# ARP and DHCP

Goal:

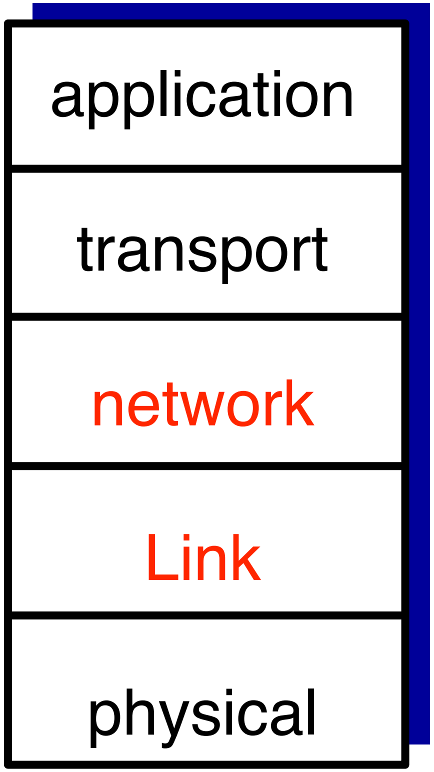
To understand the basic functionality of ARP and DHCP.

# Roadmap

1. ARP
2. DHCP
3. ARP and 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?



application

transport

network

Link

physical

# 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.

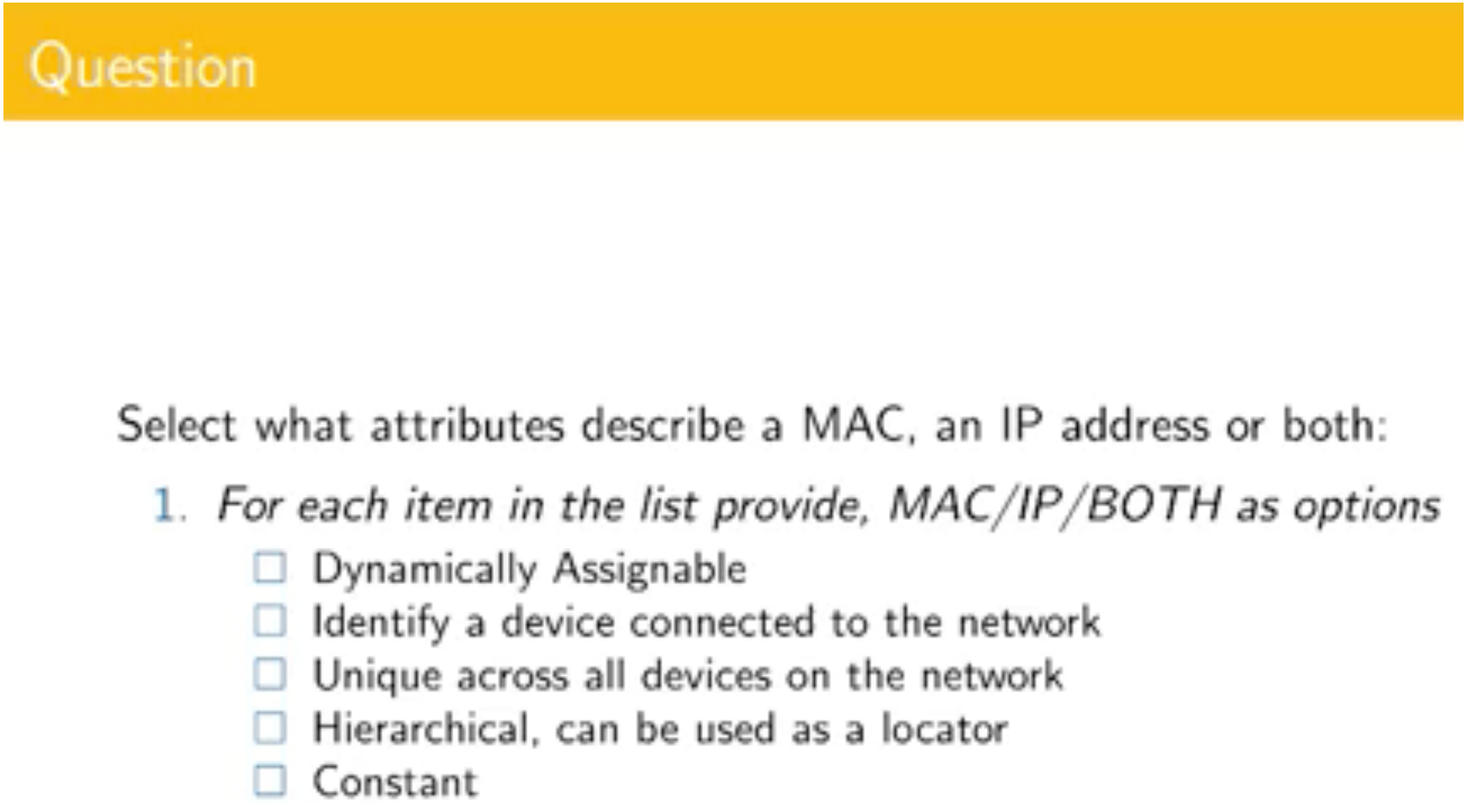
# why have a MAC address at all?

- 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 signify the final destination

ARP: connects IP to MAC

# Question



Question

Select what attributes describe a MAC, an IP address or both:

1. *For each item in the list provide, MAC/IP/BOTH as options*
   - □ Dynamically Assignable
   - □ Identify a device connected to the network
   - □ Unique across all devices on the network
   - □ Hierarchical, can be used as a locator
   - □ Constant

# MAC vs. IP addresses

- MAC addresses
  - Are associated with a network adapter
- IP addresses
  - Not dependent on hardware
  - Assigned by some authority
  - Have a hierarchical structure
    - geographical location

ARP (Address Resolution Protocol)

- It relates MAC addresses with IP addresses

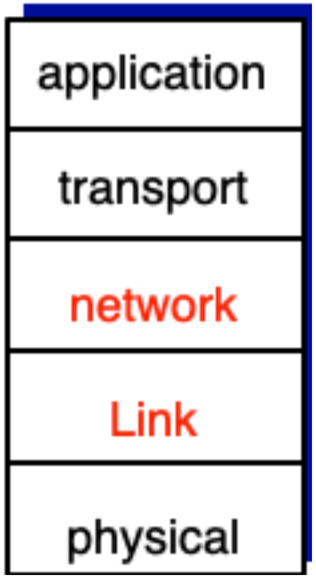
# ARP (address resolution protocol)s

- 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: it goes from the internetwork layer to the link layer.

# how does ARP work? Postcard example

- a postcard is sent to Serge who lives at some residence building
- the Postman knows the postcard is for Serge and knows his address.

- transport layer: recipient’s name (Serge)
- internetwork layer: Serge’s address
- link layer: the mailman brings the postcard



application

transport

network

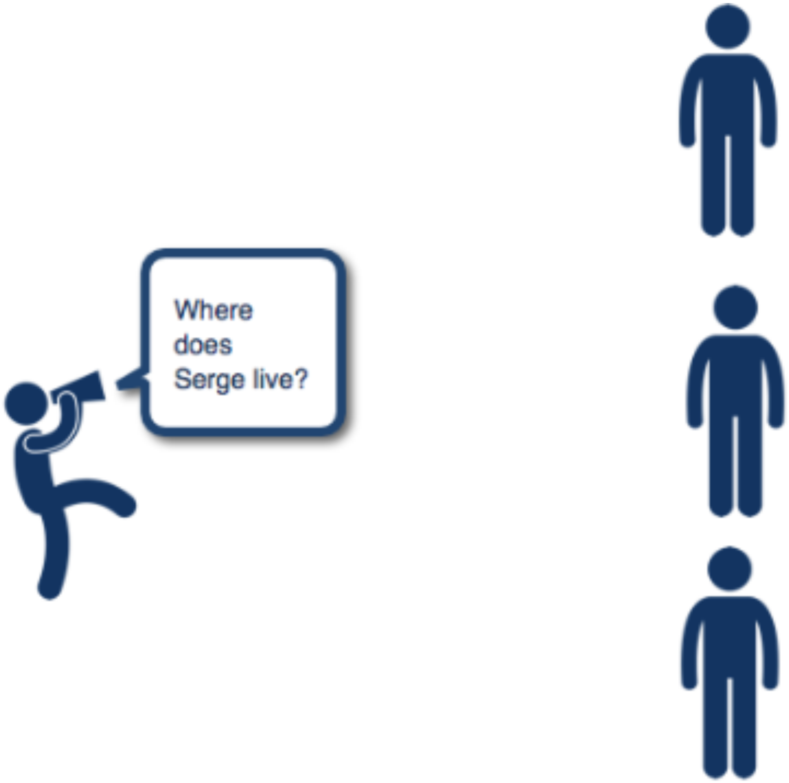
Link

physical

# how does ARP work?

## Postcard example

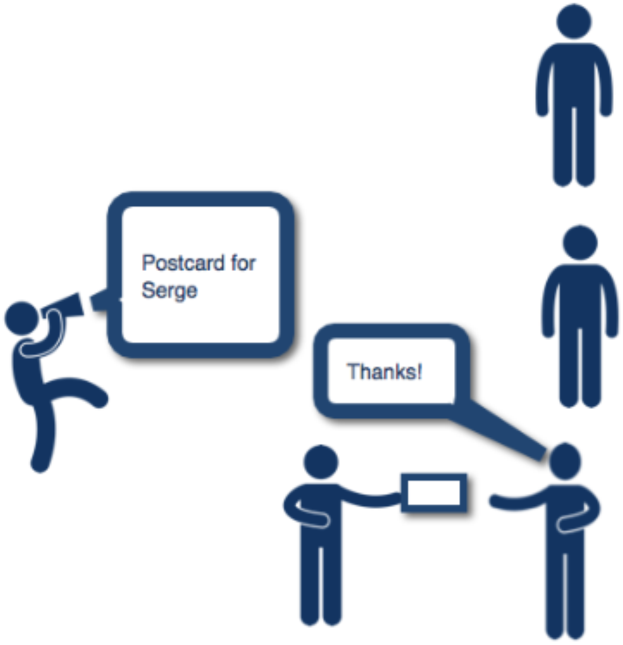
- Using internetwork routing the packet has arrived at the final destination.
- The mailman broadcasts "Where does Serge live?"
- Everybody hears the mailman's announcement, including Serge.



# how does ARP work?

## Postcard example

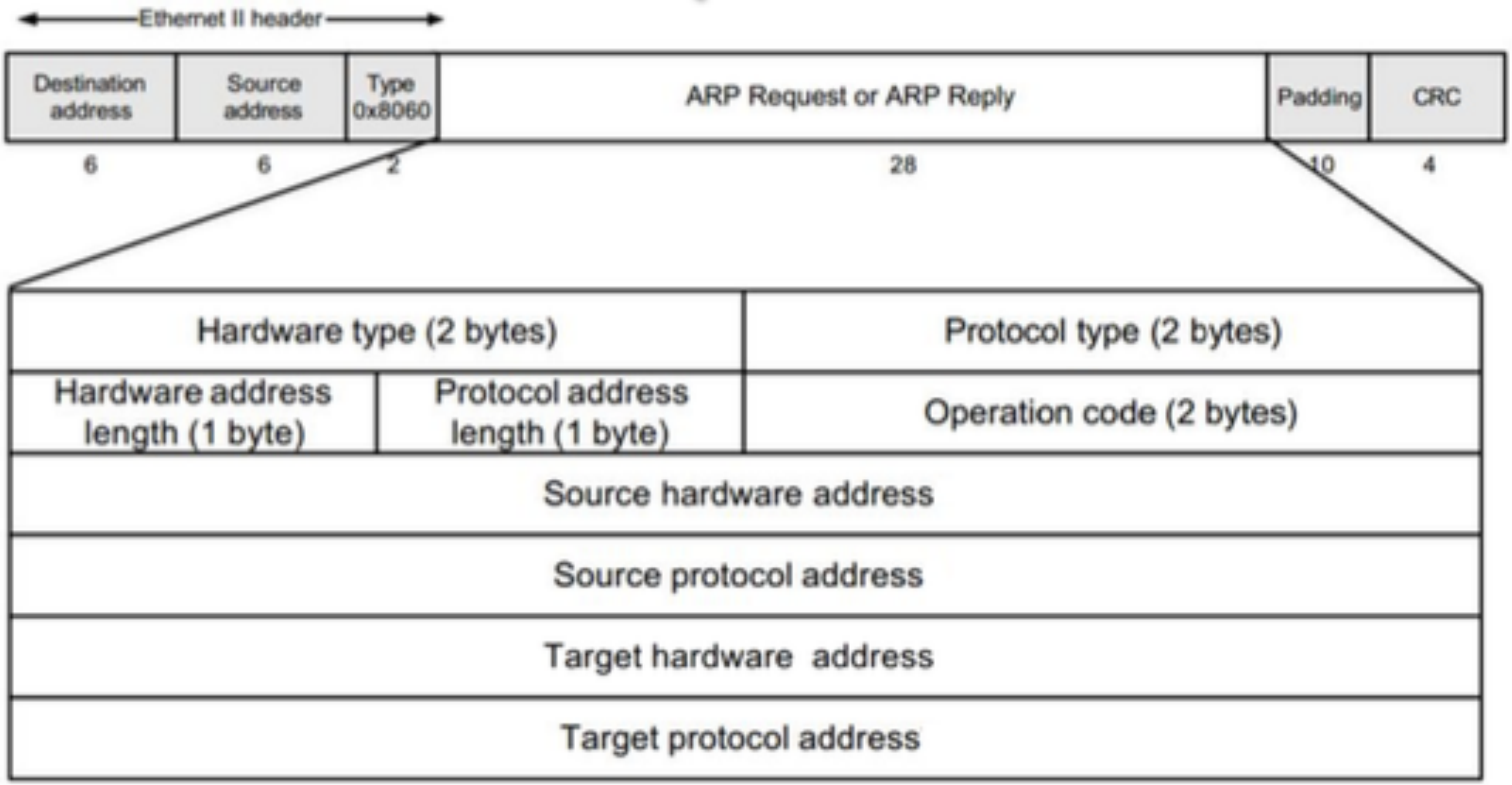
- Serge would notice it and acknowledge it by shouting his location back … "I live here".
- The next time the mailman wants to deliver a postcard to Serge, he won't need to ask again.
    - He will know where and how to find Serge.



# how does ARP work?

- ARP sends an ethernet broadcast query that states the intended destination IP address.
- If the target device is present on the network, it sends a direct non-broadcast reply that states his MAC address.
- To make sure this process is not repeated for every single packet, ARP caches previous results in a lookup table.

# ARP structure packet



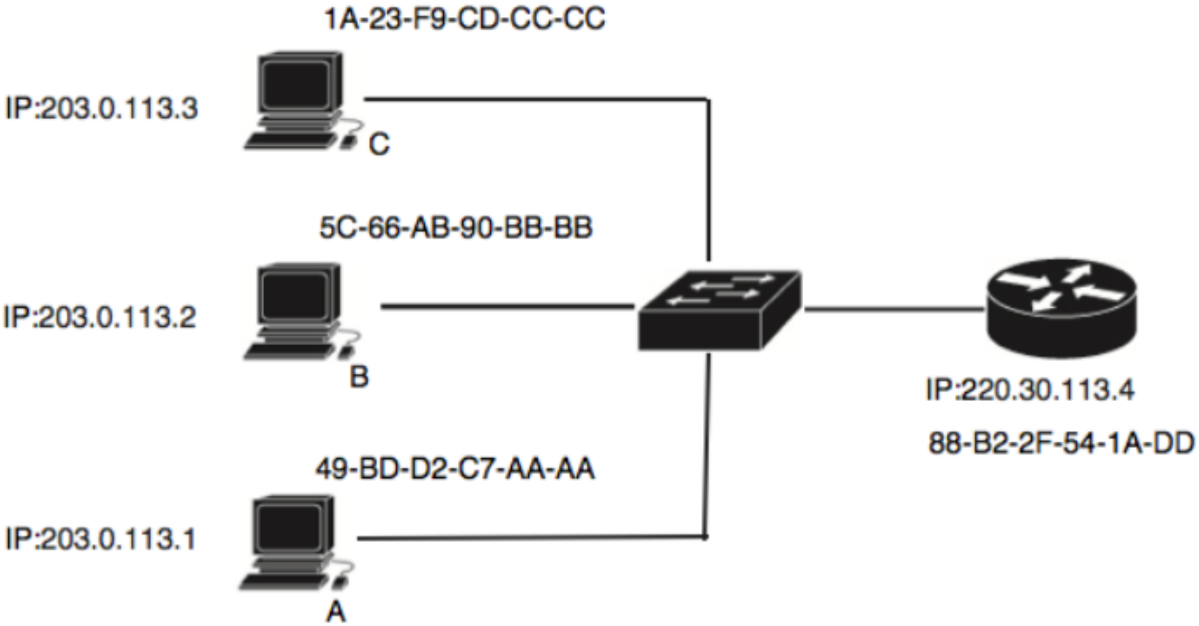
Ethernet II header

| Destination address | Source address | Type 0x8060 | ARP Request or ARP Reply | Padding | CRC |
|---|---|---|---|---|---|
| 6 | 6 | 2 | 28 | 10 | 4 |

| | | |
|---|---|---|
| Hardware type (2 bytes) | | Protocol type (2 bytes) |
| Hardware address length (1 byte) | Protocol address length (1 byte) | Operation code (2 bytes) |
| Source hardware address | | |
| Source protocol address | | |
| Target hardware  address | | |
| Target protocol address | | |

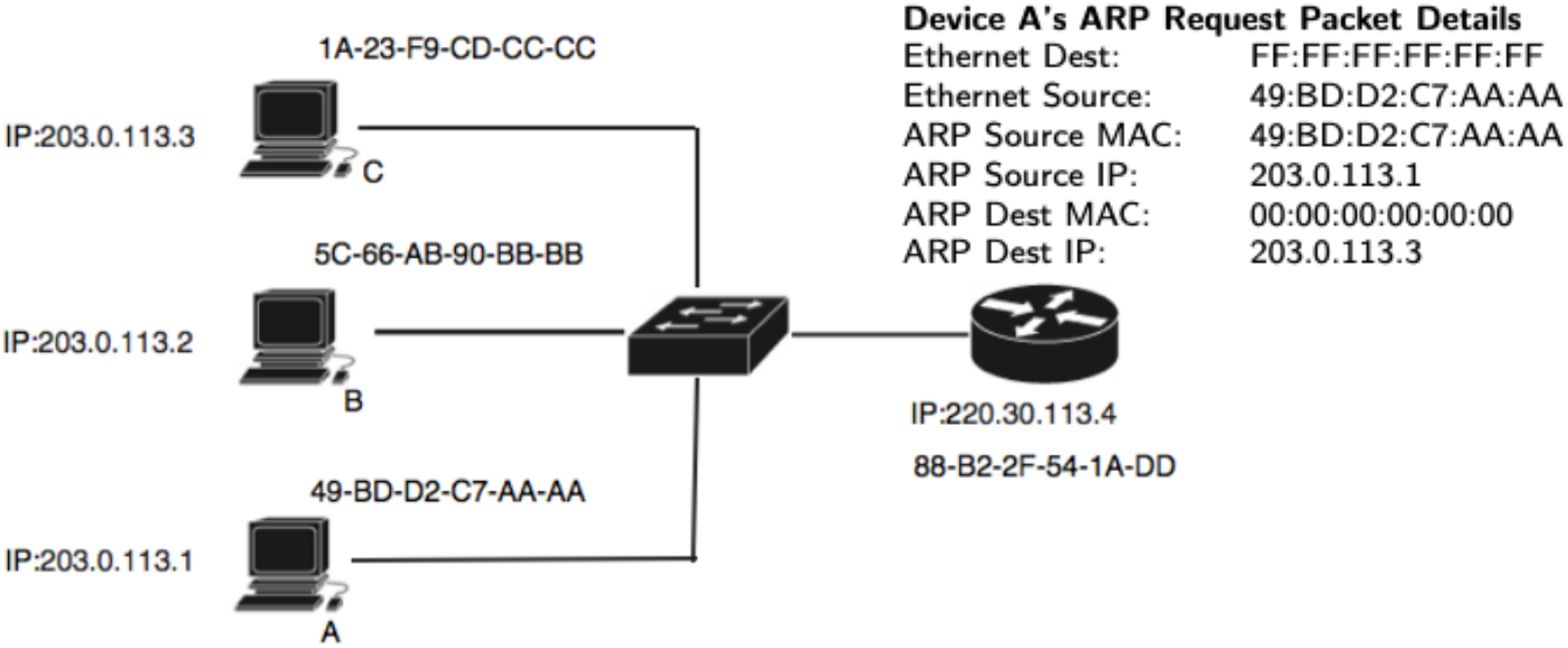
Type 0x8060 = ARP packet

# how does ARP work?



- 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

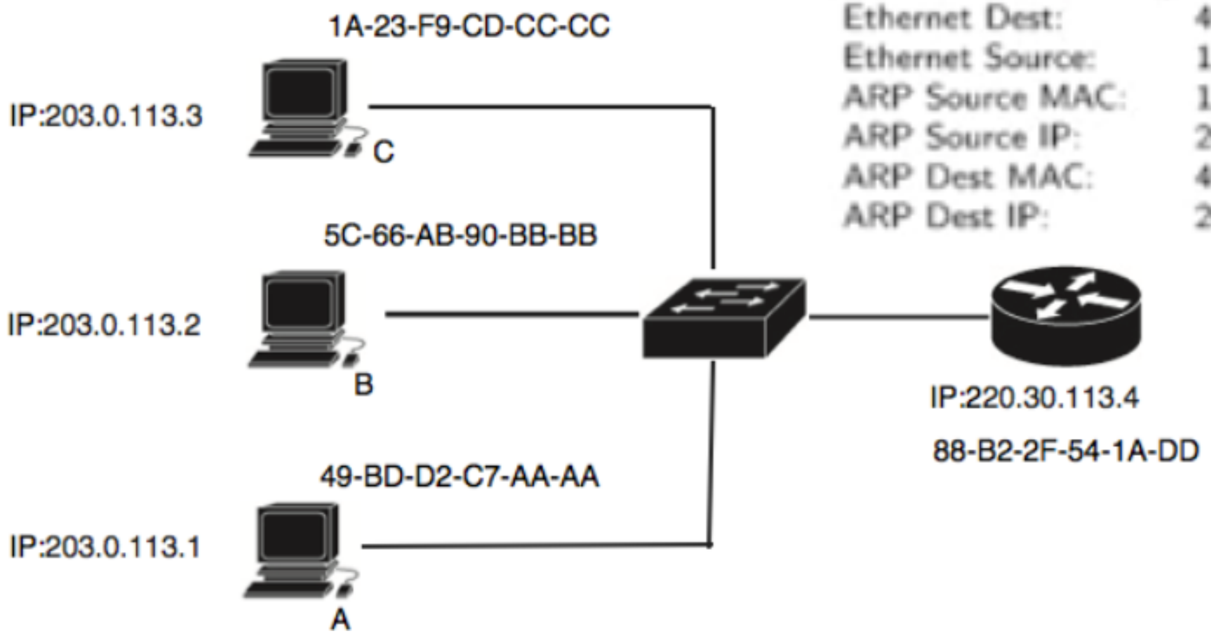


**Device A's ARP Request Packet Details**

| | |
|---|---|
| Ethernet Dest: | FF:FF:FF:FF:FF:FF |
| Ethernet Source: | 49:BD:D2:C7:AA:AA |
| ARP Source MAC: | 49:BD:D2:C7:AA:AA |
| ARP Source IP: | 203.0.113.1 |
| ARP Dest MAC: | 00:00:00:00:00:00 |
| ARP Dest IP: | 203.0.113.3 |

- 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

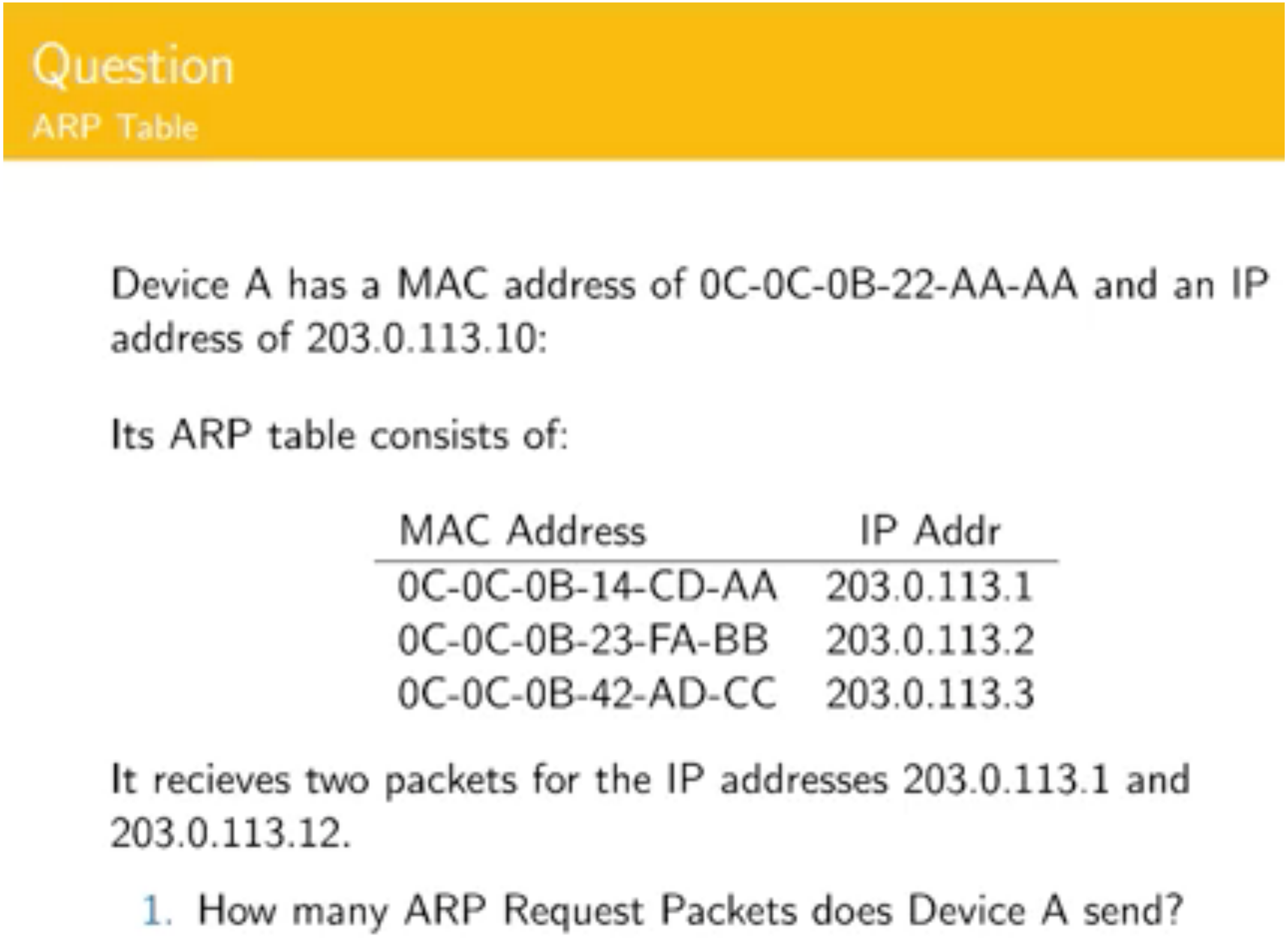


| Device C's ARP Response Packet Details | |
|---|---|
| Ethernet Dest: | 49:BD:D2:C7:AA:AA |
| Ethernet Source: | 1A:23:F9:CD:CC:CC |
| ARP Source MAC: | 1A:23:F9:CD:CC:CC |
| ARP Source IP: | 203.0.113.3 |
| ARP Dest MAC: | 49:BD:D2:C7:AA:AA |
| ARP Dest IP: | 203.0.113.1 |

- 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

# Question



## Question

ARP Table

Device A has a MAC address of 0C-0C-0B-22-AA-AA and an IP address of 203.0.113.10:

Its ARP table consists of:

| MAC Address | IP Addr |
|---|---|
| 0C-0C-0B-14-CD-AA | 203.0.113.1 |
| 0C-0C-0B-23-FA-BB | 203.0.113.2 |
| 0C-0C-0B-42-AD-CC | 203.0.113.3 |

It recieves two packets for the IP addresses 203.0.113.1 and 203.0.113.12.

1. How many ARP Request Packets does Device A send?

# Roadmap

1. ARP
2. DHCP
3. ARP and DHCP security

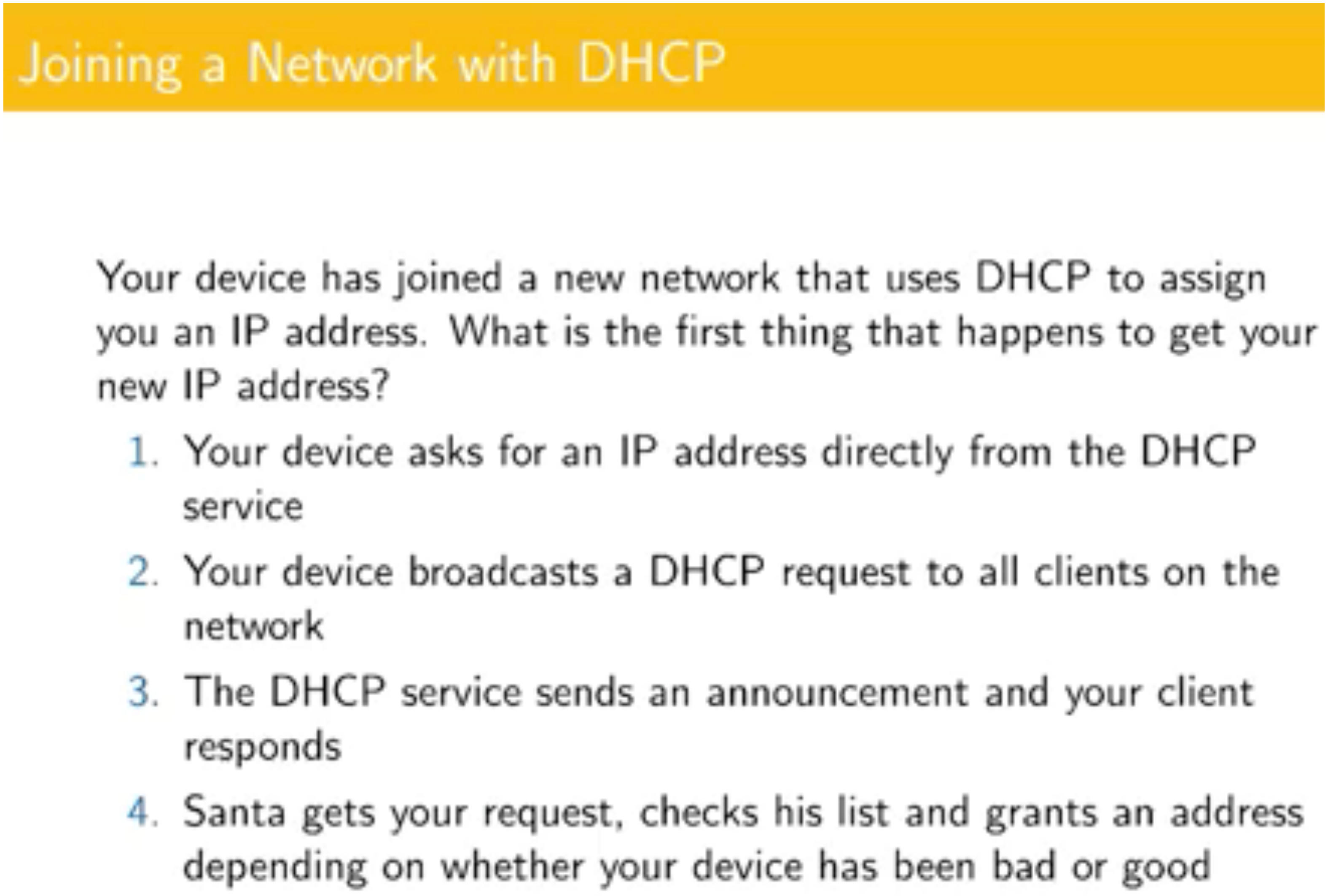
# DHCP - Dynamic Hosting Control Protocol

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

# DHCP - newly added device

1. DHCP Server Discovery - finding the DHCP server.
2. DHCP 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

# Question



## Joining a Network with DHCP

Your device has joined a new network that uses DHCP to assign you an IP address. What is the first thing that happens to get your new IP address?

1. Your device asks for an IP address directly from the DHCP service
2. Your device broadcasts a DHCP request to all clients on the network
3. The DHCP service sends an announcement and your client responds
4. Santa gets your request, checks his list and grants an address depending on whether your device has been bad or good

# Roadmap

1. ARP
2. DHCP
3. ARP and 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 an IP the false DHCP server pointed to.

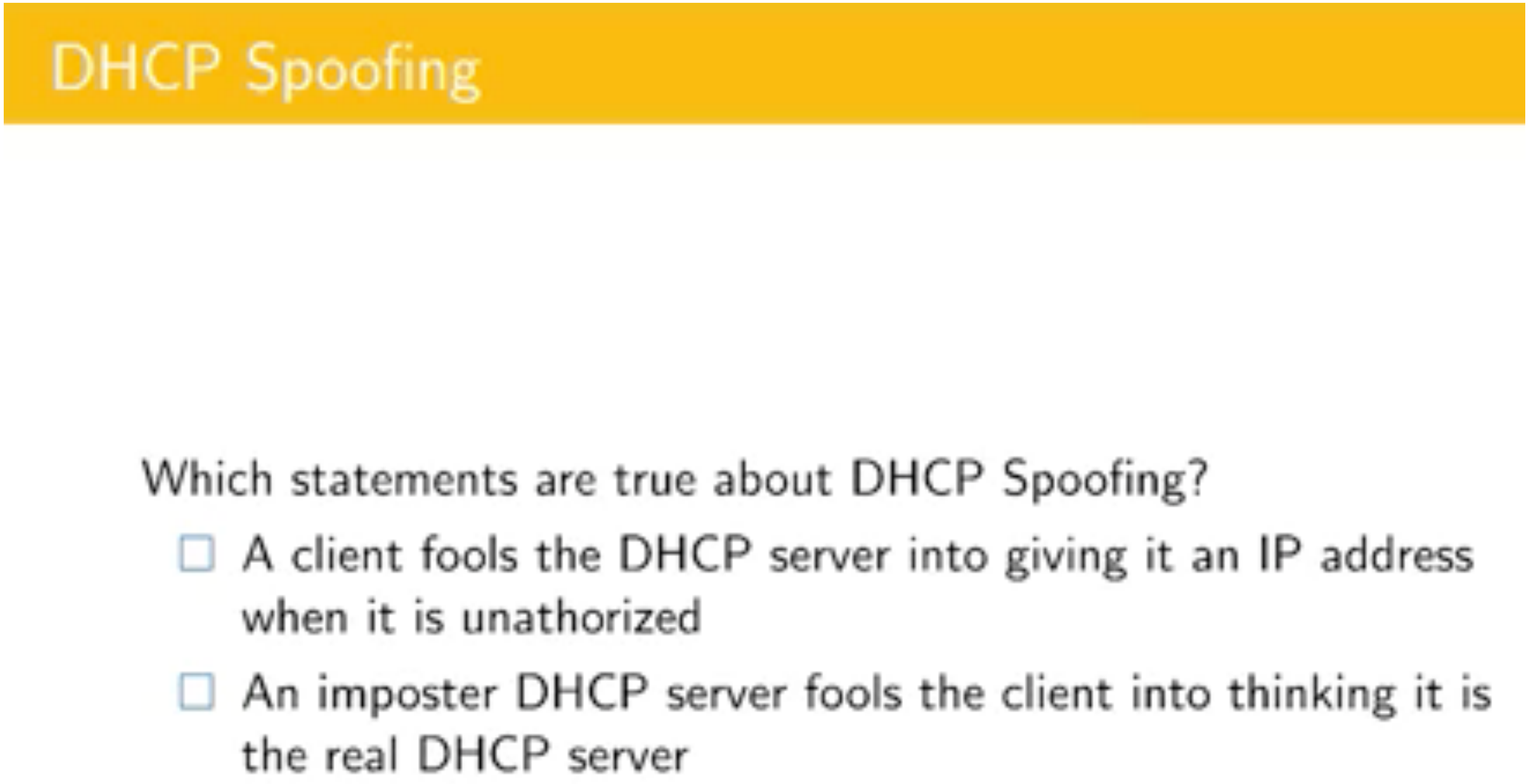
Spoofing: a malicious server provides the client with malicious IP information

# 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, cell phones) from accessing the network.

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

# Question



## DHCP Spoofing

Which statements are true about DHCP Spoofing?

- □ A client fools the DHCP server into giving it an IP address when it is unathorized
- □ An imposter DHCP server fools the client into thinking it is the real DHCP server

# summary

- ARP and DHCP
- DHCP spoofing and starvation attacks