

e.g., connecting your laptop to the Wi-Fi

- A. The Requester uses an IP broadcast to send out a DHCP Discovery Request
- B. When the DHCP server sees the Request, it picks up the Request and prepares for the next step ...
- C. The server recommends an IP address to the Requester
  - A. Several servers on the network can offer IP addresses
- D. The Laptop accesses one of the offers, which contains information about the server and the IP address to talk to

# Roadmap

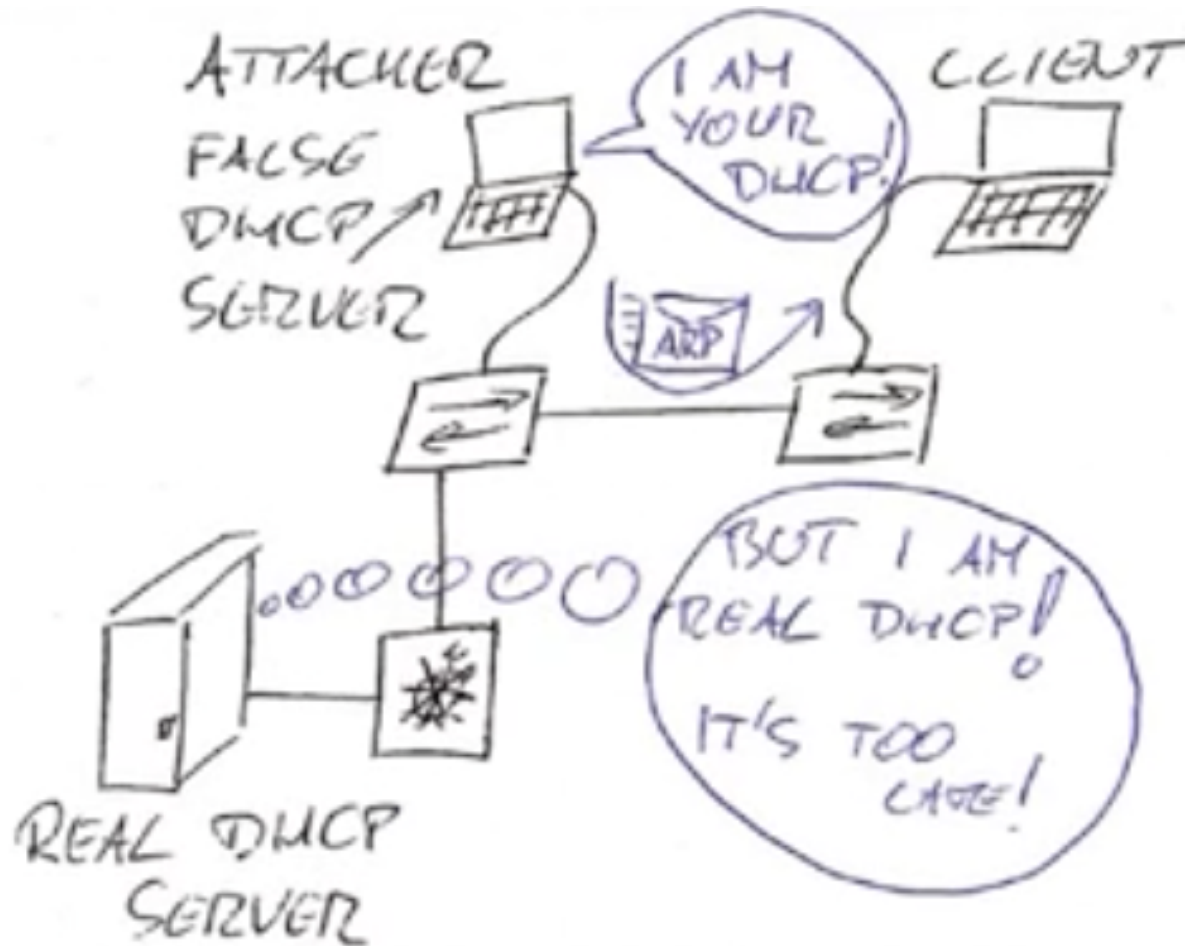
1. ARP
2. DHCP
3. DHCP security

# DHCP Spoofing in 3 steps

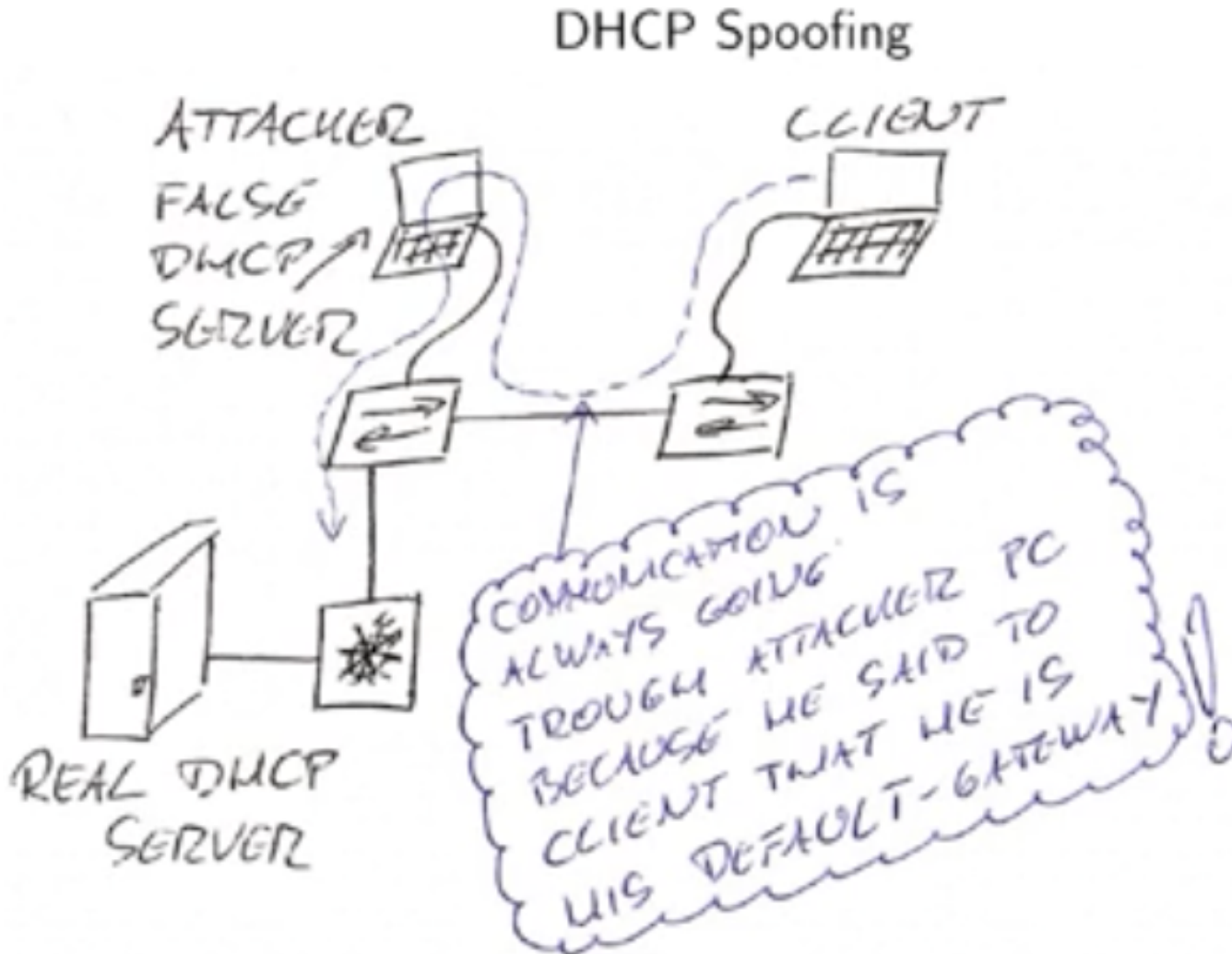
1. **Client** sends a **DHCP Request**.
2. **DHCP Request** responded to by a **false DHCP server** faster than the actual/real server.
3. Traffic from **Client** now goes to some IP which the false DHCP server pointed to.

**Spoofing:** a malicious server provides the client with malicious IP information

# DHCP Spoofing



# DHCP Spoofing



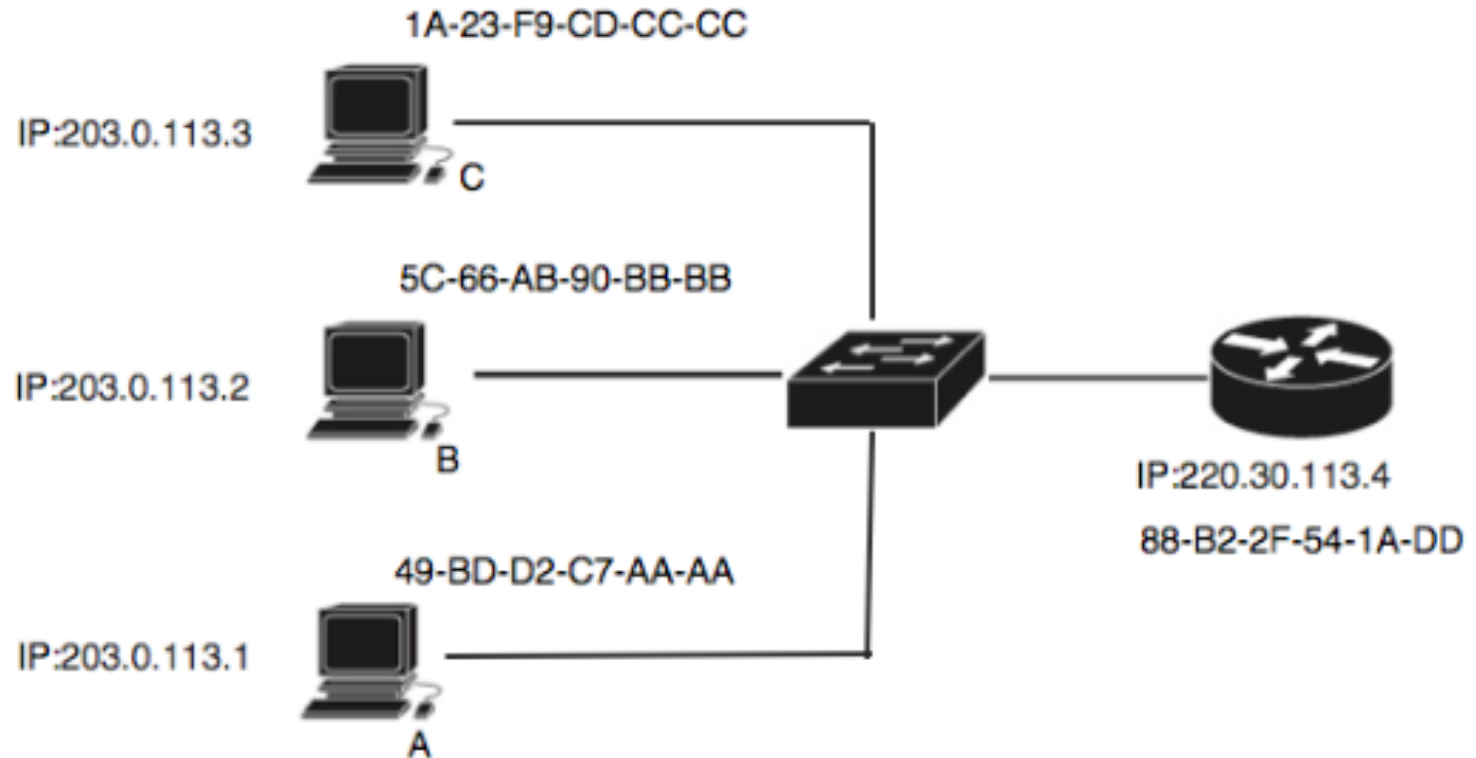
# DHCP starvation

1. An **attacker** creates many clients that make requests to the DHCP server.
2. The **attacker** thus **floods** the DHCP server with requests from MACs that do not exist.
3. DHCP starvation **prevents** legitimate clients (laptops ...) from accessing the network.

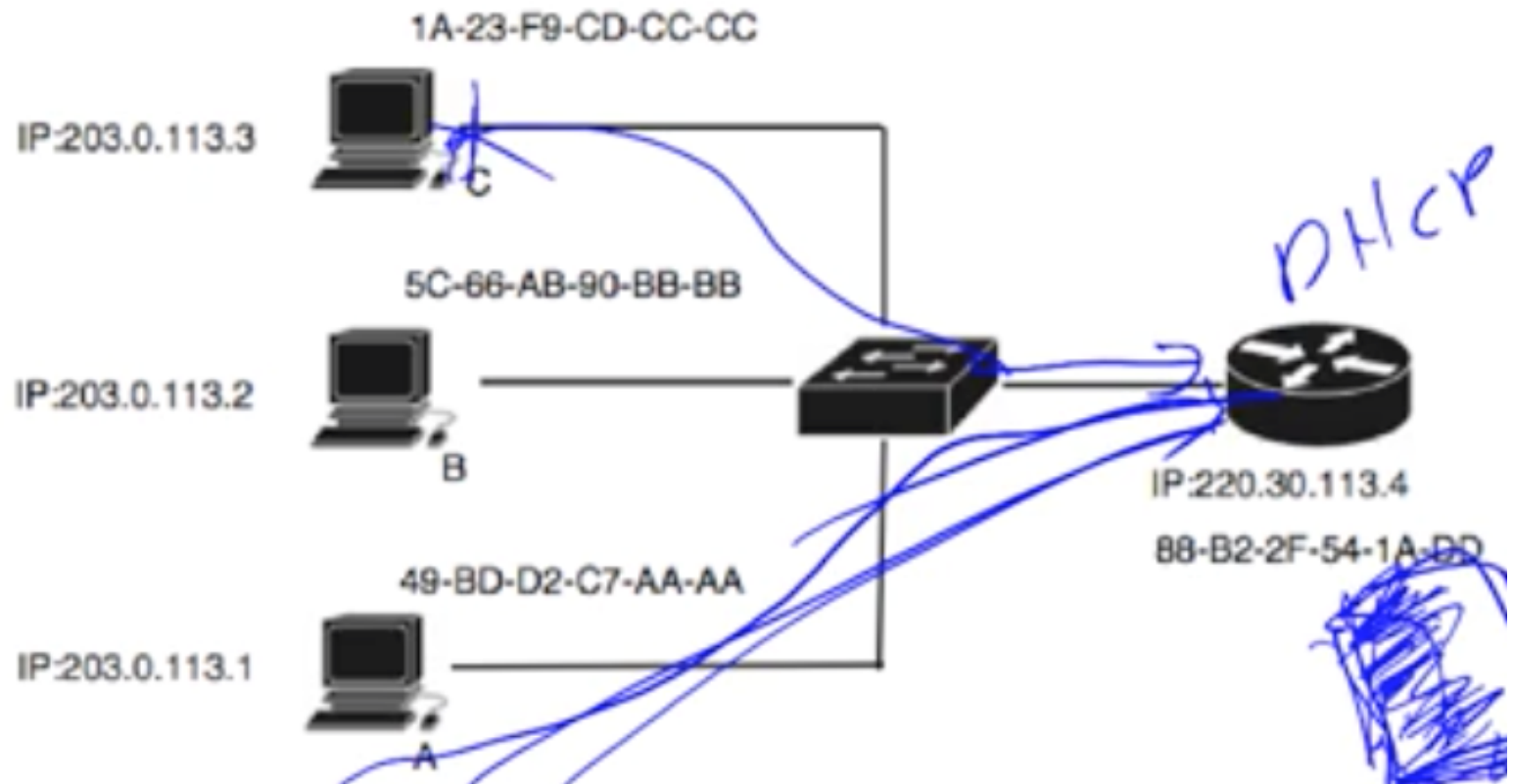
**recall:** a DHCP server responds to a client request with an IP address



# DHCP starvation



# DHCP starvation



# summary

- ARP and DHCP
- DHCP spoofing and starvation attacks