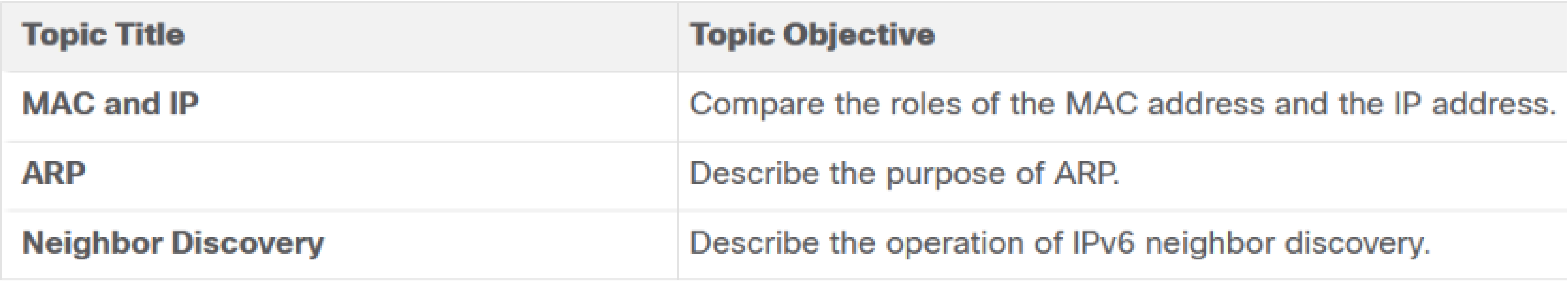
NETACAD
UNIT 9
ADDRESS RESOLUTION

Created by Frank Schneemann, MS EdTech
Bonita Vista H.S.
Southwestern College, Chula Vista CA.
www.edtechnology.com

This presentation is in no way intended to substitute for the regular Netacad lessons.
It is only meant to explain parts of the Netacad curriculum that students may need help understanding
The regular Netacad curriculum contains many teaching tools such as Packet Tracers, Quizzes, Video's, reviews, chapter summaries and other concepts not included in these tutorials.
Please avail yourself of the regular Netacad lessons

What will I learn to do in this module?

Module Objective: Explain how ARP and ND enable communication on a network.



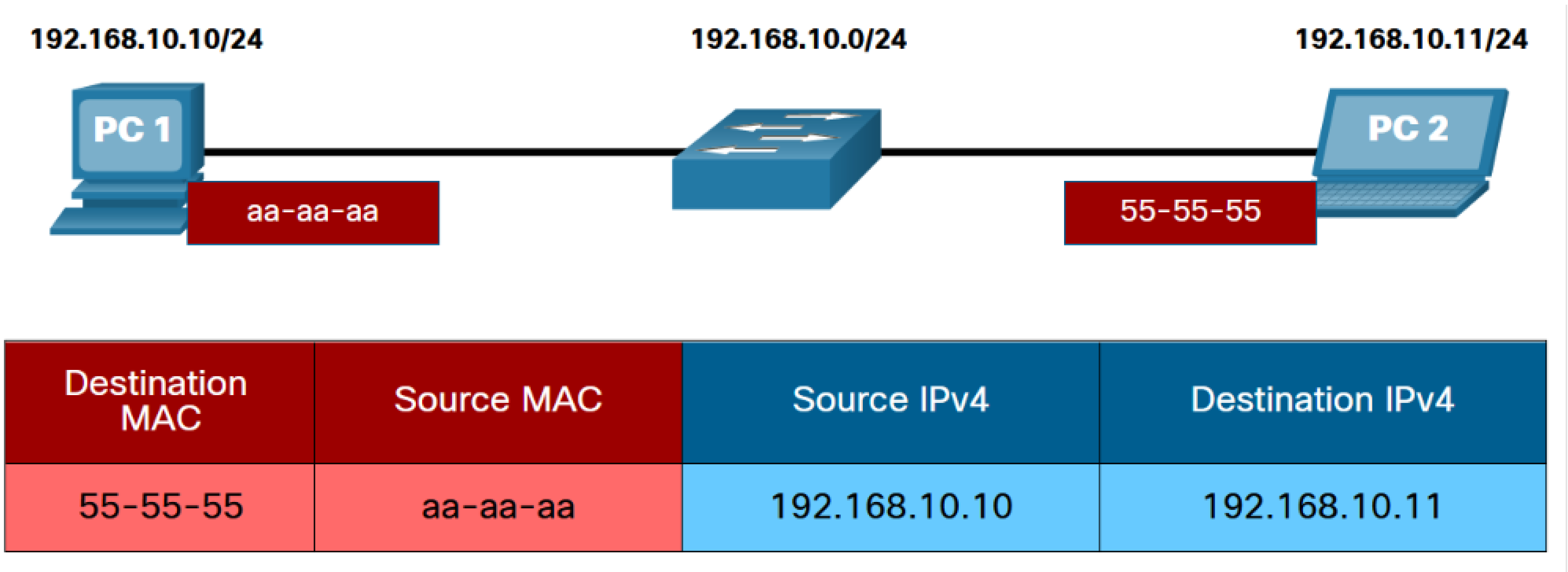
Topic Title	Topic Objective
MAC and IP	Compare the roles of the MAC address and the IP address.
ARP	Describe the purpose of ARP.
Neighbor Discovery	Describe the operation of IPv6 neighbor discovery.

MAC and IP

Destination on Same Network

There are two primary addresses assigned to a device on an Ethernet LAN:

Physical address (the MAC address) – Used for NIC to NIC communications on the same Ethernet network.
Logical address (the IP address) – Used to send the packet from the source device to the destination device. The destination IP address may be on the same IP network as the source or it may be on a remote network.



Destination MAC	Source MAC	Source IPv4	Destination IPv4
55-55-55	aa-aa-aa	192.168.10.10	192.168.10.11

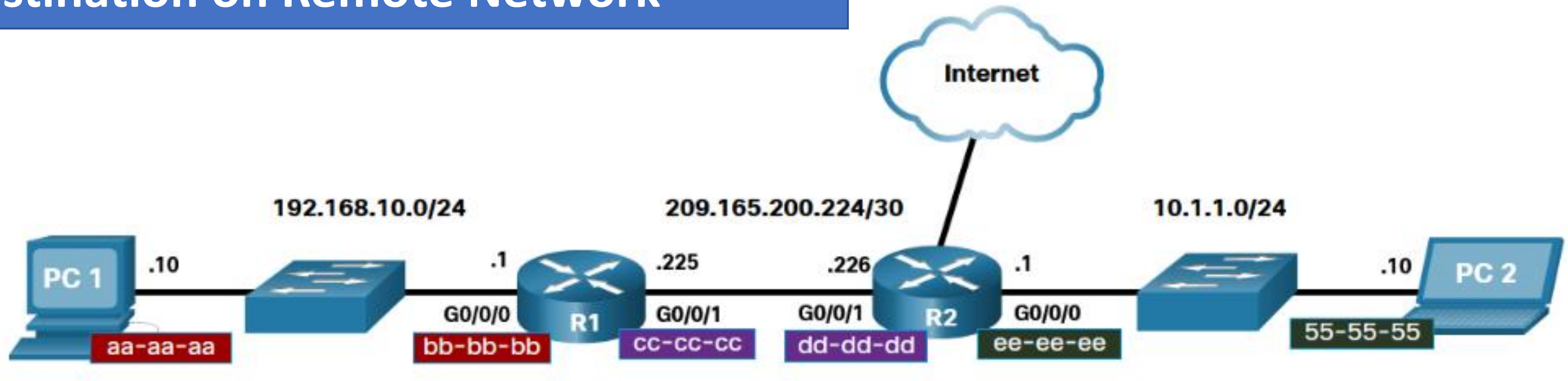
The Layer 2 Ethernet frame contains the following:

Destination MAC address – This is the simplified MAC address of PC2, 55-55-55.
Source MAC address – This is the simplified MAC address of the Ethernet NIC on PC1, aa-aa-aa.

The Layer 3 IP packet contains the following:

Source IPv4 address – This is the IPv4 address of PC1, 192.168.10.10.
Destination IPv4 address – This is the IPv4 address of PC2, 192.168.10.11.

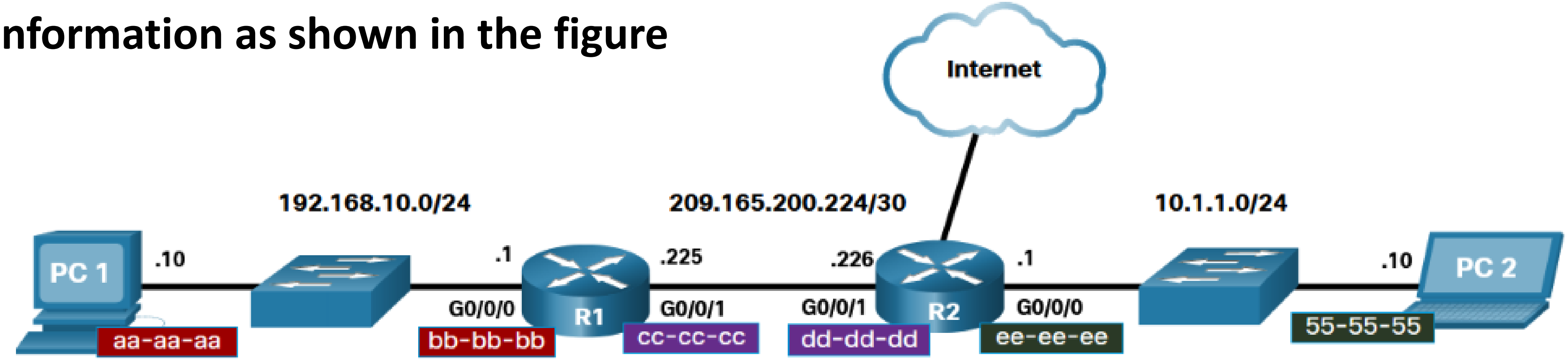
Destination on Remote Network



Destination MAC	Source MAC	Source IPv4	Destination IPv4
bb-bb-bb	aa-aa-aa	192.168.10.10	10.1.1.10

In this example, PC1 wants to send a packet to PC2. PC2 is located on remote network. Because the destination IPv4 address is not on the same local network as PC1, the destination MAC address is that of the local default gateway on the router.

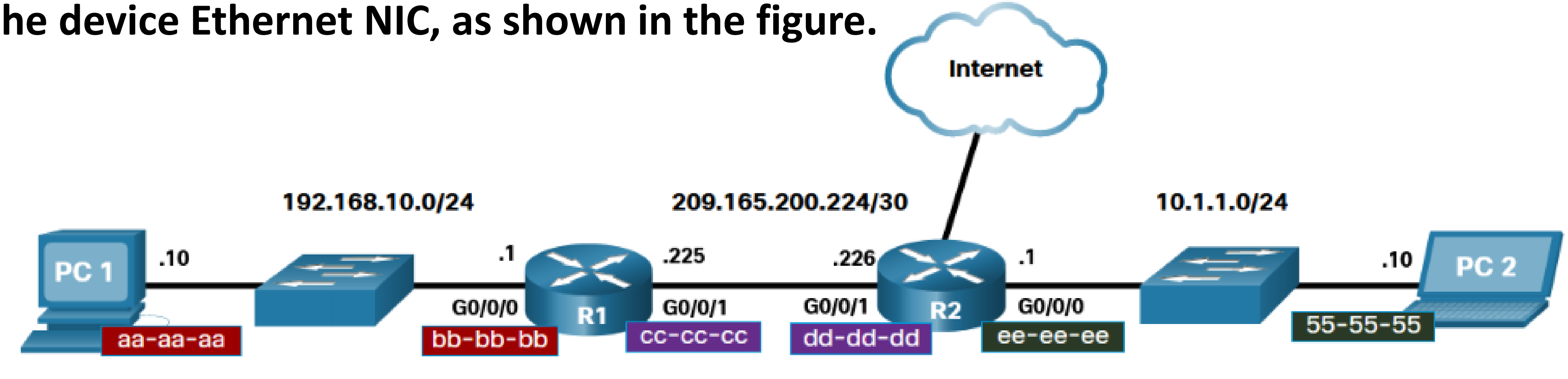
In our example, R1 would now encapsulate the packet with new Layer 2 address information as shown in the figure



Destination MAC	Source MAC	Source IPv4	Destination IPv4
dd-dd-dd	cc-cc-cc	192.168.10.10	10.1.1.10

The new destination MAC address would be that of the R2 G0/0/1 interface and the new source MAC address would be that of the R1 G0/0/1 interface.

Along each link in a path, an IP packet is encapsulated in a frame. The frame is specific to the data link technology that is associated with that link, such as Ethernet. If the next-hop device is the final destination, the destination MAC address will be that of the device Ethernet NIC, as shown in the figure.

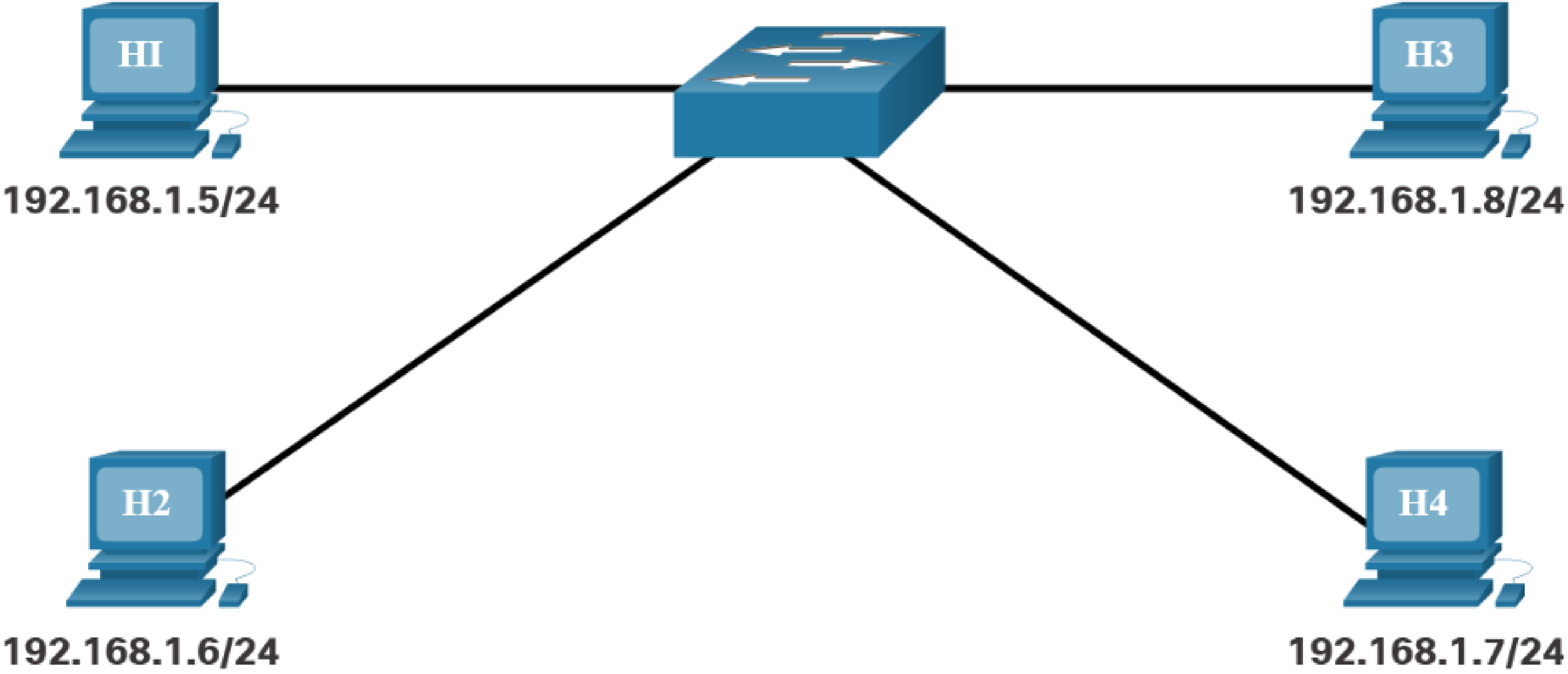


Destination MAC	Source MAC	Source IPv4	Destination IPv4
55-55-55	ee-ee-ee	192.168.10.10	10.1.1.10

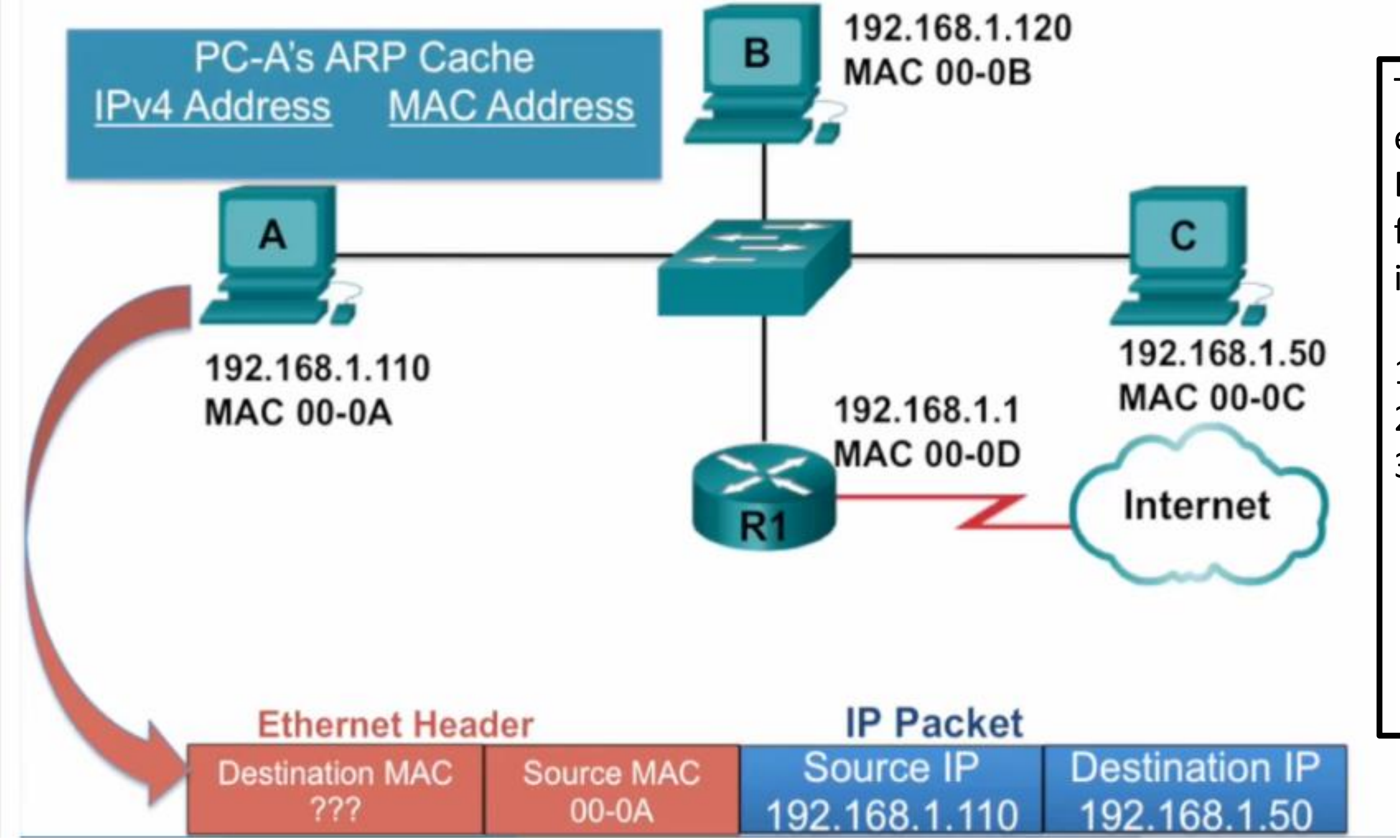
How are the IP addresses of the IP packets in a data flow associated with the MAC addresses on each link along the path to the destination? For IPv4 packets, this is done through a process called Address Resolution Protocol (ARP). For IPv6 packets, the process is ICMPv6 Neighbor Discovery (ND).

ARP Overview

I need to send information to 192.168.1.7, but I only have the IP address. I don't know the MAC address of the device that has that IP.



ARP REQUEST ON SAME NETWORK

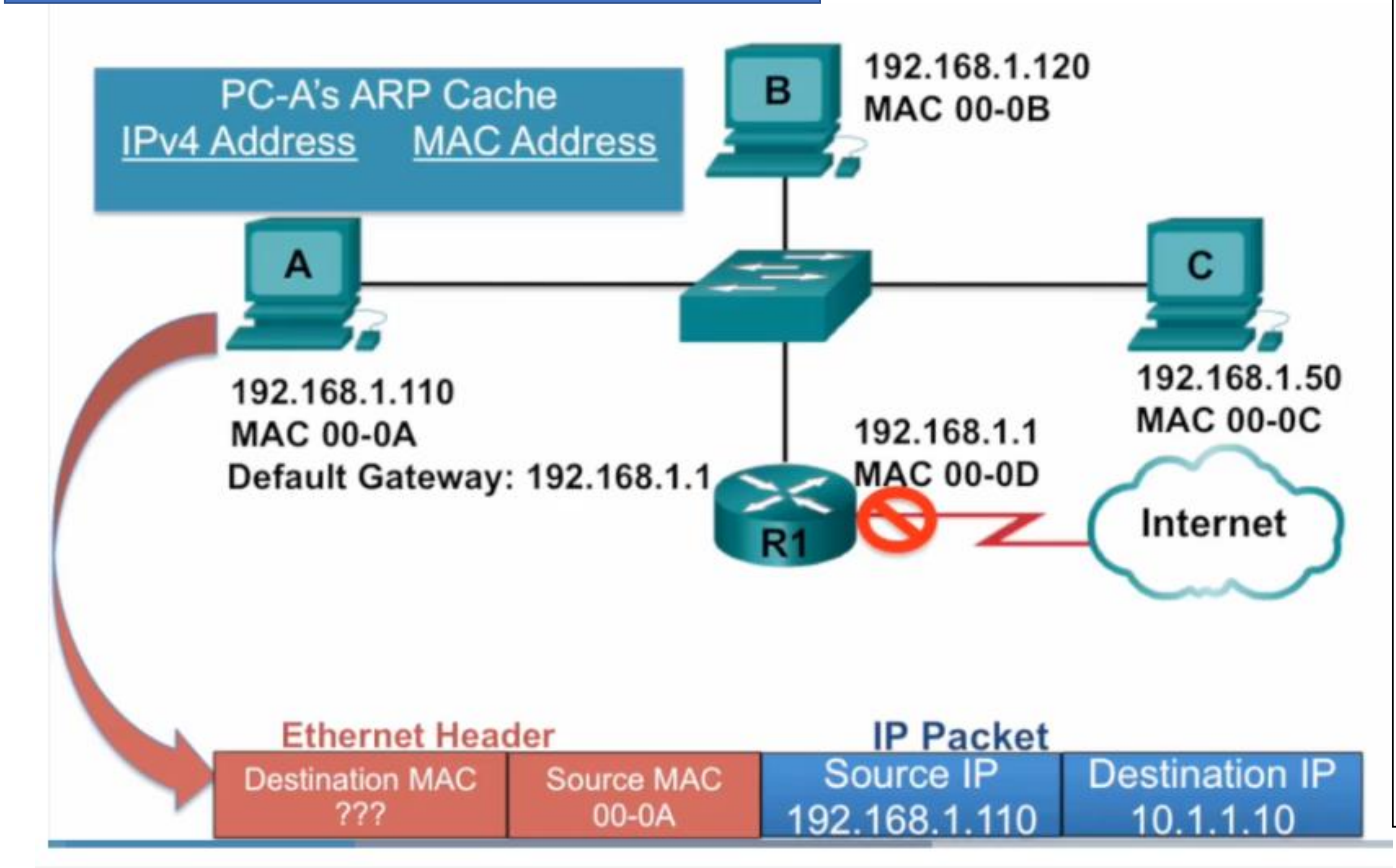


FRAME

The ARP request is encapsulated in an Ethernet frame using the following header information:

1. Destination MAC
2. Source MAC address.
3. Type - informs the receiving NIC that the data portion of the frame needs to be passed to the ARP process.

ARP REQUEST ON A REMOTE NETWORK



10.1.1.10 IS ON A REMOTE NETWORK

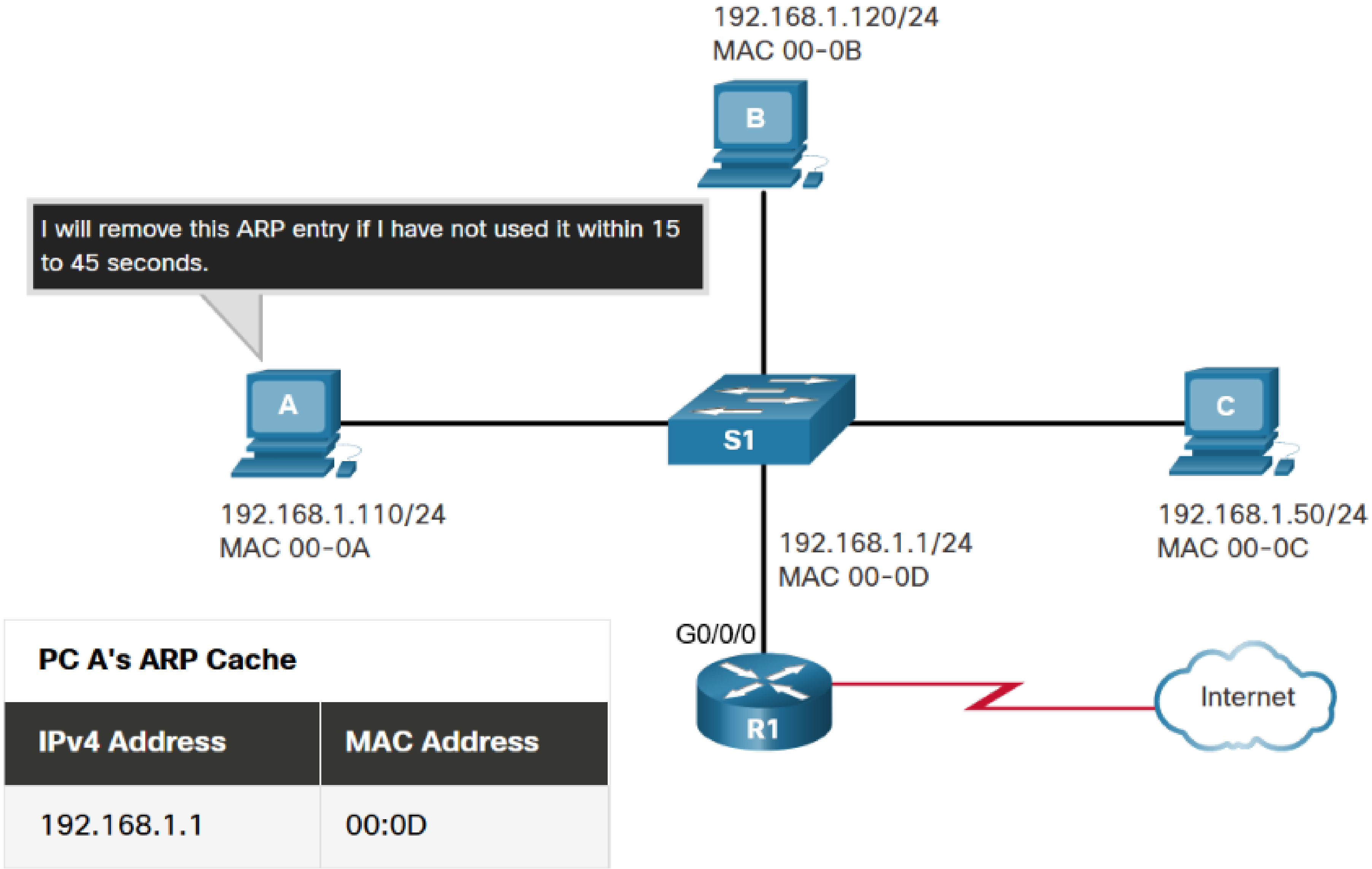
ARP REQUEST IS SENT TO THE DEFAULT GATEWAY

DEFAULT GATEWAY RESPONDS WITH ITS OWN MAC ADDRESS

GATEWAY IP AND MAC ADDRESS ARE ADDED TO COMPUTER "A" ARP TABLE

ROUTER WILL SEARCH REMOTE NETWORKS

Removing Entries from an ARP Table



I will remove this ARP entry if I have not used it within 15 to 45 seconds.

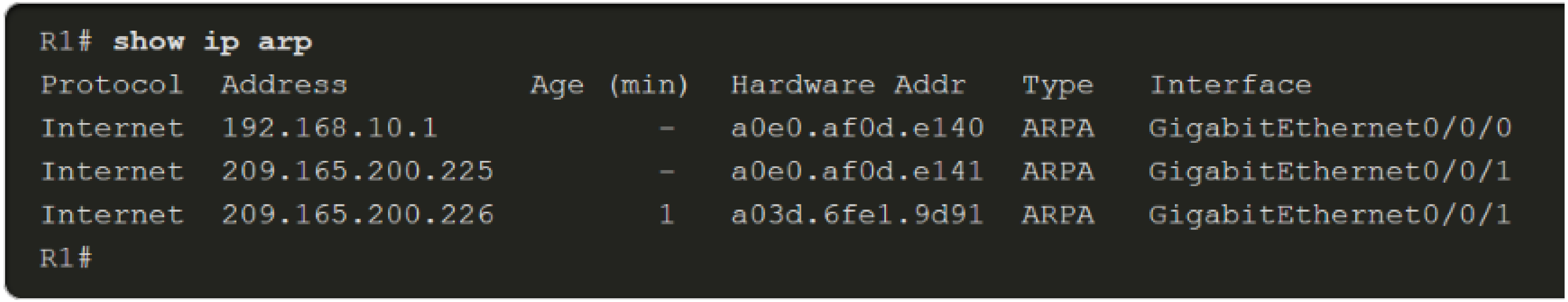
PC A's ARP Cache

IPv4 Address	MAC Address
192.168.1.1	00:0D

For each device, an ARP cache timer removes ARP entries that have not been used for a specified period of time. The times differ depending on the operating system of the device. For example, newer Windows operating systems store ARP table entries between 15 and 45 seconds, as illustrated in the figure.

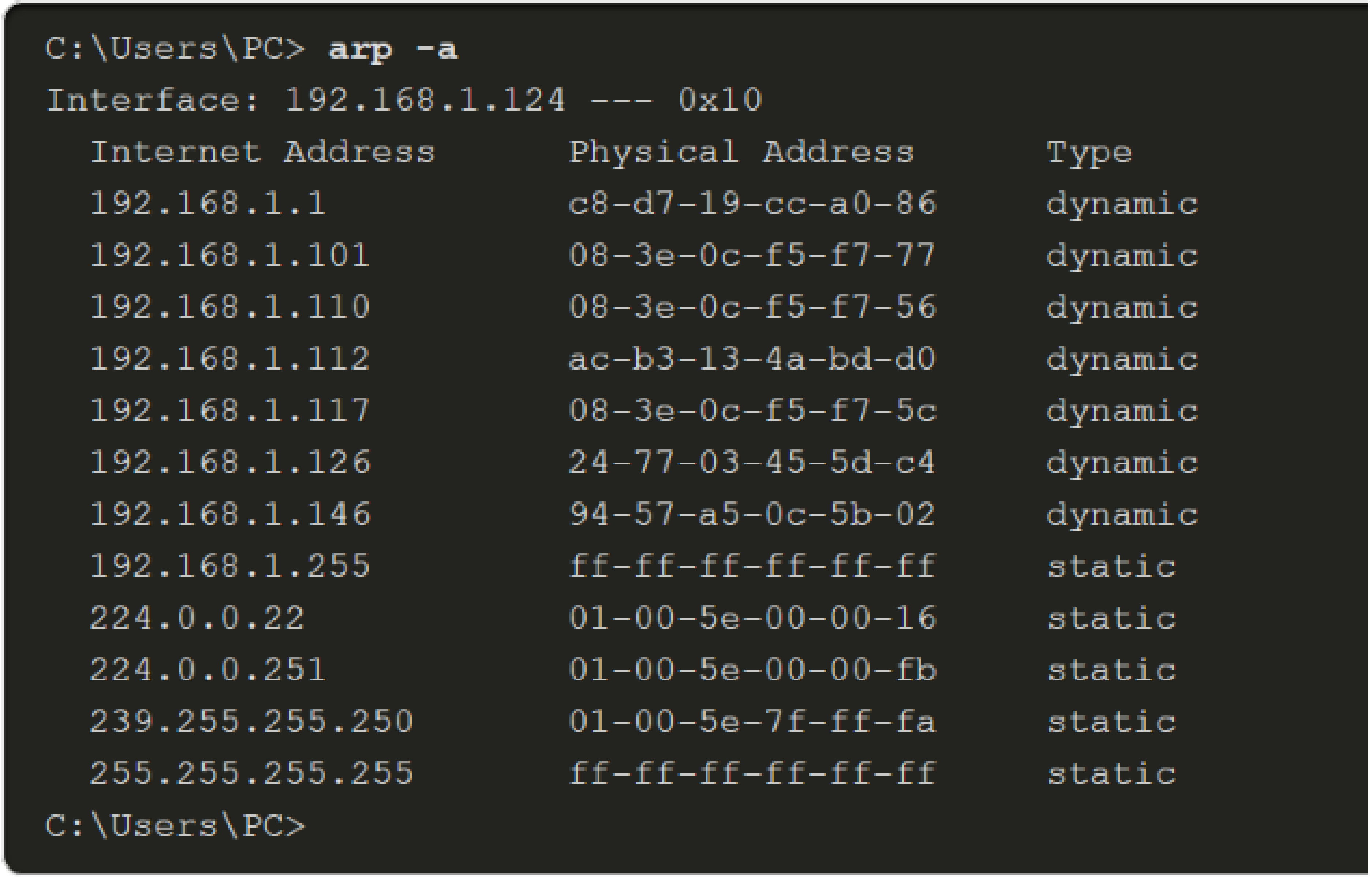
ARP Tables on Networking Devices

On a Cisco router, the show ip arp command is used to display the ARP table, as shown in the figure



```
R1# show ip arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  192.168.10.1             -  a0e0.af0d.e140  ARPA   GigabitEthernet0/0/0
Internet  209.165.200.225          -  a0e0.af0d.e141  ARPA   GigabitEthernet0/0/1
Internet  209.165.200.226          1  a03d.6fe1.9d91  ARPA   GigabitEthernet0/0/1
R1#
```

On a Windows 10 PC, the arp –a command is used to display the ARP table, as shown in the figure.



```
C:\Users\PC> arp -a
Interface: 192.168.1.124 --- 0x10
  Internet Address      Physical Address      Type
  192.168.1.1           c8-d7-19-cc-a0-86     dynamic
  192.168.1.101         08-3e-0c-f5-f7-77     dynamic
  192.168.1.110         08-3e-0c-f5-f7-56     dynamic
  192.168.1.112         ac-b3-13-4a-bd-d0     dynamic
  192.168.1.117         08-3e-0c-f5-f7-5c     dynamic
  192.168.1.126         24-77-03-45-5d-c4     dynamic
  192.168.1.146         94-57-a5-0c-5b-02     dynamic
  192.168.1.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
C:\Users\PC>
```

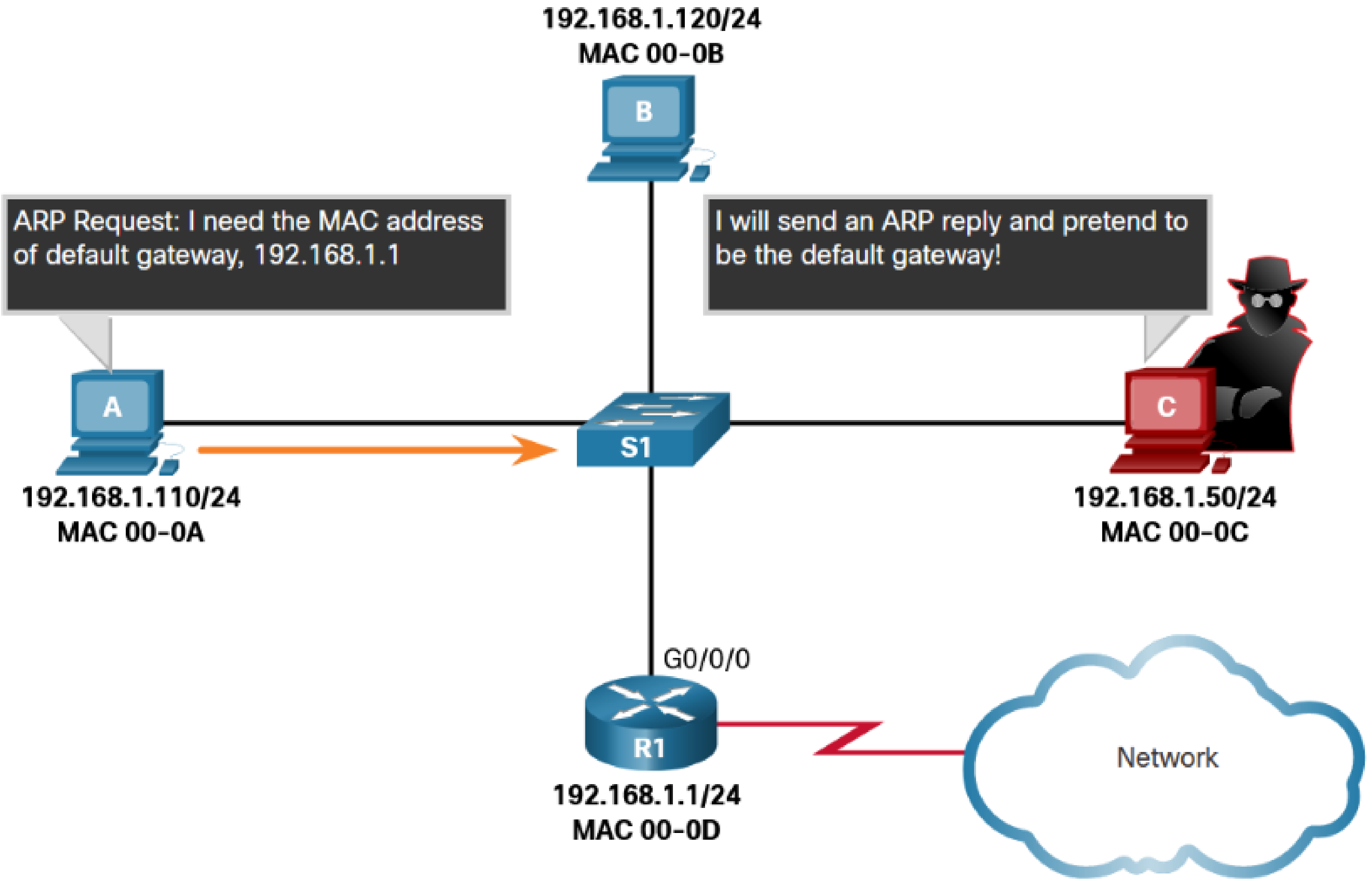
Check the ARP table on your personal computer.

Open a Command window

Type arp –a

You will see the ip and mac addresses of computers you have been accessing.

ARP SPOOFING

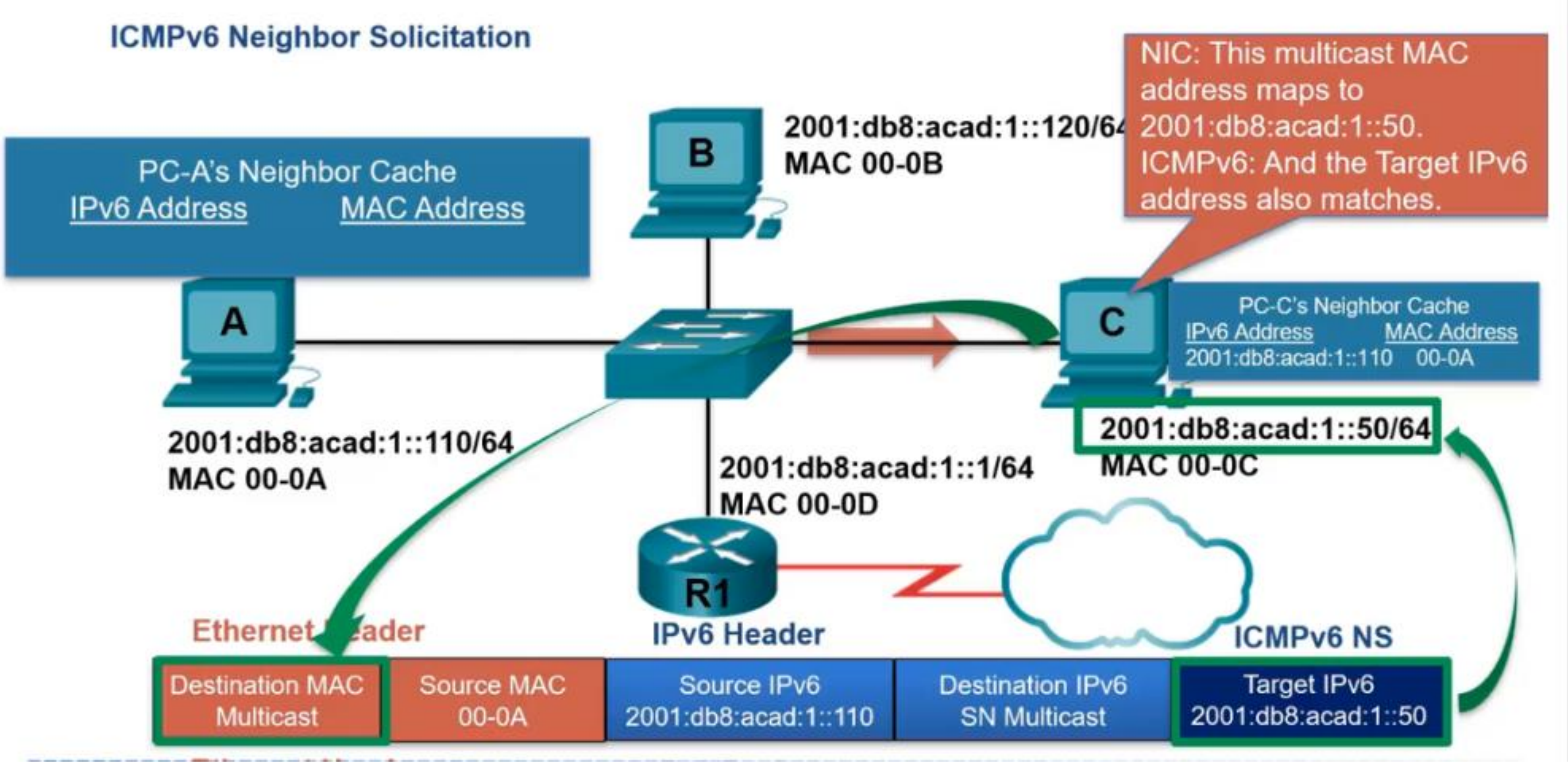


ARP Request: I need the MAC address of default gateway, 192.168.1.1

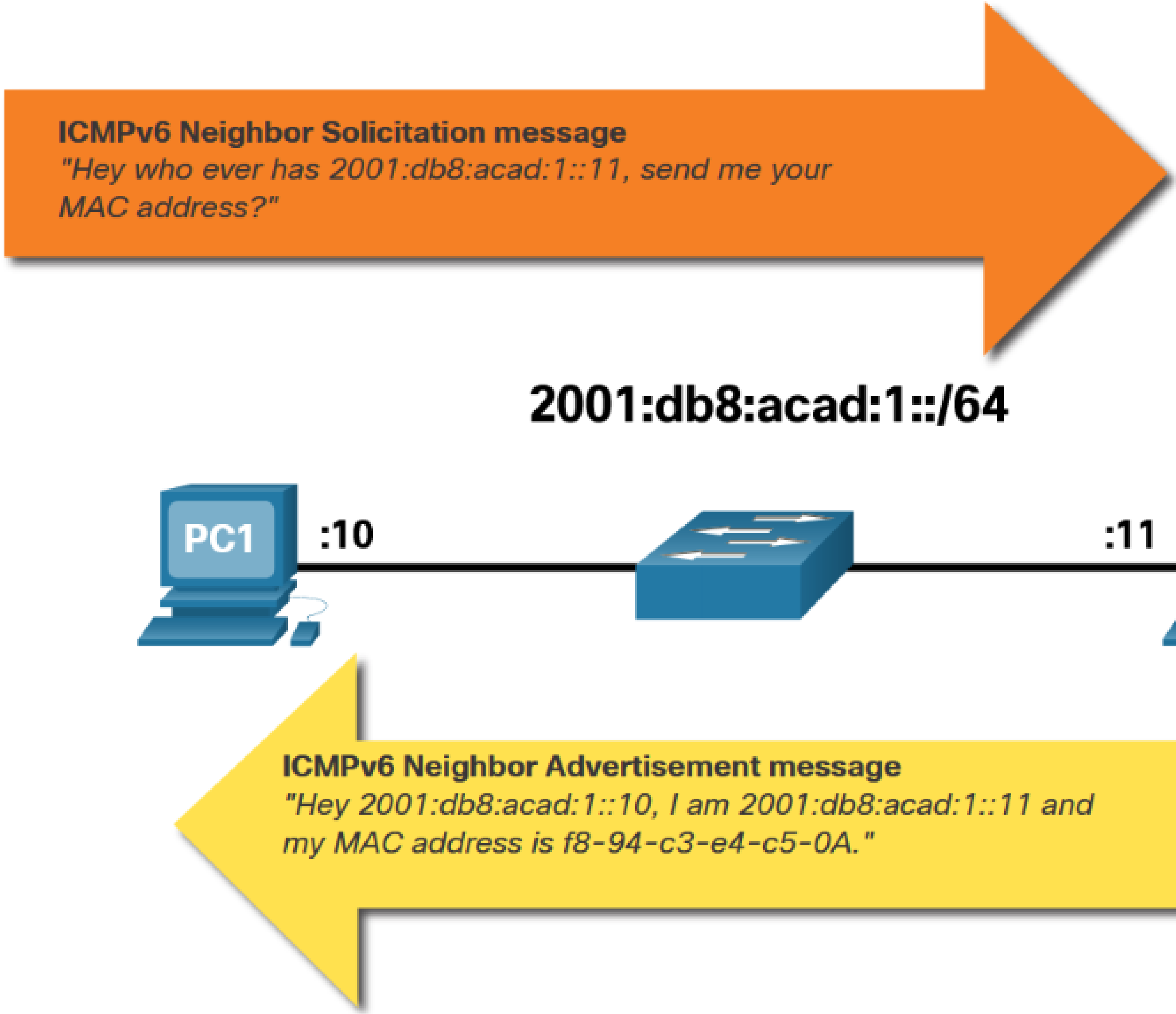
I will send an ARP reply and pretend to be the default gateway!

IPv6 Neighbor Discovery

If your network is using the IPv6 communications protocol, the Neighbor Discovery protocol, or ND, is what you need to match IPv6 addresses to MAC addresses. This topic explains how ND works.



IPv6 Neighbor Discovery - Address Resolution


ICMPv6 Neighbor Solicitation message
"Hey who ever has 2001:db8:acad:1::11, send me your MAC address?"
2001:db8:acad:1::/64
PC1
:10
:11
PC2
ICMPv6 Neighbor Advertisement message
"Hey 2001:db8:acad:1::10, I am 2001:db8:acad:1::11 and my MAC address is f8-94-c3-e4-c5-0A."

ICMPv6 Neighbor Solicitation messages are sent using special Ethernet and IPv6 multicast addresses. This allows the Ethernet NIC of the receiving device to determine whether the Neighbor Solicitation message is for itself without having to send it to the operating system for processing.

PC2 replies to the request with an ICMPv6 Neighbor Advertisement message which includes its MAC address.

THANK YOU FOR YOUR ATTENTION

IF YOU NEED MORE HELP, VISIT MY WEB PAGE:

www.edtechnology.com

YOU WILL FIND AN EMAIL LINK ON THE PAGE