In this section, we have focused on IPv4, and you may be wondering whether there is an IPv6 equivalent. The simple answer is yes, but in reality, it is a little more complex. IPv6 uses what is known as **unique local addresses**, which have the prefix `fc00::/7`. However, because IPv6 has so many addresses available compared to IPv4, these are not generally configured as there are enough public IPv6 addresses for every device in the world. We will discuss IPv6 in more detail in `Chapter 12`, *Understanding IPv6*.

MAC addresses

A MAC address is a means of identifying a device on the local network. It is an address that has many names. As well as being referred to as a MAC address, it is also referred to as a physical address, a hardware address, or a **burnt-in address** (**BIA**). These three variations refer to the fact that the MAC address is on the physical network card, or *burnt into* the network card.

A MAC address is represented as a 48-bit hexadecimal number. Hexadecimal is referred to as a base-16 numbering system. How hexadecimal works is beyond the scope of this book, but it is important that you are able to identify a MAC address. The following screenshot shows the output of the `ipconfig /all` command and shows the MAC address (listed as a physical address) of this network card as `08-00-27-F5-50-3F`. It should be noted that if you have multiple network cards, you will see multiple MAC addresses:

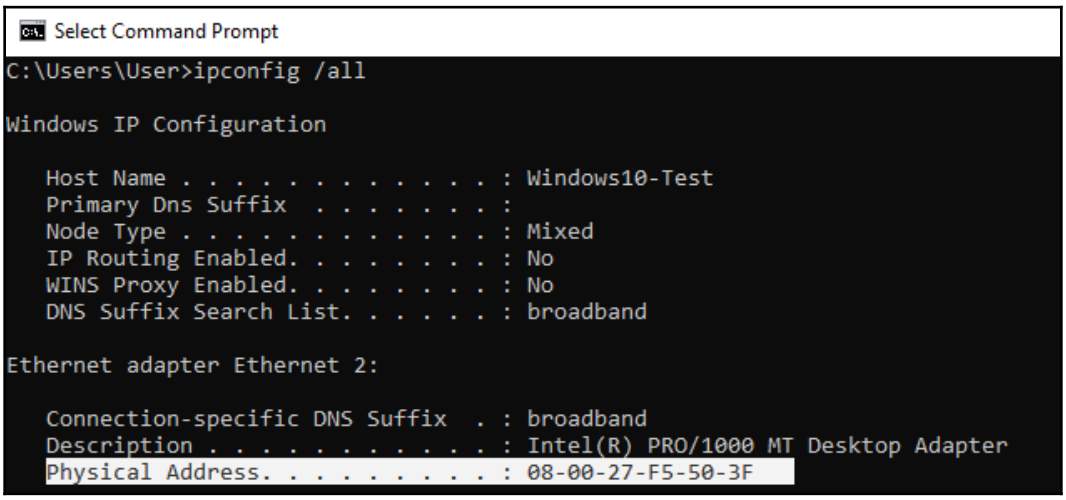

Figure 2.8: Output of ipconfig /all

In Linux, the equivalent to `ipconfig` is `ifconfig`. Although `ifconfig` is not mentioned in the exam objectives, it may appear in the answers as a distractor, and you might select it by accident under exam pressure.

Another method of listing your MAC addresses is by using the `getmac` command from the Command Prompt. However, the output is not as user-friendly, as shown in the following screenshot:

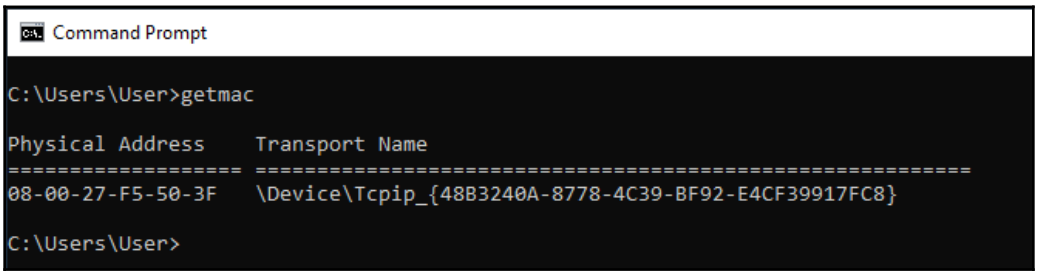

Figure 2.9: Output of getmac command

Here, we can see that the MAC address is comprised of 12 characters broken into 6 pairs. Each of these characters uses 4 bits (12 characters * 4 bits = 48 bits). As you can see, each pair is separated by a `-`. This is specific to Windows, and you may see `:`, `_`, or even no separator, depending on the system you are looking at.

You may be asked to identify a MAC address from an answer set. There are three things to look for: first, whether there are 12 characters, second, whether each individual character is either a number between 0-9 or a letter between A-F, and third, whether there are no double colons, for example, `::`. The latter is a legitimate character set in IPv6 addresses and may mislead you.

MAC addresses are not randomly generated. They should be globally unique and no two network cards should have the same MAC address. To facilitate this, each network card manufacturer is issued an **Organizationally Unique Identifier** (**OUI**). The OUI is the first six characters of the MAC address. Using the MAC address shown in the preceding screenshots, my OUI is `08-00-27`. Using an online OUI lookup website, I can see that my network card is from PCS Computer Systems GmbH. The last six characters should only be allocated to one network card by the manufacturer.

Activity 4: Identify your MAC address using any of the methods described previously. Then, using an online OUI lookup site, identify the manufacturer of your network card.

Although MAC addresses are supposed to be globally unique, they can be spoofed using software.

To find a MAC address related to a particular IP address, our computer will use the **Address Resolution Protocol** (**ARP**). When using the ARP, your computer shouts out to all the devices on the network (broadcasts), asking who has the IP address you are communicating with. All the devices on the network will receive that ARP request and will look at the IP address that was requested. If the IP address doesn't belong to that device, it will ignore the request. If the IP address does belong to the device, it will send an ARP reply saying that IP address ABC belongs to MAC address XYZ. The following screenshot shows a Wireshark capture of an ARP request, while the screenshot after that shows the ARP response.

In the following screenshot, we can see that, at *line 48*, the ARP request where the source MAC address `58:ba:d4:9c:10:80`, with a source IP address of `192.168.1.1`, is asking who has `192.168.1.15`. Note that the destination MAC address is `ff:ff:ff:ff:ff:ff`, which is a broadcast MAC address that's used when you want to speak to all the devices on the network:

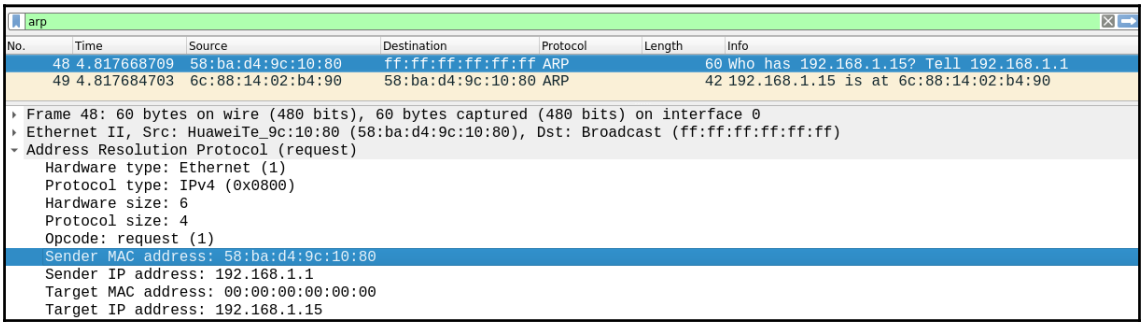

Figure 2.10: ARP request