CSCI 466: Networks

Link Layer: Addressing, LANs, ARP

Reese Pearsall

Fall 2023

Announcements

Next week’s quiz will be on Wednesday

No class Friday (Veterans Day)

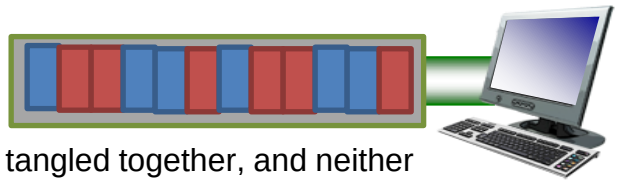
PA2 Grades

Multiple Access Links

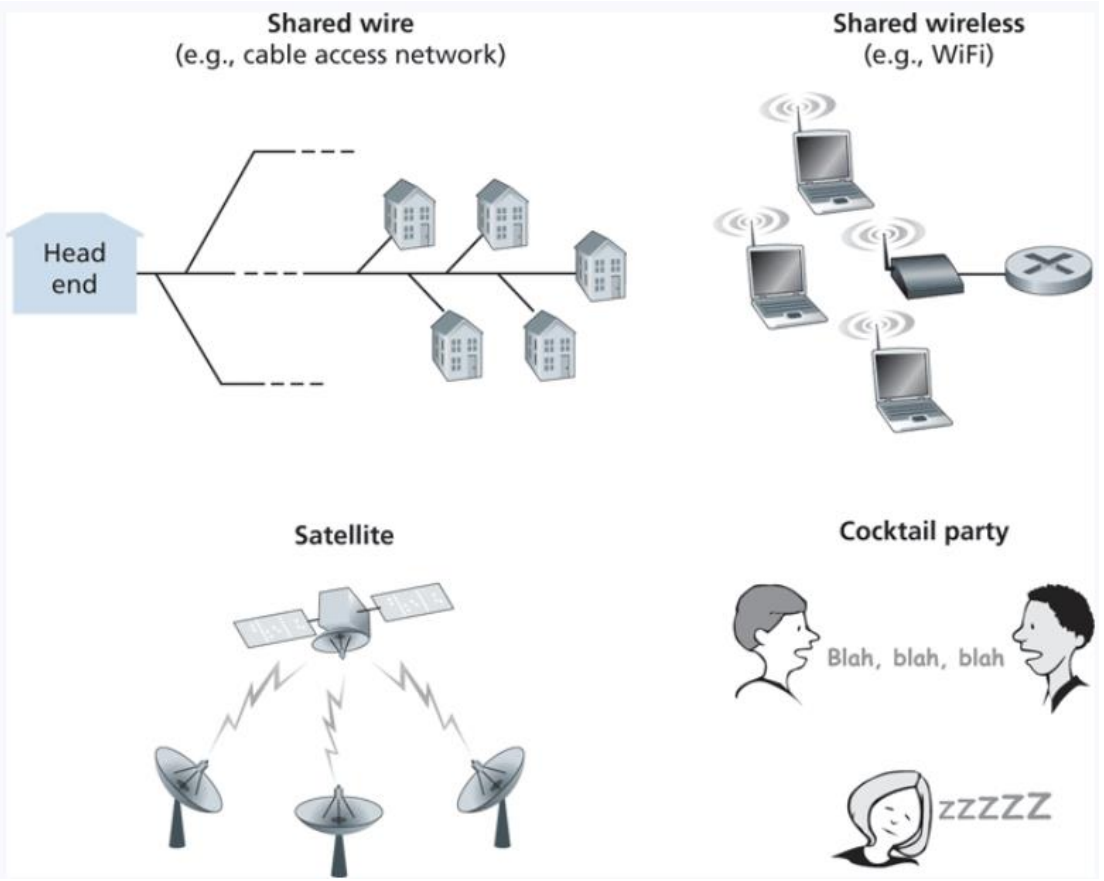
Shared medium = possibility for receivers to get two frame at the same time, AKA a **collision**

Frame X

Frame y



Frames get tangled together, and neither frame can be read clearly by receiver

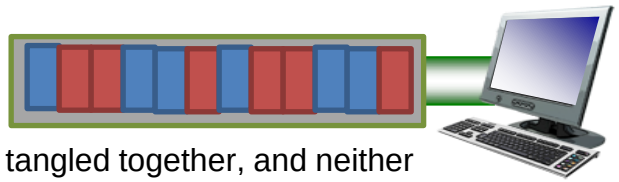


Multiple Access Links

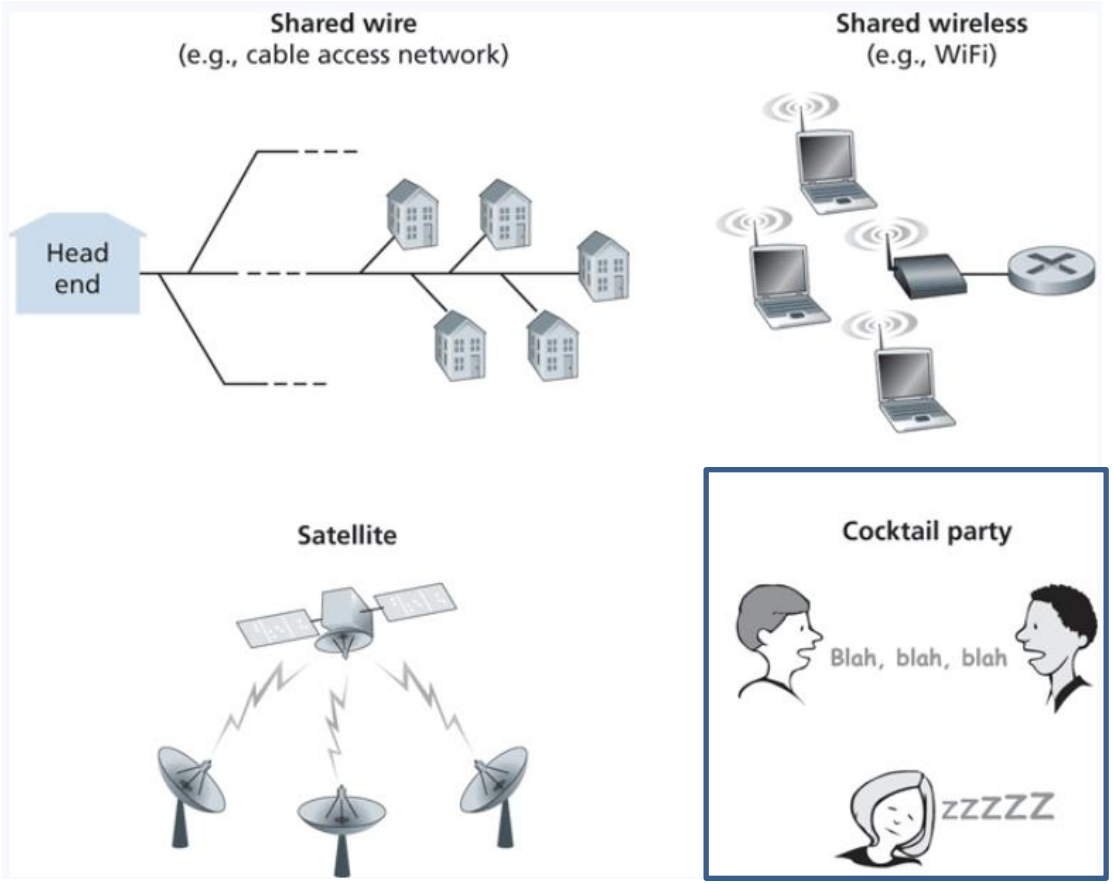
Shared medium = possibility for receivers to get two frame at the same time, AKA a **collision**

Frame X

Frame y



Frames get tangled together, and neither frame can be read clearly by receiver



"Give everyone a chance to speak."

"Don't speak until you are spoken to."

"Don't monopolize the conversation."

"Raise your hand if you have a question."

"Don't interrupt when someone is speaking."

"Don't fall asleep when someone is talking."

In English, we have some rules to prevent collisions from happening

In the link layer, we will discuss 3 multiple access protocols:
Channel Partitioning, **Random Access**, and **Taking Turns**

Random Access

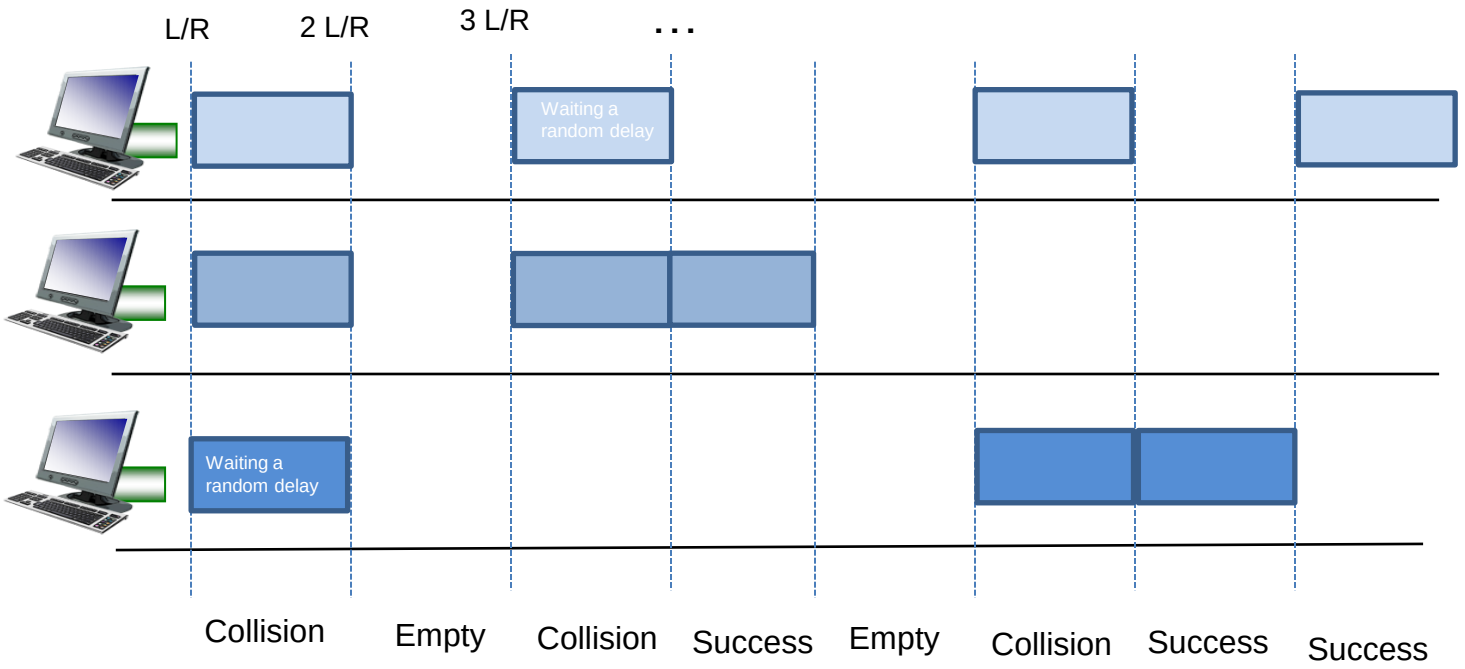
Collisions will occur, but we will try to *recover* from them

Slotted ALOHA: Divide up time into discrete L/R “slots”

If collisions occur, the colliding nodes will flip a coin to see who should retransmit

L = size of frame
R = Bandwidth

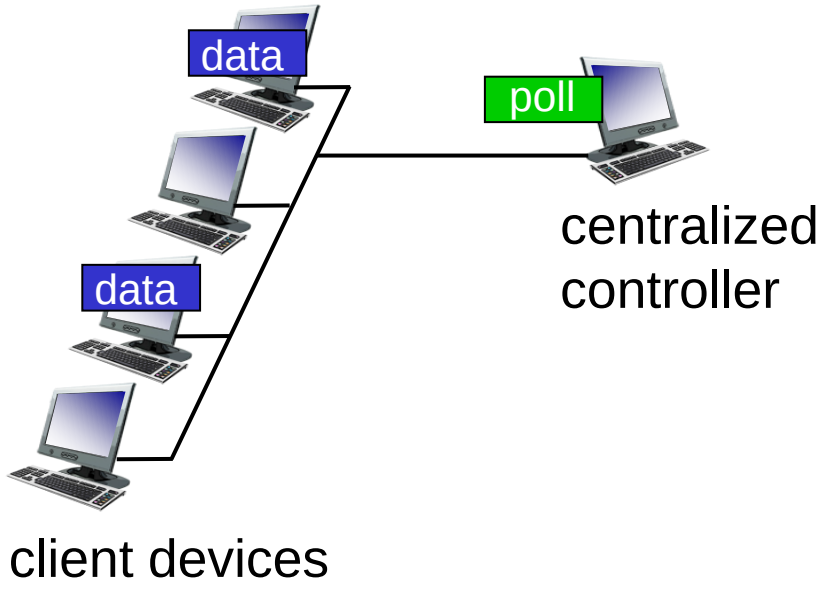
L/R = Time needed to transmit one frame



“Taking turns” MAC protocols

polling:

- centralized controller “invites” other nodes to transmit in turn
- typically used with “dumb” devices
- concerns:
  - polling overhead
  - latency
  - single point of failure (master)
- Bluetooth uses polling

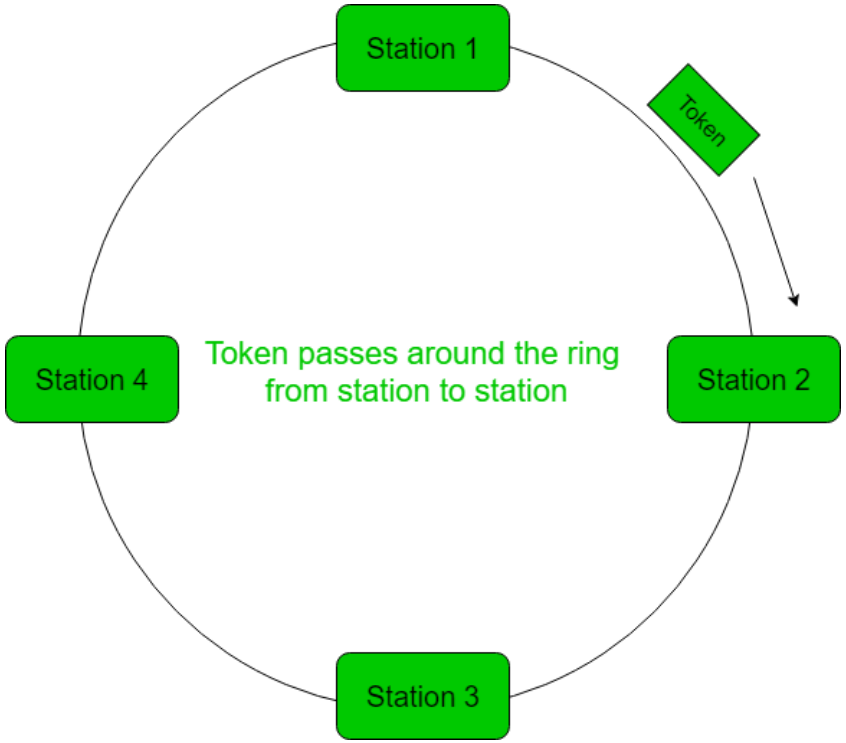


Taking Turns

Token Passing

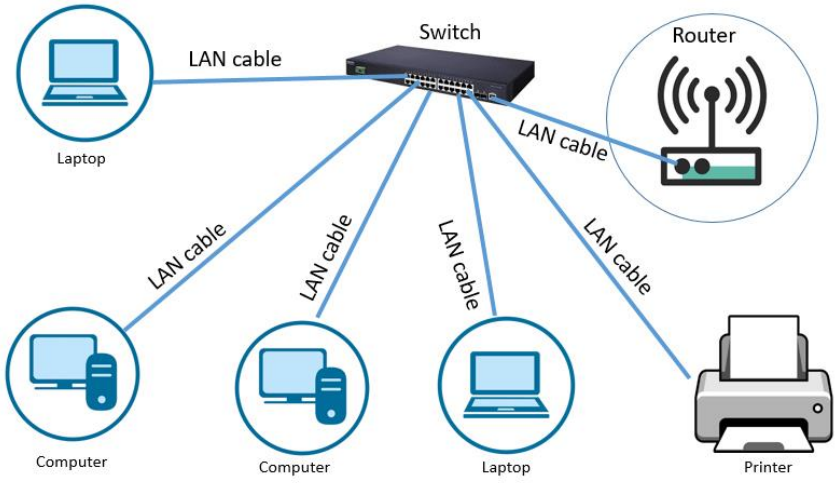
Nodes are connected in a circular manner, and pass a special frame (token) between each other

Can only transmit messages if you have the token

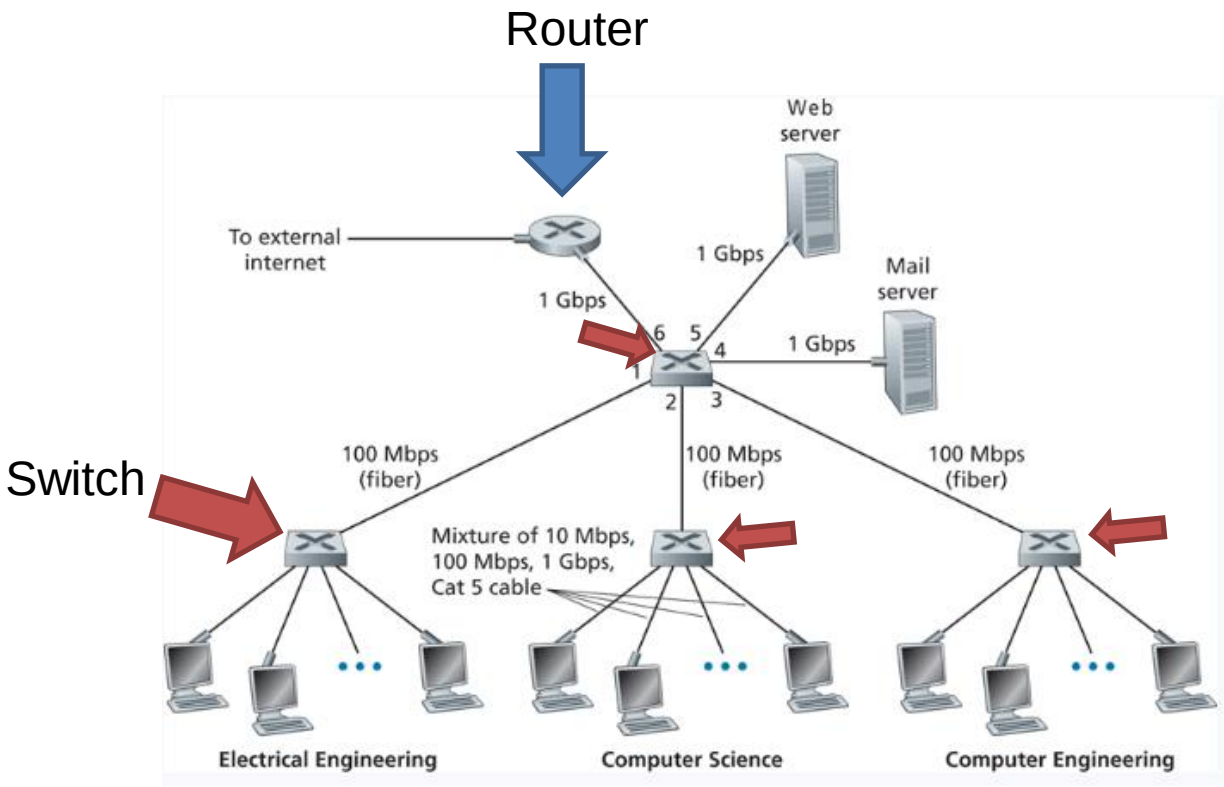


LAN

Local Area Network (LAN)- A collection of devices in one physical location, typically that share a centralized internet connection



Local Area Network



(Within a LAN, we could have several Subnets)

MAC addresses

- 32-bit IP address:
  - *network-layer* address for interface
  - used for layer 3 (network layer) forwarding
  - e.g.: 128.119.40.136
- MAC (or LAN or physical or Ethernet) address:
  - function: used "locally" to get frame from one interface to another physically-connected interface (same subnet, in IP-addressing sense)
  - 48-bit MAC address (for most LANs) burned in NIC ROM, also sometimes software settable
  - e.g.: 1A-2F-BB-76-09-AD

hexadecimal (base 16) notation
(each "numeral" represents 4 bits)

Why do we need MAC addresses?

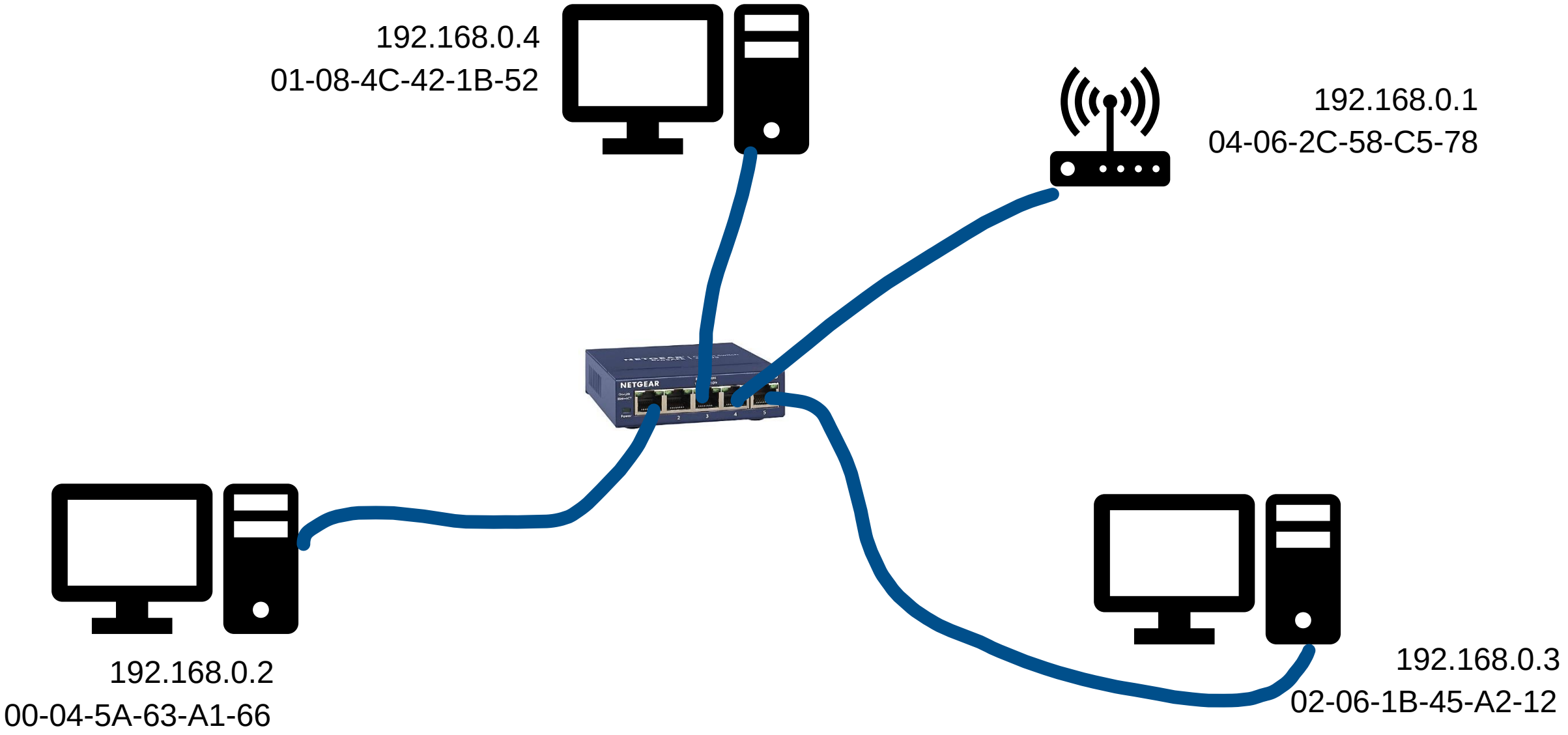
We need a way to *physically identify* a device on a network

IP addresses change frequently, but a MAC address will always be the same

An IP address is used to locate a device, a MAC address is used to identify a device

IP Address = Street Address, MAC Address = Name of person living in House

We need both an IP address and a MAC address to transmit a message


192.168.0.4
01-08-4C-42-1B-52
192.168.0.1
04-06-2C-58-C5-78
NETGEAR
192.168.0.2
00-04-5A-63-A1-66
192.168.0.3
02-06-1B-45-A2-12

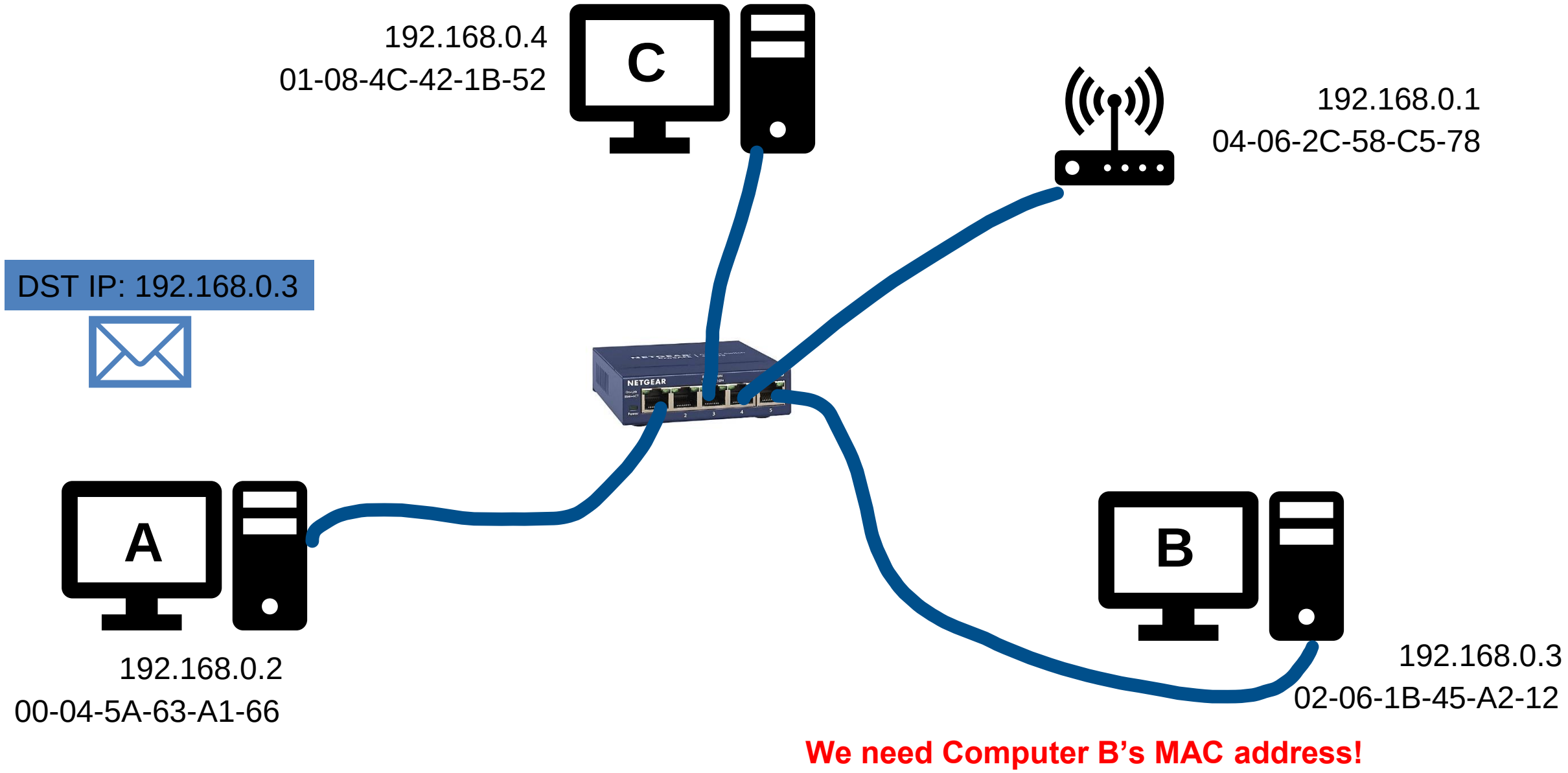
192.168.0.4
01-08-4C-42-1B-52

192.168.0.1
04-06-2C-58-C5-78

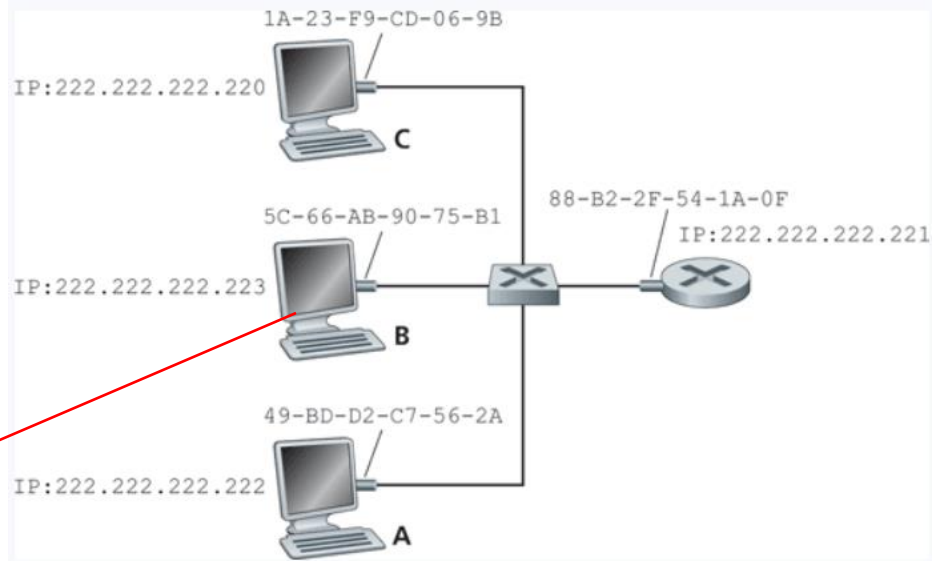
DST IP: 192.168.0.3

192.168.0.2
00-04-5A-63-A1-66

192.168.0.3
02-06-1B-45-A2-12


192.168.0.4
01-08-4C-42-1B-52
C
192.168.0.1
04-06-2C-58-C5-78
DST IP: 192.168.0.3
NETGEAR
A
B
192.168.0.2
00-04-5A-63-A1-66
192.168.0.3
02-06-1B-45-A2-12
We need Computer B's MAC address!

ARP



Protocol for mapping **IP Addresses** to **MAC addresses**

Used *only* for hosts and router interfaces **on the same subnet**

First the machine checks its **ARP table**

IP Address	MAC Address	TTL
222.222.222.221	88-B2-2F-54-1A-0F	13:45:00
222.222.222.223	5C-66-AB-90-75-B1	13:52:00

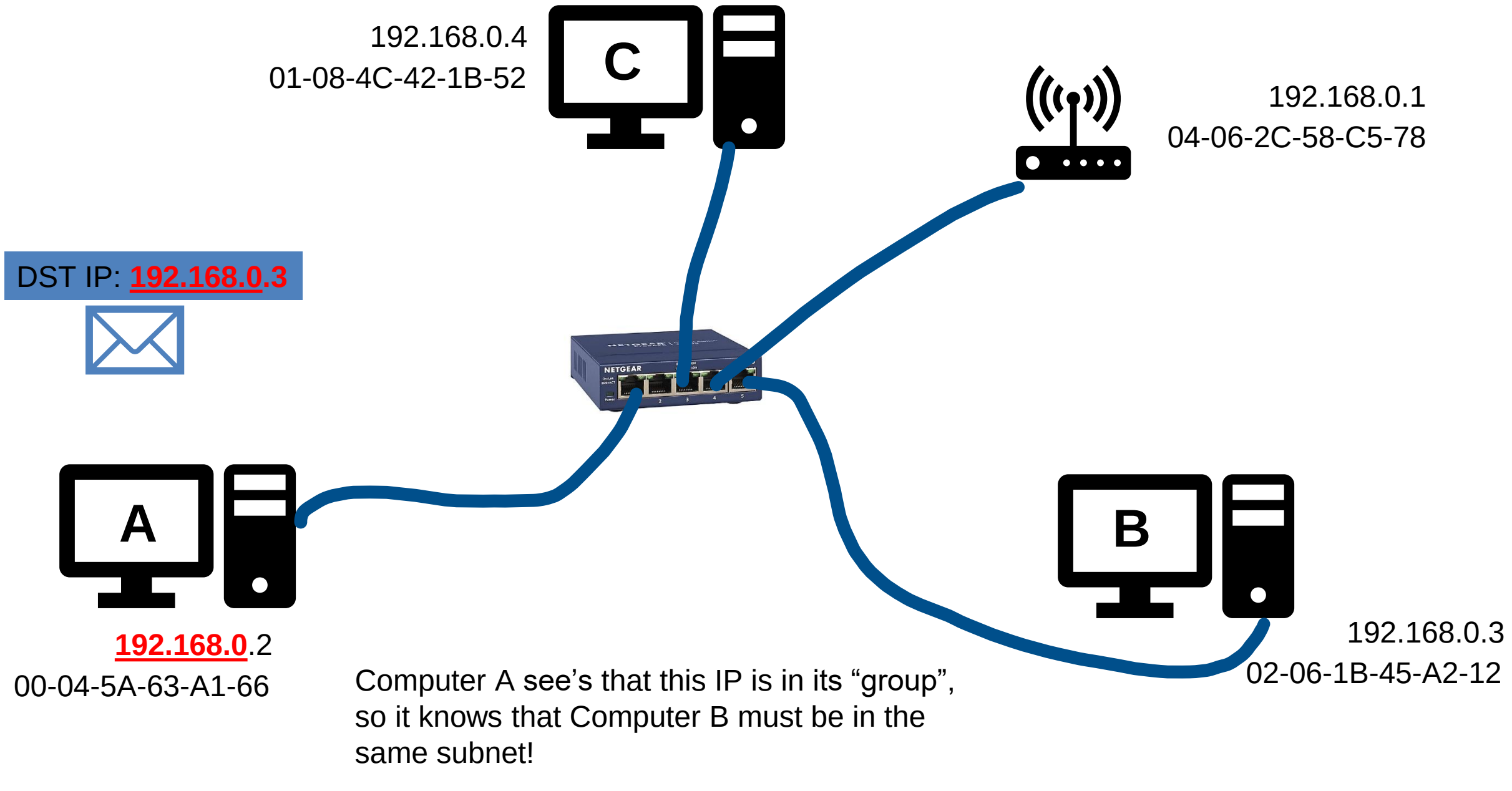
If the entry does not exist in the table, construct and send an **ARP** packet

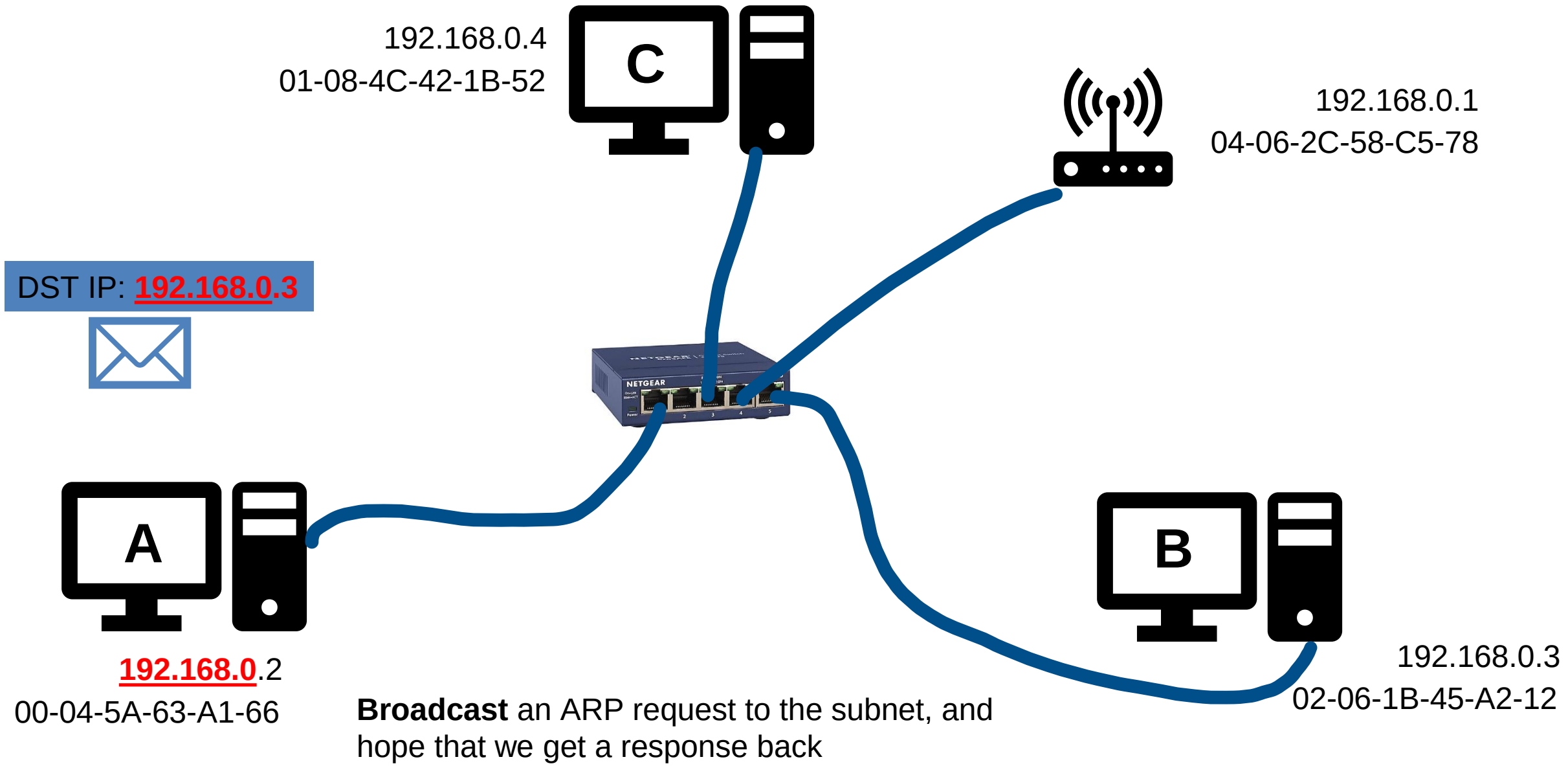
Broadcasts the ARP packet to all interfaces on the LAN (255.255.255.255)

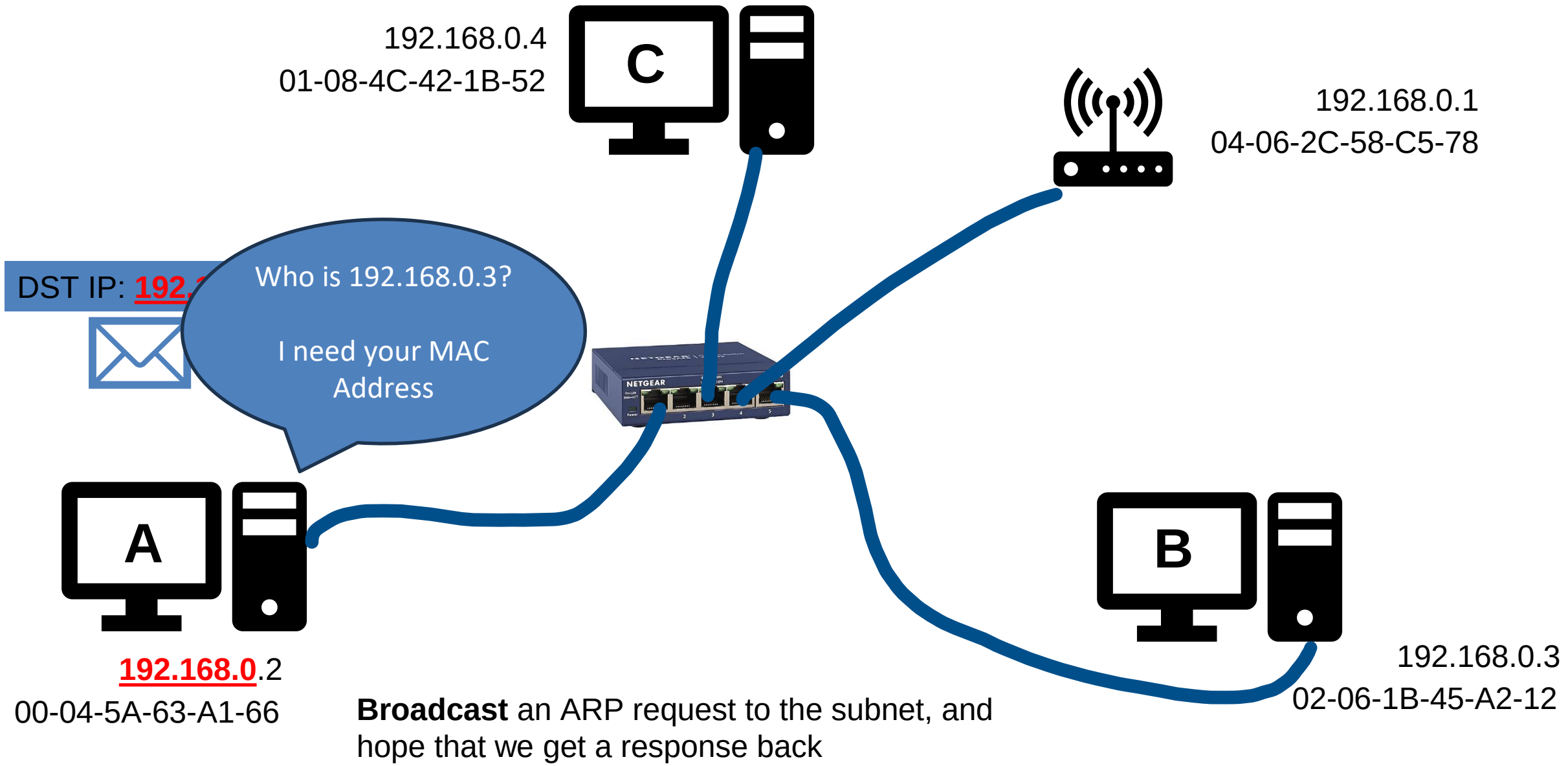
These tables are self-updated, and do not require manual entry*

ARP

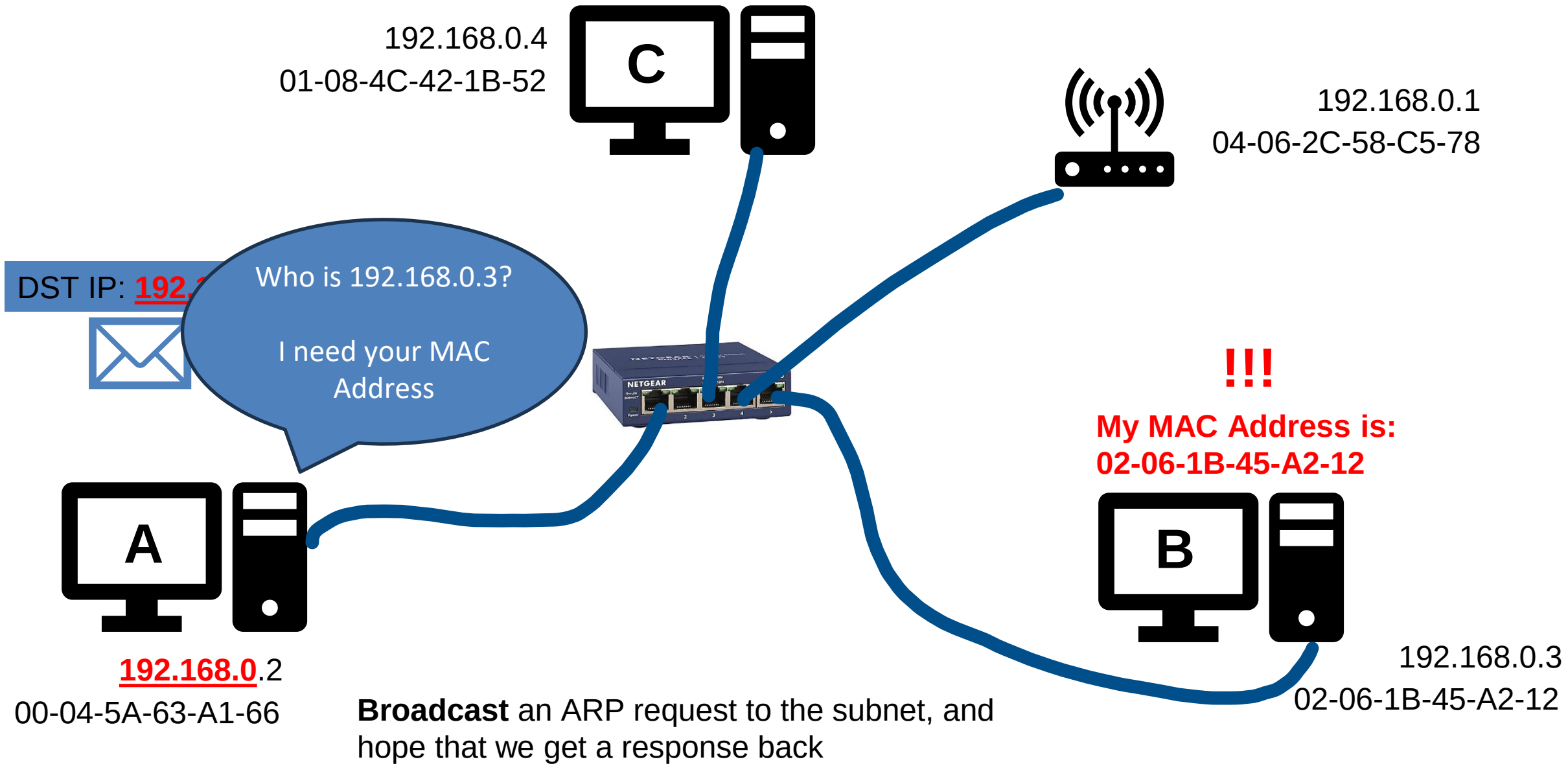
- A wants to send datagram to B
  - B's MAC address not in A's ARP table.
- A broadcasts ARP query packet, containing B's IP address
  - destination MAC address = FF-FF-FF-FF-FF-FF
  - all nodes on LAN receive ARP query
- B receives ARP packet, replies to A with its (B's) MAC address
  - frame sent to A's MAC address (unicast)
- A caches (saves) IP-to-MAC address pair in its ARP table until information becomes old (times out)
  - soft state: information that times out (goes away) unless refreshed
- ARP is "plug-and-play":
  - nodes create their ARP tables *without intervention from net administrator*

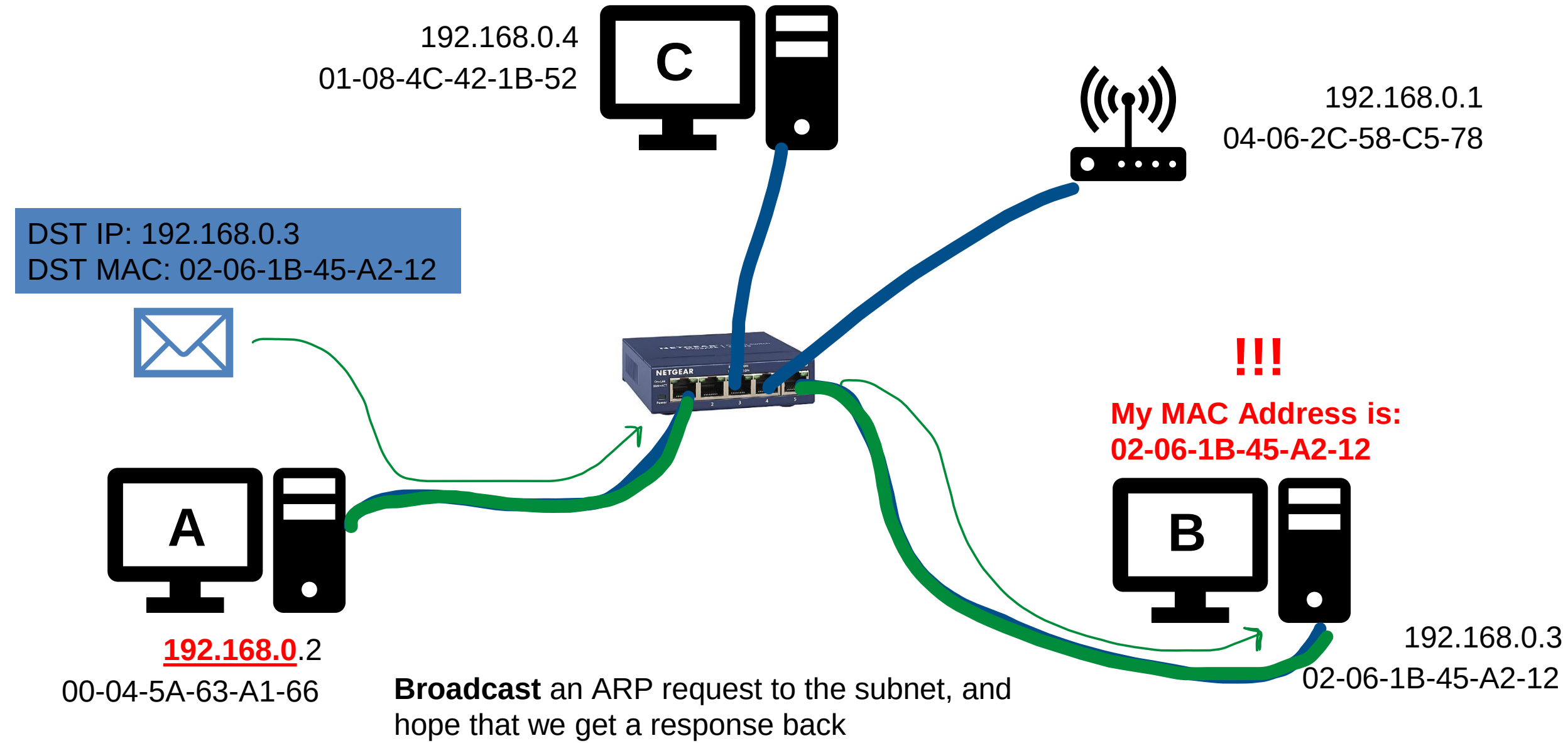

192.168.0.4
01-08-4C-42-1B-52
C
192.168.0.1
04-06-2C-58-C5-78
DST IP: 192.168.0.3
NETGEAR
A
B
192.168.0.2
00-04-5A-63-A1-66
192.168.0.3
02-06-1B-45-A2-12
Computer A see's that this IP is in its "group", so it knows that Computer B must be in the same subnet!


192.168.0.4
01-08-4C-42-1B-52
C
192.168.0.1
04-06-2C-58-C5-78
DST IP: 192.168.0.3
NETGEAR
A
B
192.168.0.2
00-04-5A-63-A1-66
192.168.0.3
02-06-1B-45-A2-12
Broadcast an ARP request to the subnet, and hope that we get a response back

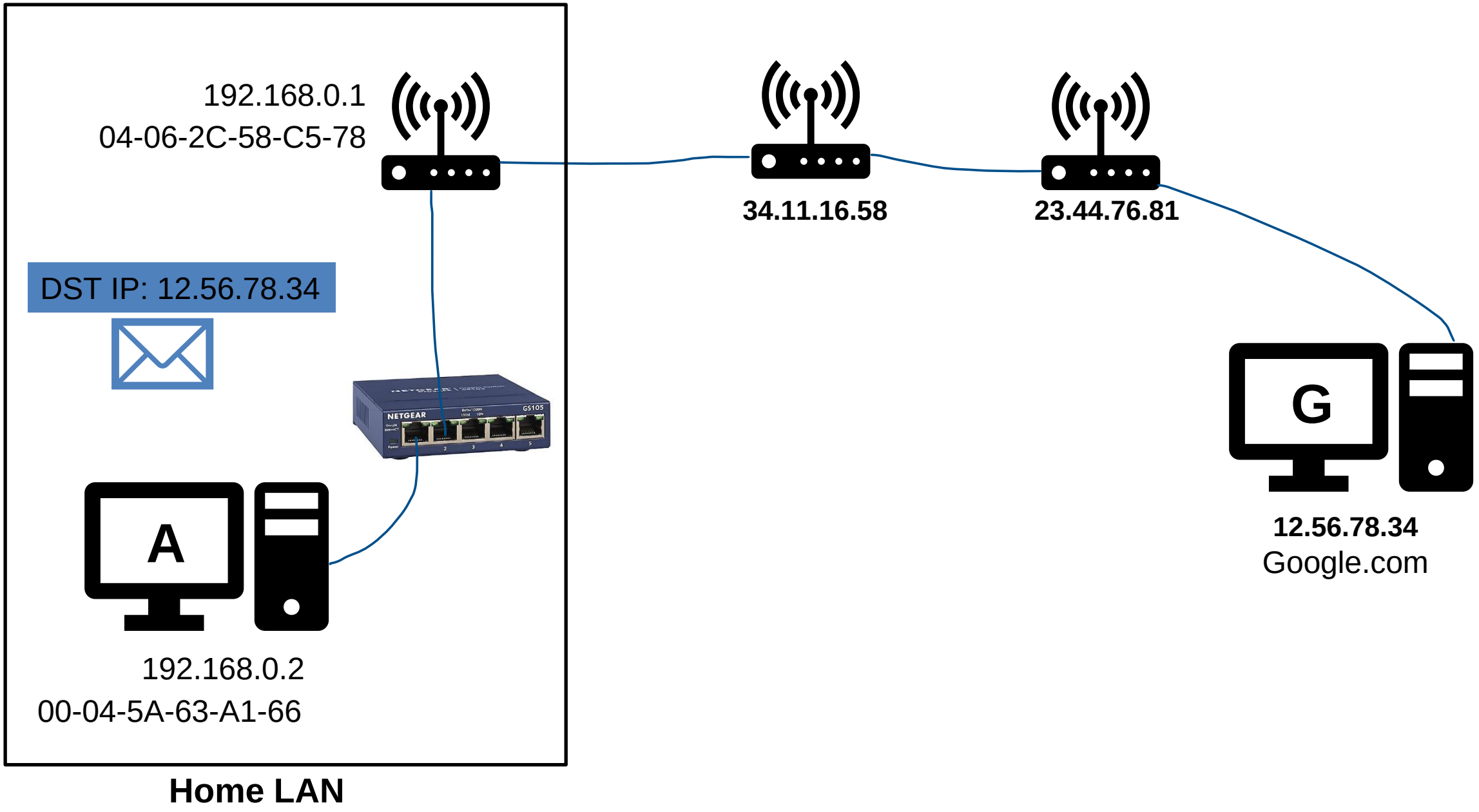


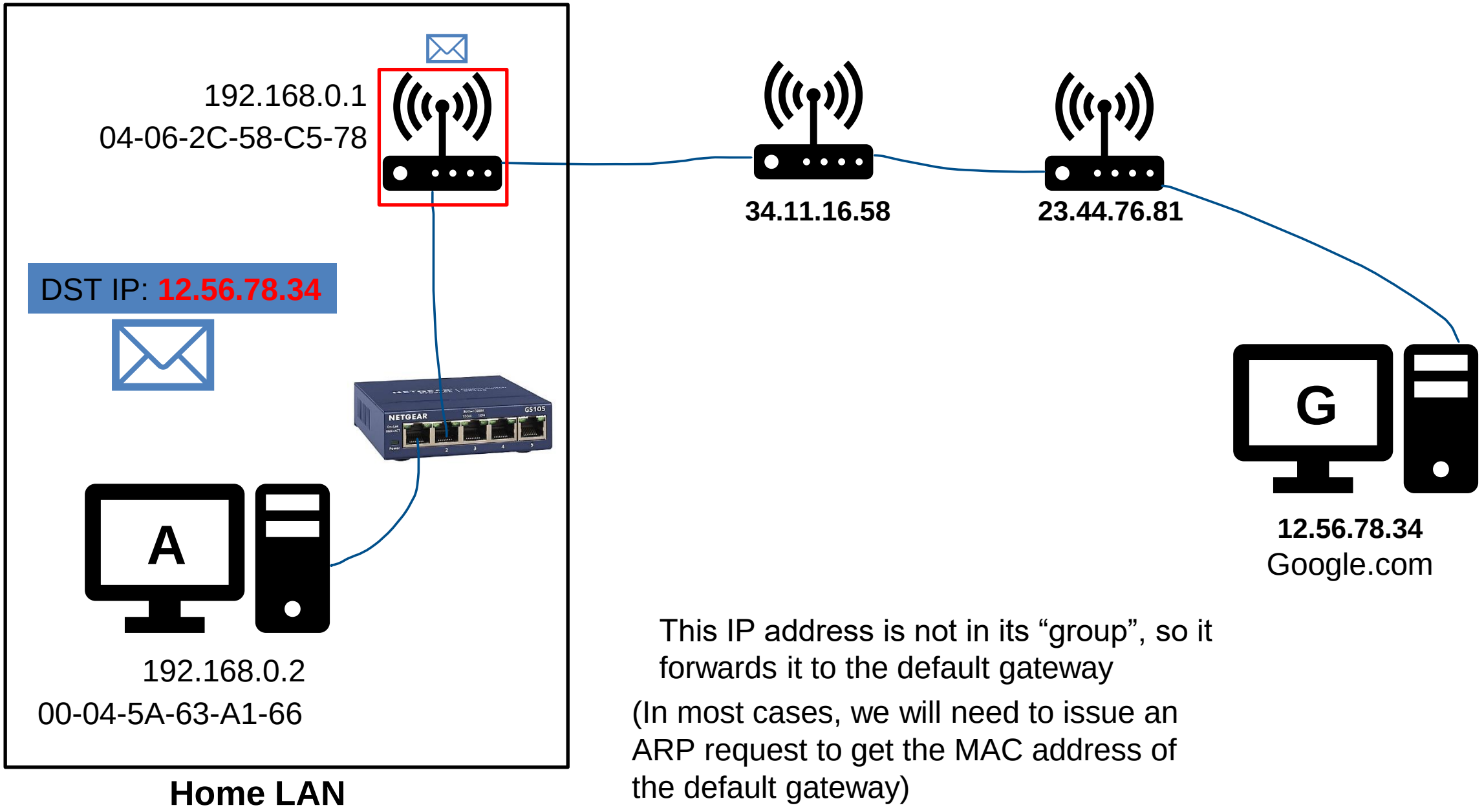
Broadcast an ARP request to the subnet, and hope that we get a response back


192.168.0.4
01-08-4C-42-1B-52
C
192.168.0.1
04-06-2C-58-C5-78
DST IP: 192.
Who is 192.168.0.3?
I need your MAC Address
!!!
My MAC Address is:
02-06-1B-45-A2-12
A
B
192.168.0.2
00-04-5A-63-A1-66
192.168.0.3
02-06-1B-45-A2-12
Broadcast an ARP request to the subnet, and hope that we get a response back



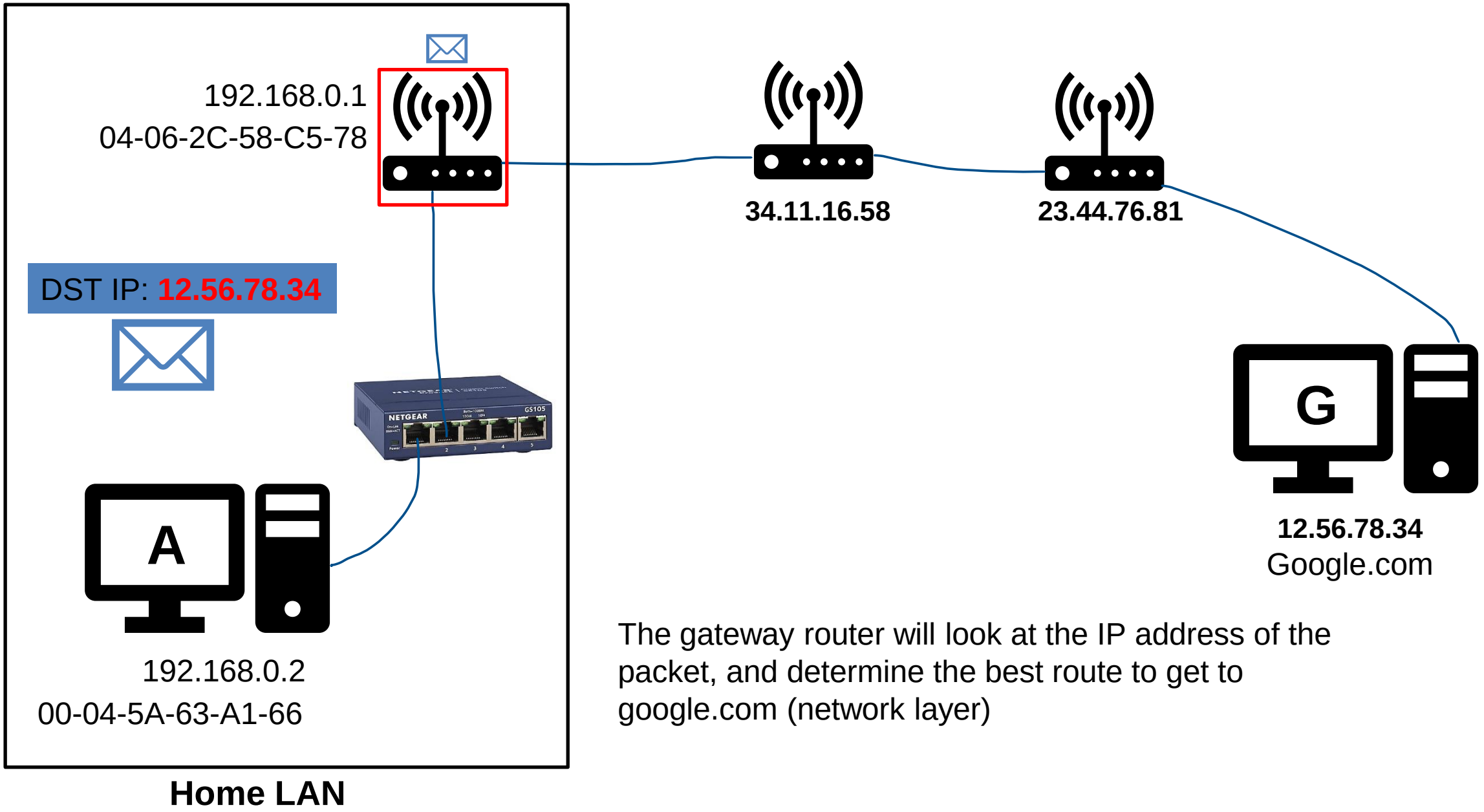
Broadcast an ARP request to the subnet, and hope that we get a response back


192.168.0.1
04-06-2C-58-C5-78
34.11.16.58
23.44.76.81
DST IP: 12.56.78.34
NETGEAR
GS105
A
G
192.168.0.2
00-04-5A-63-A1-66
12.56.78.34
Google.com
Home LAN

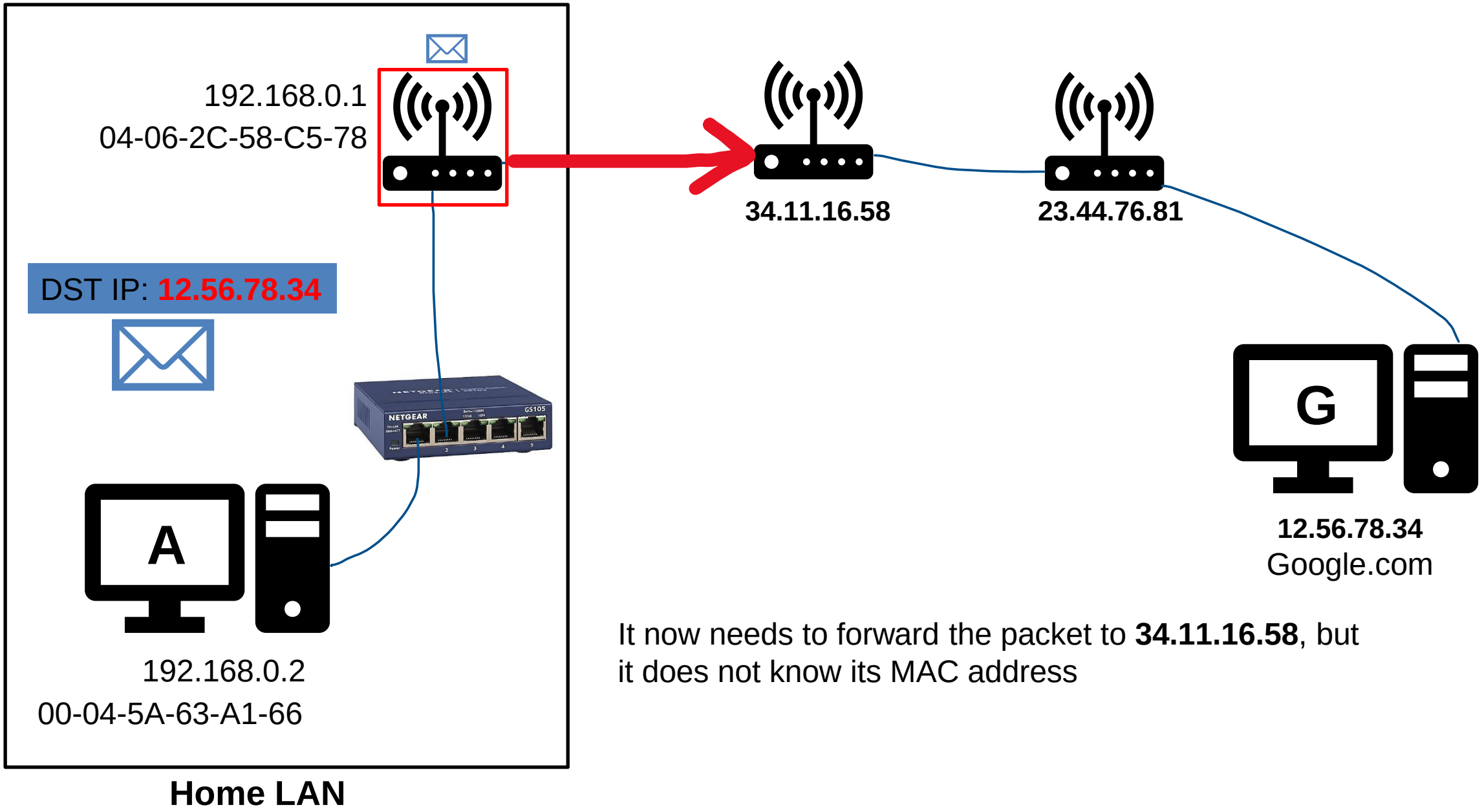


This IP address is not in its “group”, so it forwards it to the default gateway

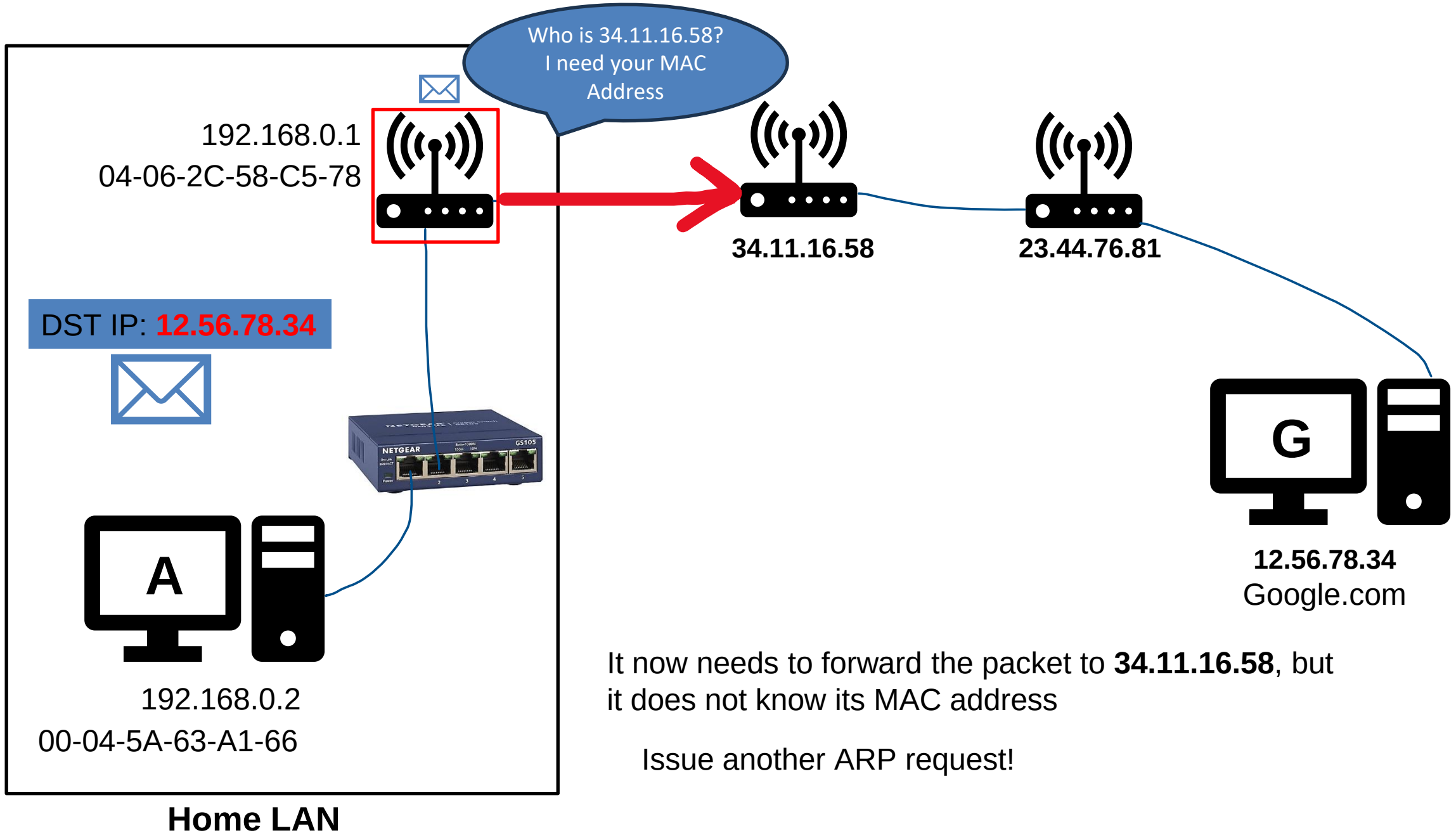
(In most cases, we will need to issue an ARP request to get the MAC address of the default gateway)



The gateway router will look at the IP address of the packet, and determine the best route to get to google.com (network layer)

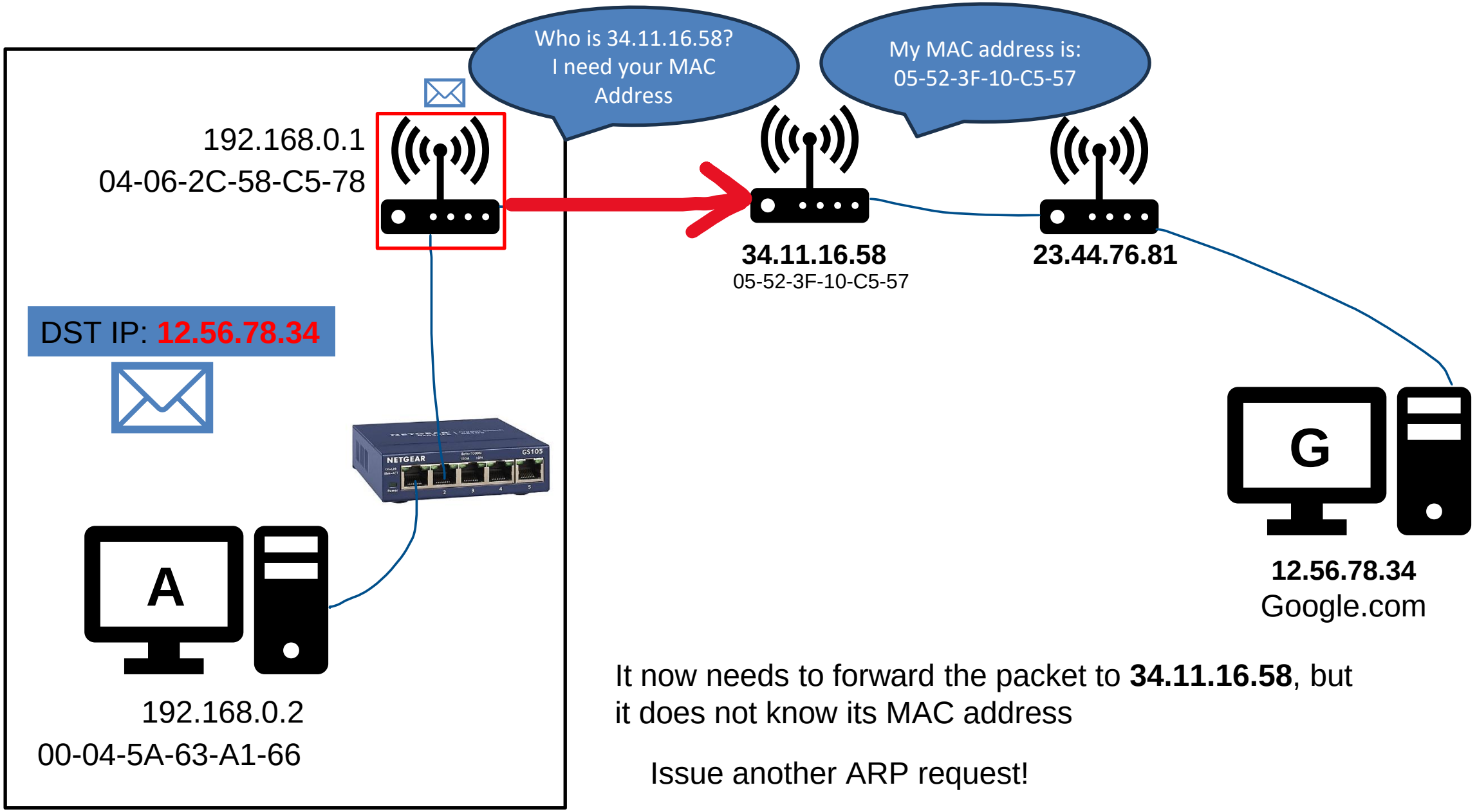


It now needs to forward the packet to **34.11.16.58**, but it does not know its MAC address



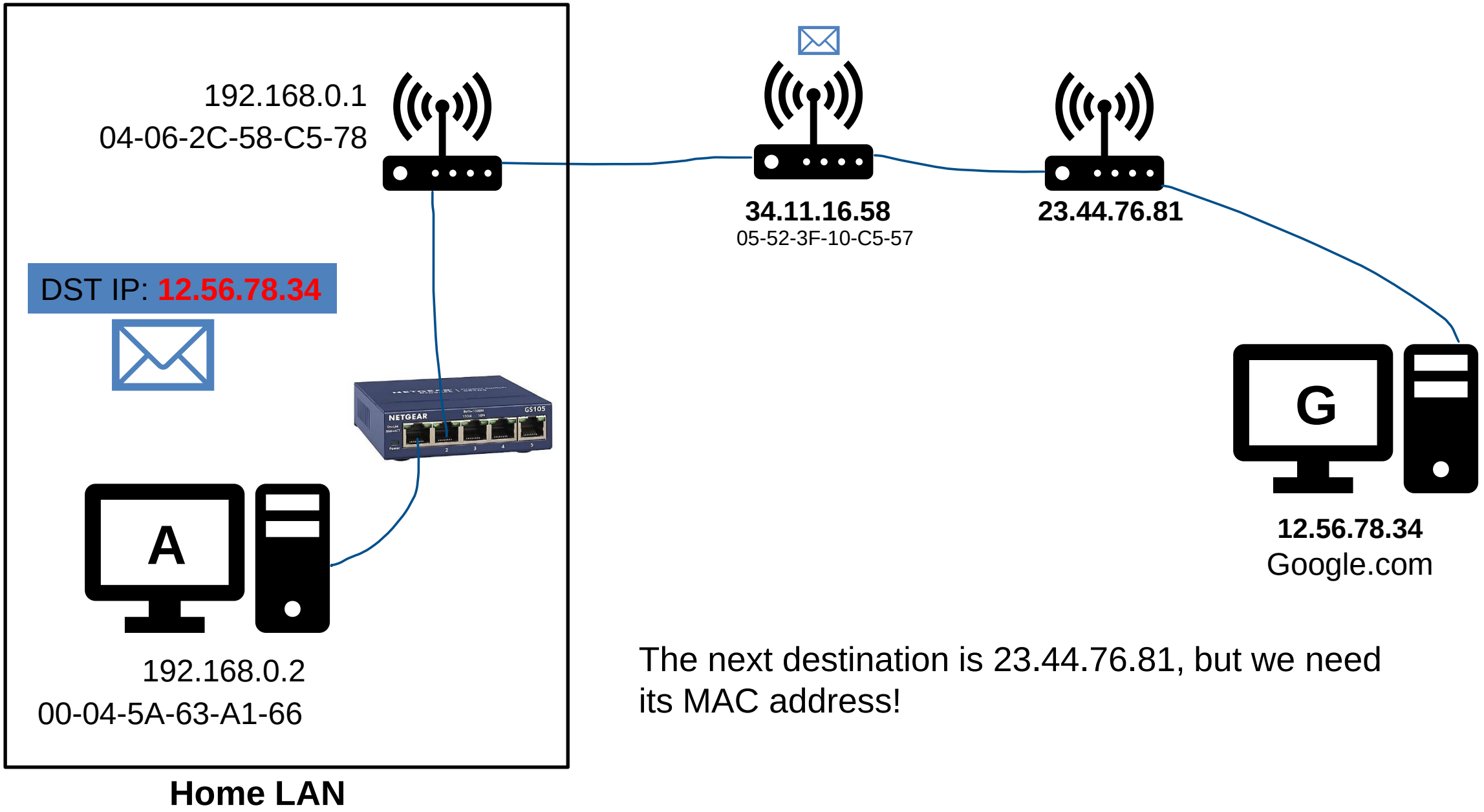
It now needs to forward the packet to **34.11.16.58**, but it does not know its MAC address

Issue another ARP request!

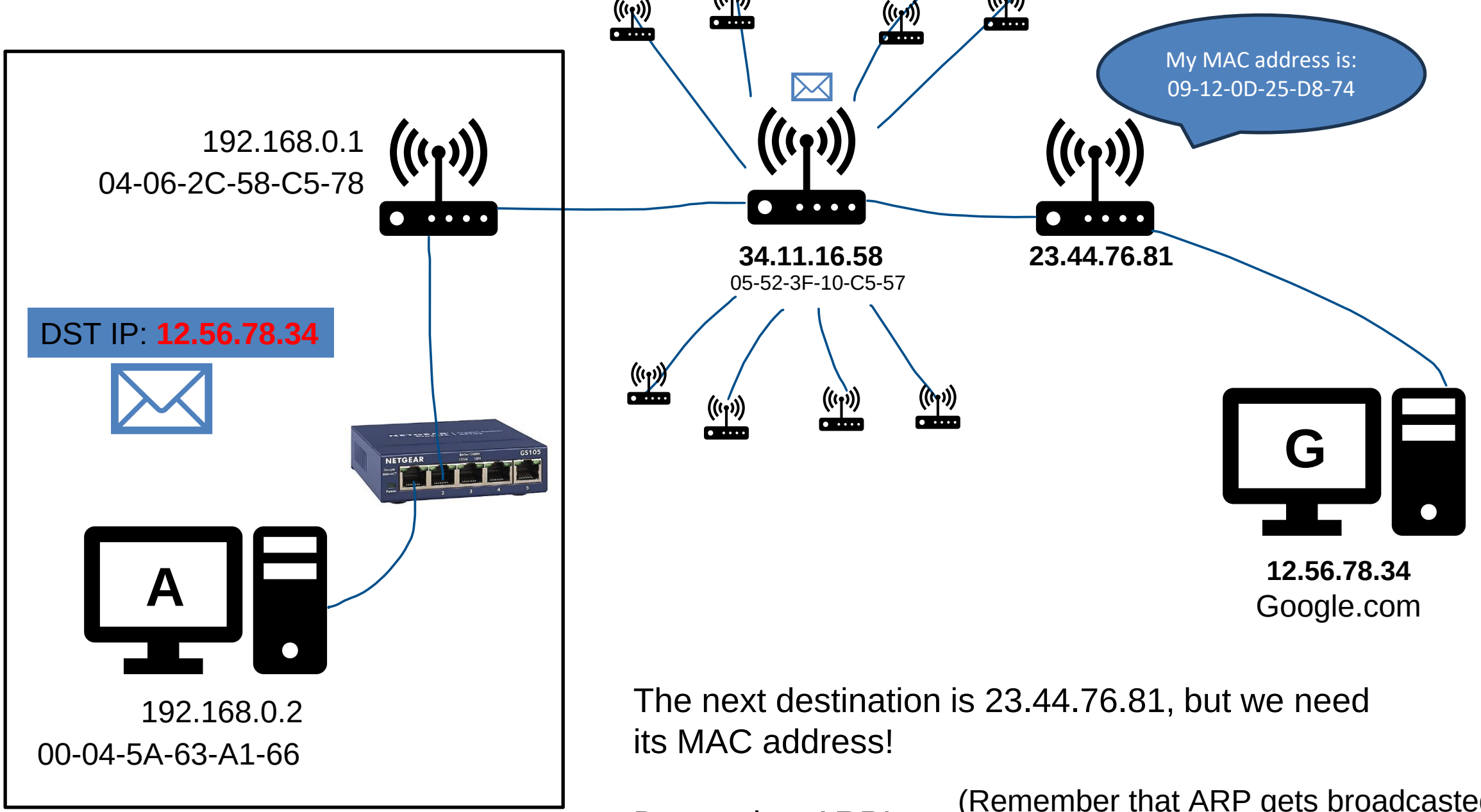


It now needs to forward the packet to **34.11.16.58**, but it does not know its MAC address

Issue another ARP request!



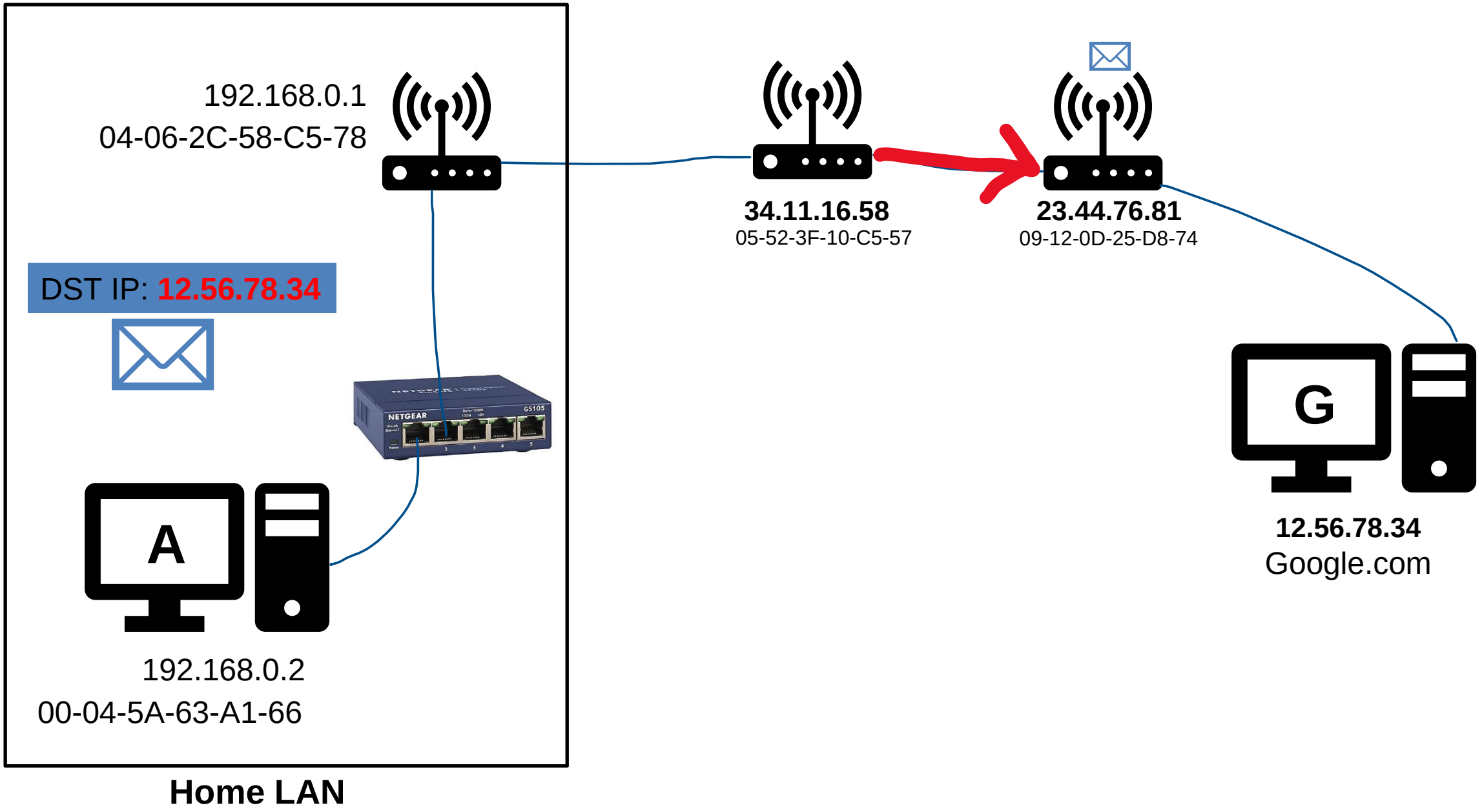
The next destination is 23.44.76.81, but we need its MAC address!

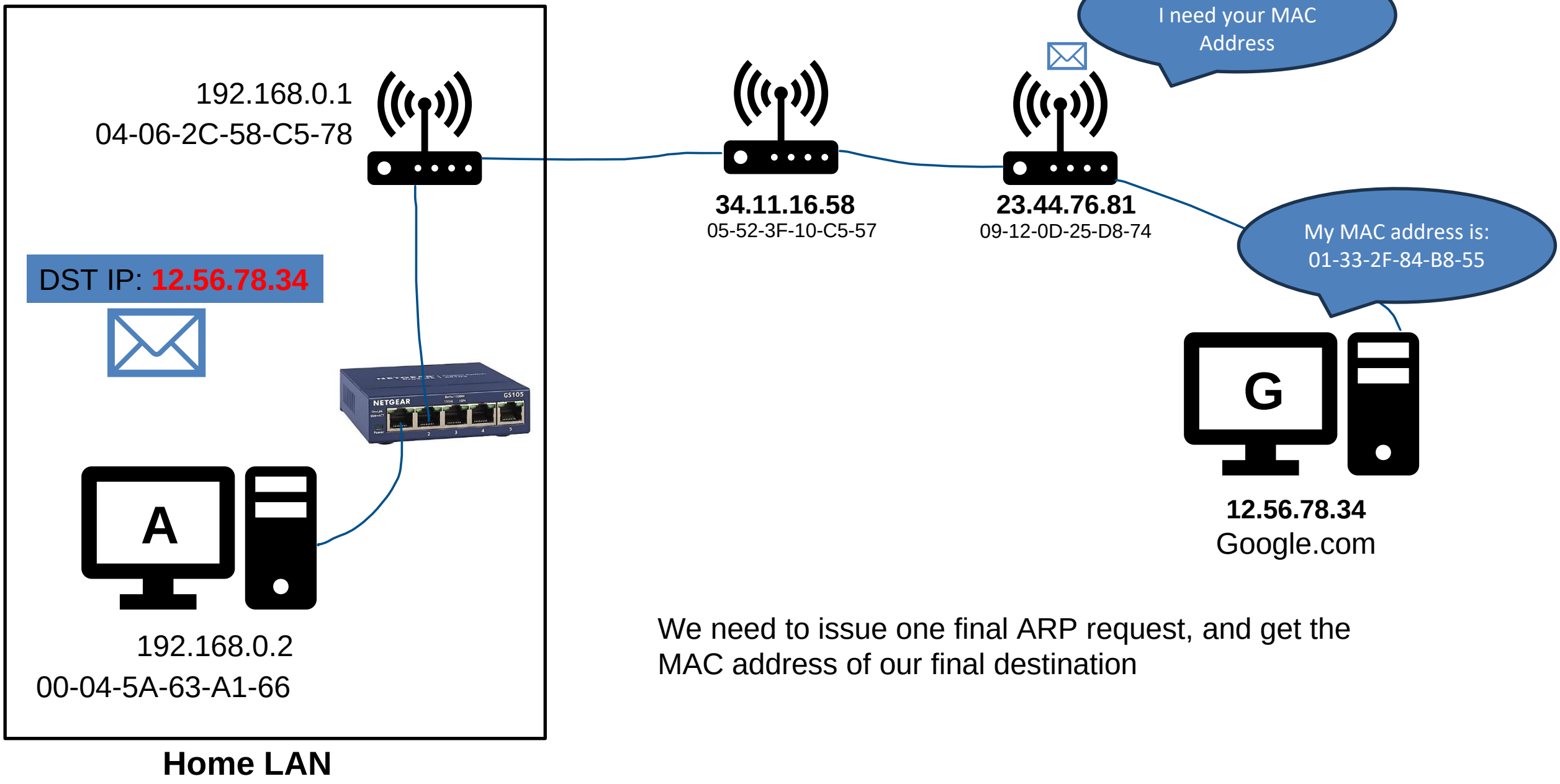


The next destination is 23.44.76.81, but we need its MAC address!

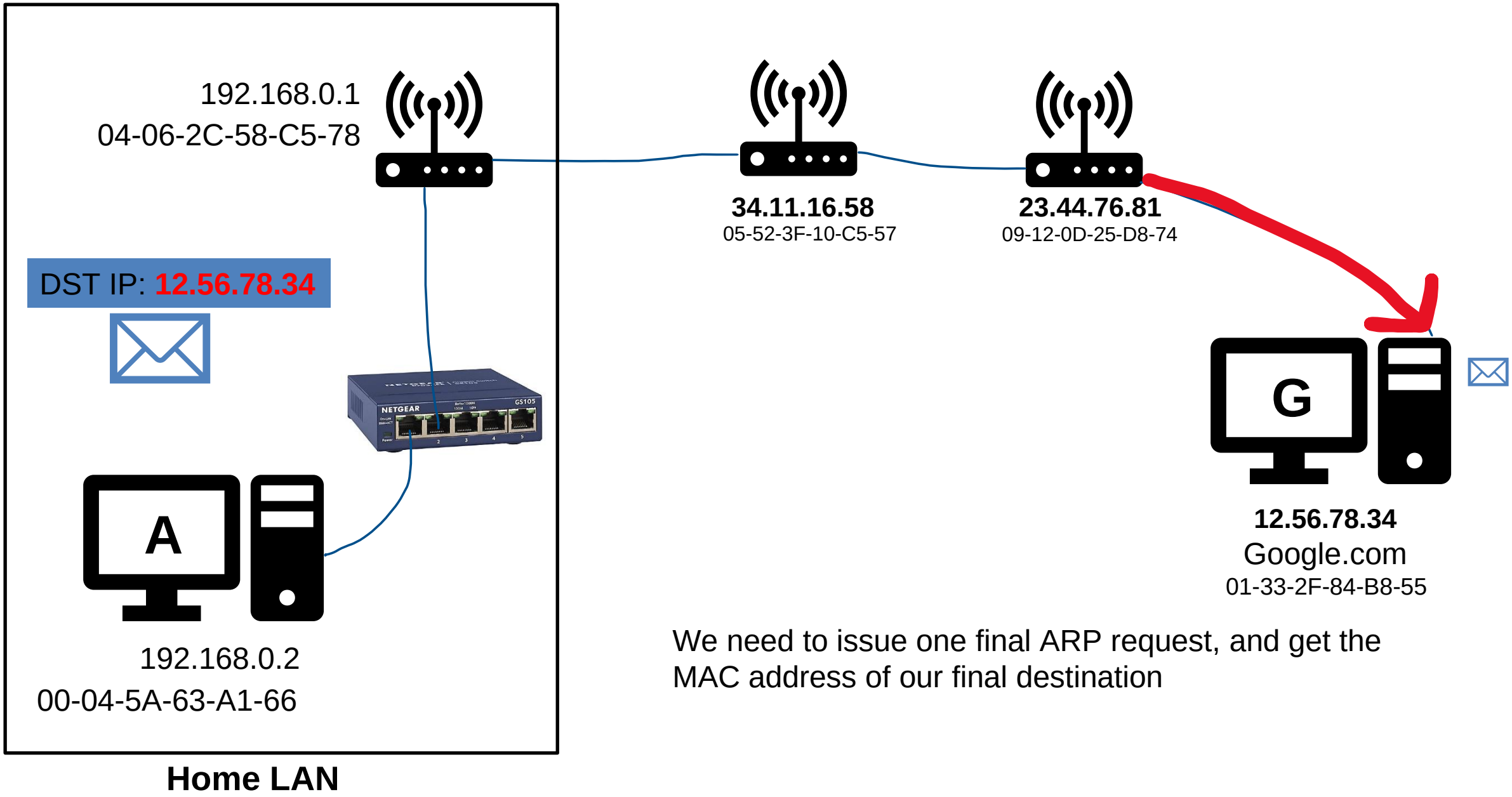
Do another ARP!

(Remember that ARP gets broadcasted to all direct neighbors)


192.168.0.1
04-06-2C-58-C5-78
34.11.16.58
05-52-3F-10-C5-57
23.44.76.81
09-12-0D-25-D8-74
DST IP: 12.56.78.34
NETGEAR
GS105
A
G
12.56.78.34
Google.com
192.168.0.2
00-04-5A-63-A1-66
Home LAN

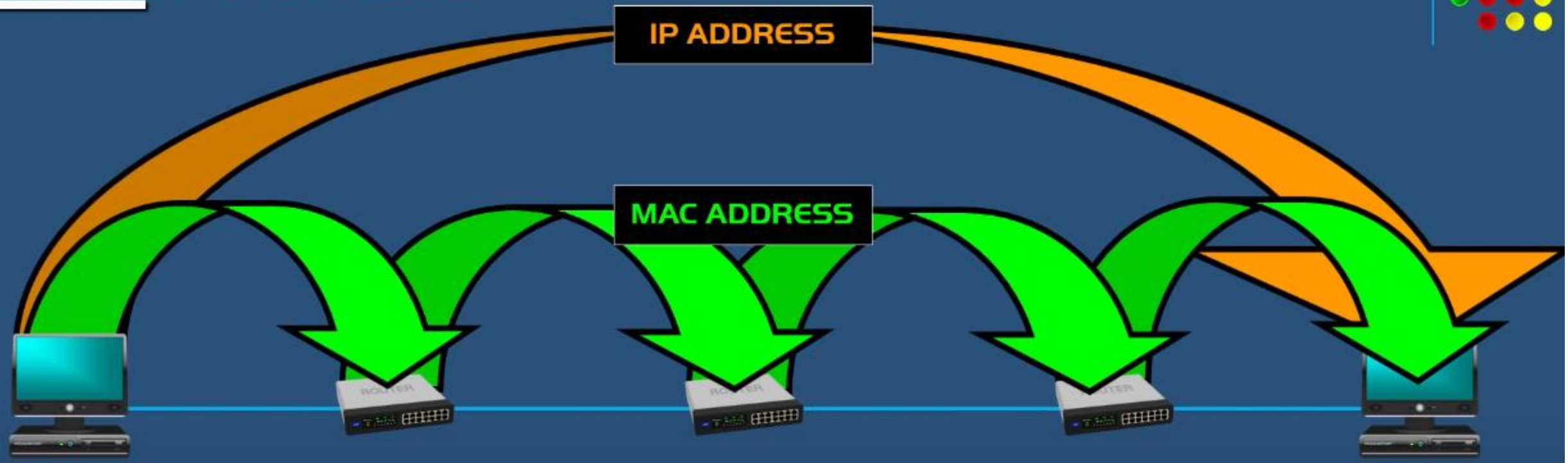


We need to issue one final ARP request, and get the MAC address of our final destination



We need to issue one final ARP request, and get the MAC address of our final destination

MAC ADDRESS



The IP address is used to locate and get to the final destination.

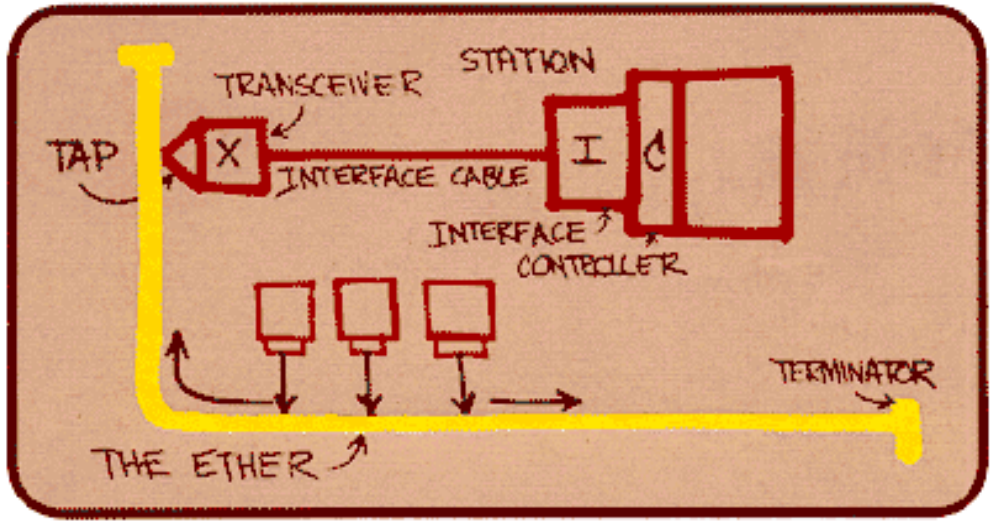
The MAC address is used at each step on its way to the final destination.

Finding your MAC Address

Ipconfig/all

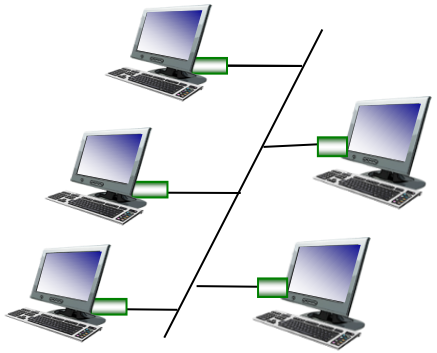
Ethernet

- "dominant" wired LAN technology:
- single chip, multiple speeds (e.g., Broadcom BCM5761)
- first widely used LAN technology
- simpler, cheap
- kept up with speed race: 10 Mbps – 10 Gbps



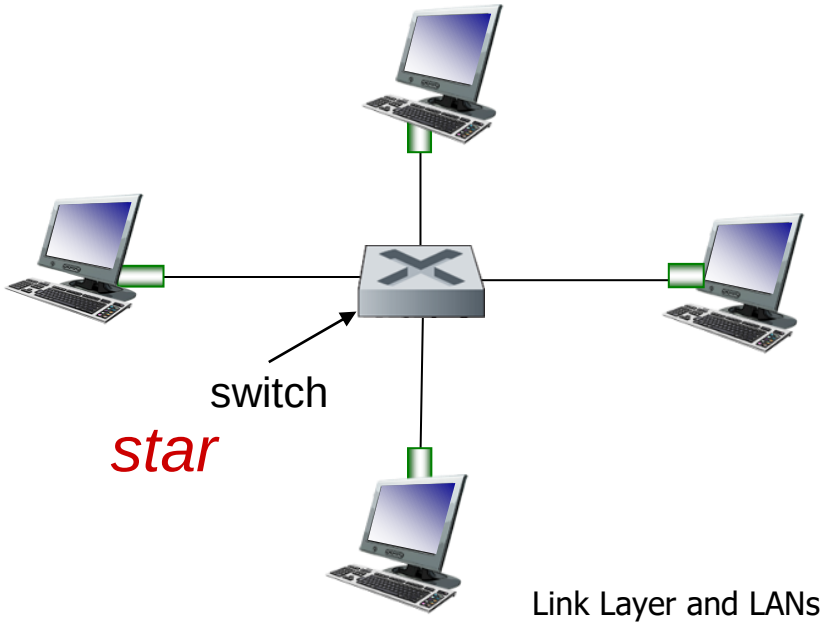
Metcalfe's Ethernet sketch

Ethernet Topology



bus: coaxial cable

(outdated)



star

Ethernet frame structure

sending adapter encapsulates IP datagram (or other network layer protocol packet) in Ethernet frame

preamble:

7 bytes with pattern 10101010 followed by one byte with pattern 10101011

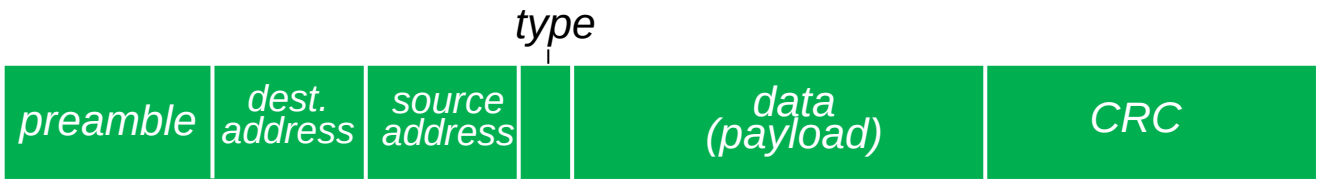
used to synchronize receiver, sender clock rates

Ethernet frame structure (more)

addresses: 6 byte source, destination MAC addresses
if adapter receives frame with matching destination address, or with broadcast address (e.g. ARP packet), it passes data in frame to network layer protocol
otherwise, adapter discards frame

type: indicates higher layer protocol (mostly IP but others possible, e.g., Novell IPX, AppleTalk)

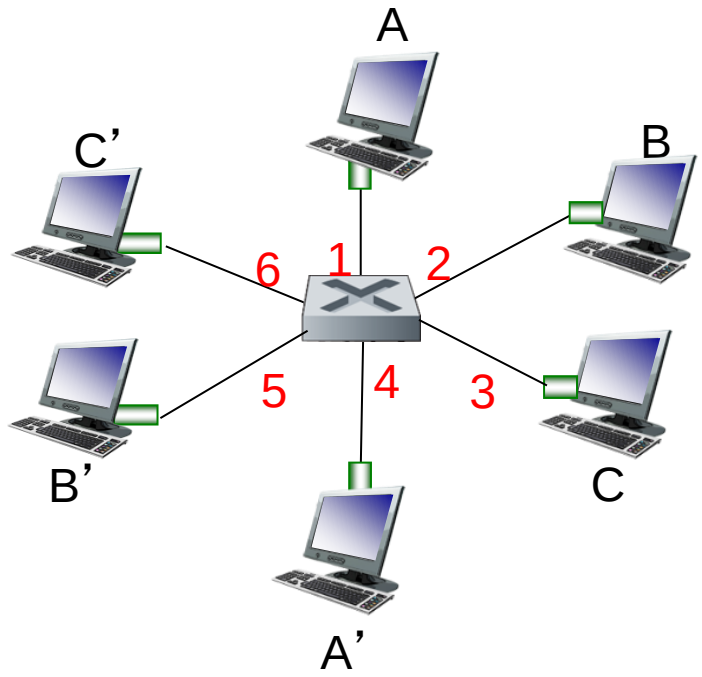
CRC: cyclic redundancy check at receiver
error detected: frame is dropped

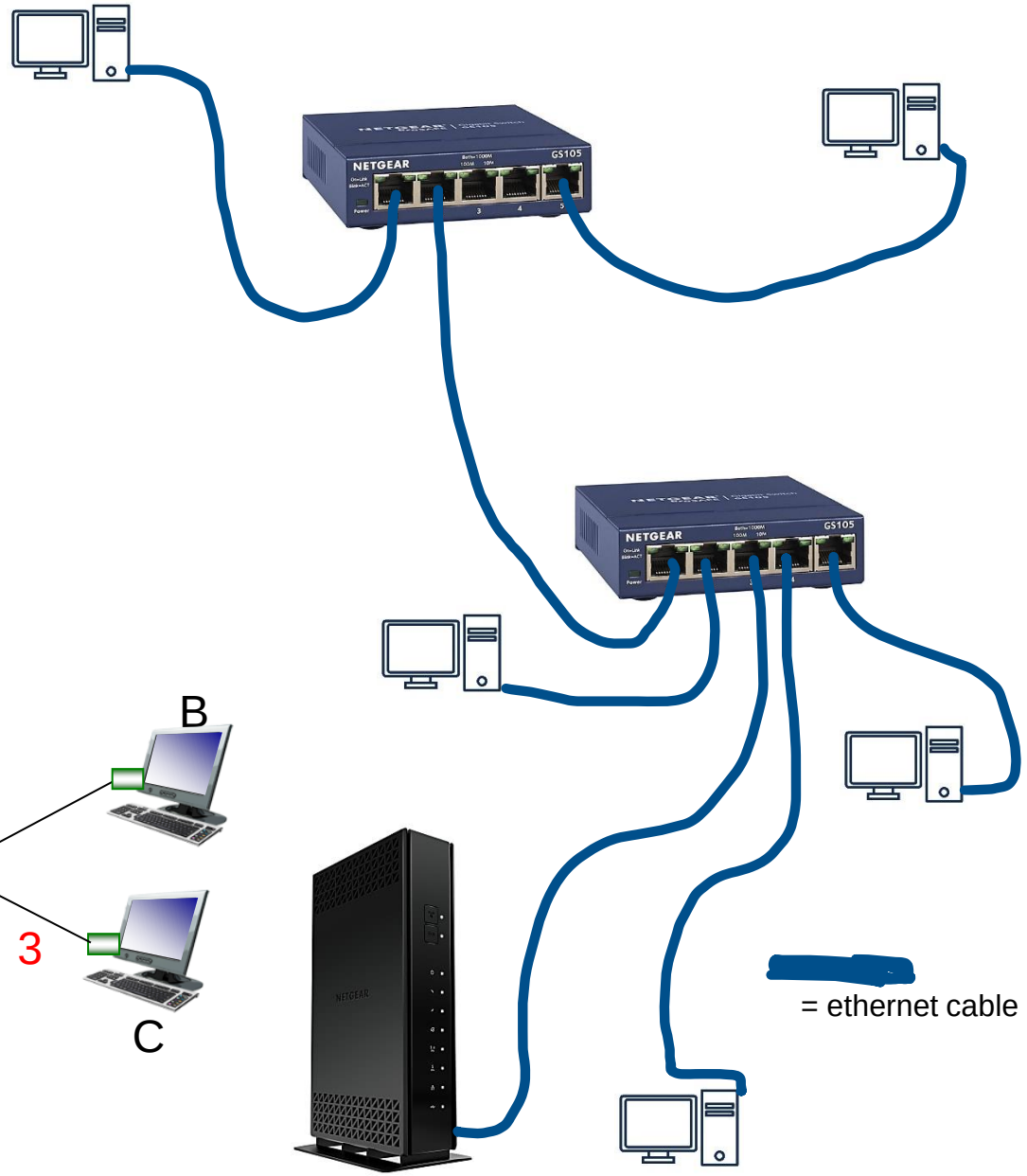


Ethernet switch

- Switches will store and forward ethernet frames
- Hosts have *dedicated*, direct connection to switch
- Ethernet protocol used on each incoming link, **but no collisions between links**
- Switching: A-A’ and B-B’ can transmit simultaneously, without collisions

- Transparent: Hosts are not aware they are connected to a switch
- Plug and play; self-learning





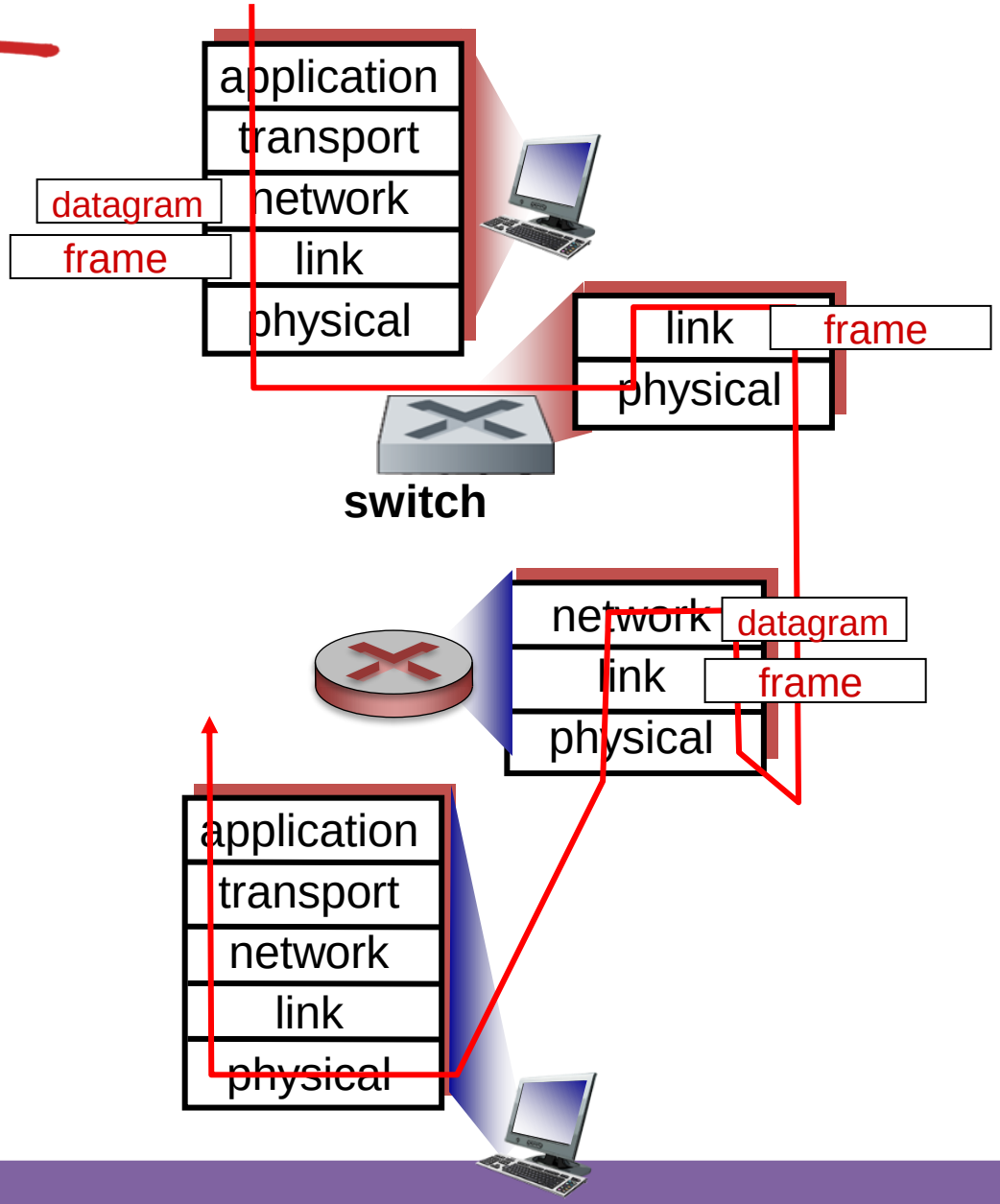
Switches vs. routers

both are store-and-forward:

- *routers:* network-layer devices (examine network-layer headers)
- *switches*: link-layer devices (examine link-layer headers)

both have forwarding tables:

- *routers:* compute tables using routing algorithms, IP addresses
- *switches:* learn forwarding table using flooding, learning, MAC addresses



https://www.youtube.com/watch?v=1z0ULvg_pW8