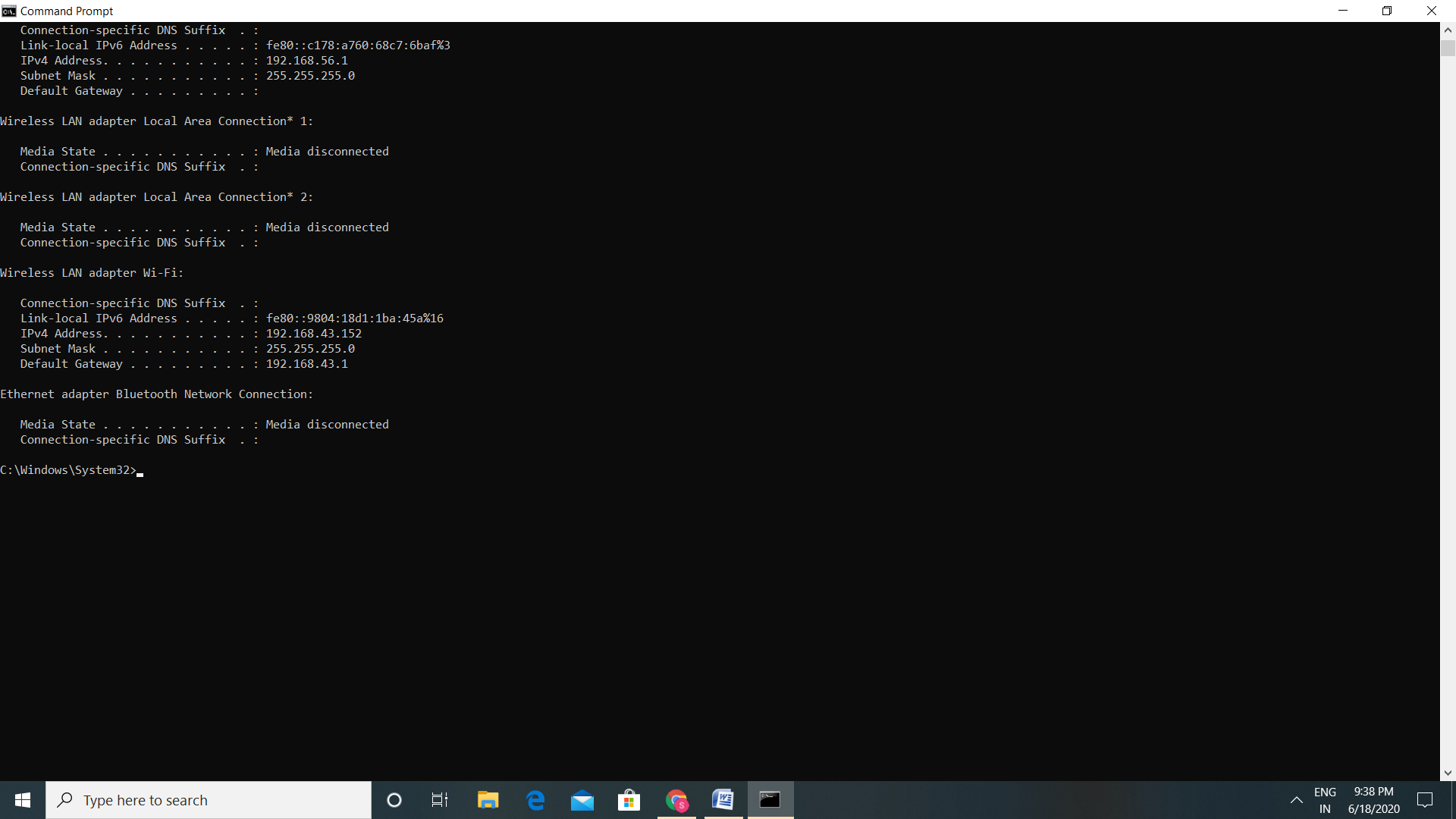
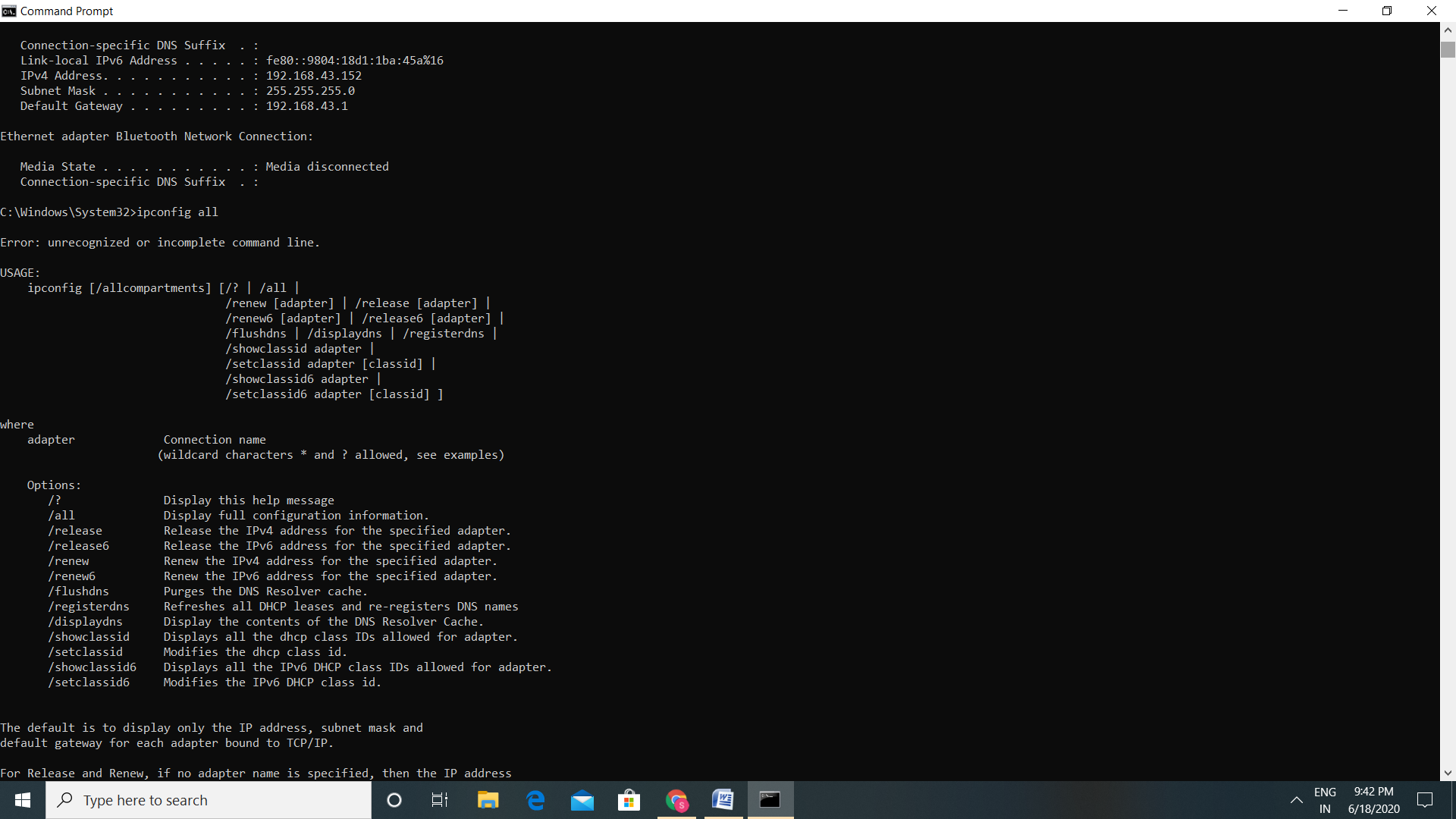
**Basic Network Utilities**

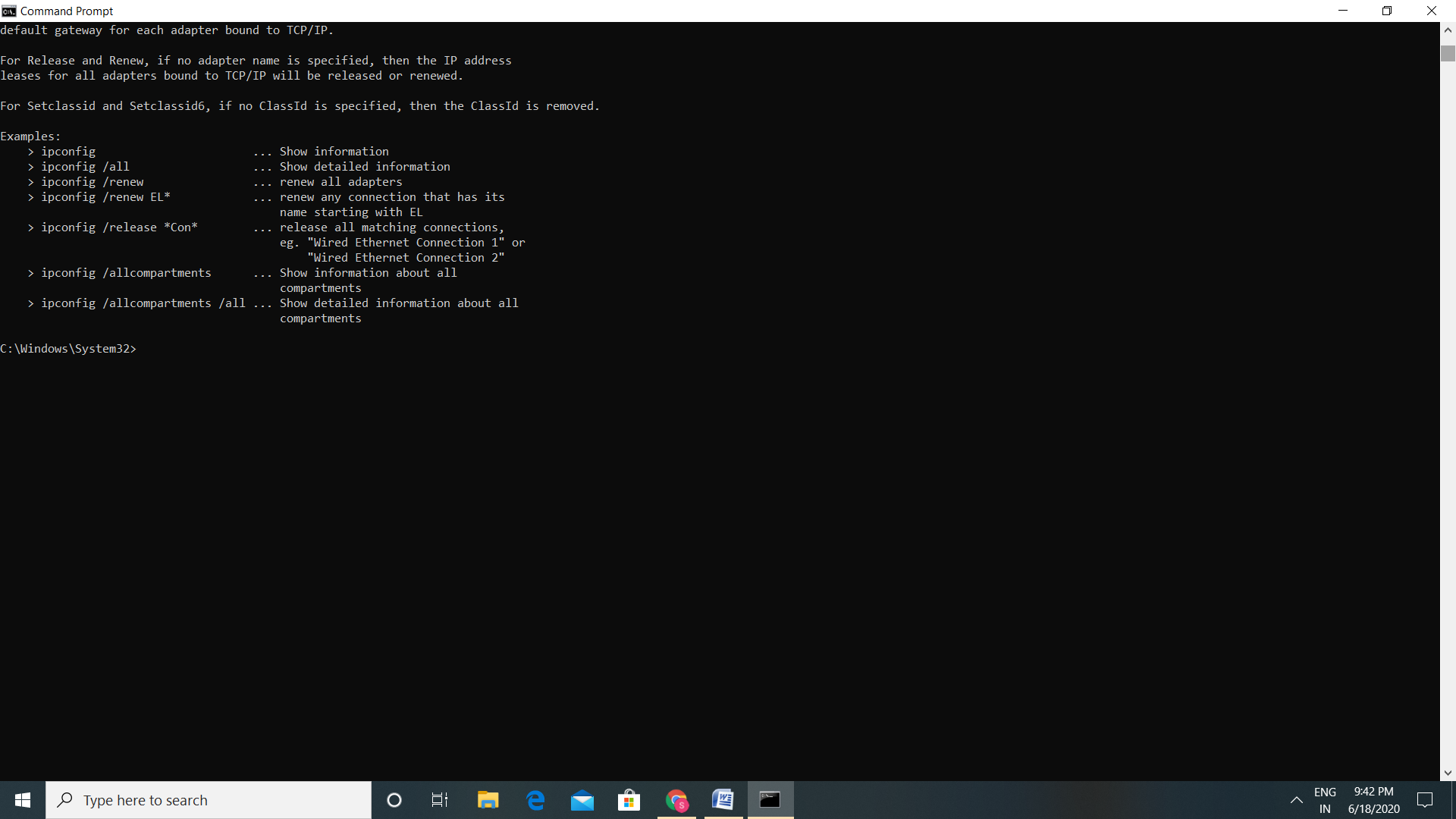
**Ipconfig**

The first thing we want to do is get information about our own system. To accomplish this, we must get a command prompt. In Windows, we do this by going to the Start menu, selecting All Programs, and then choosing Accessories. Now we can type in ipconfig. (we could input the same command in UNIX or Linux by typing in ifconfig from the shell.) After typing in ipconfig (ifconfig or ip addr in Linux), we should see something much like the below screenshot.



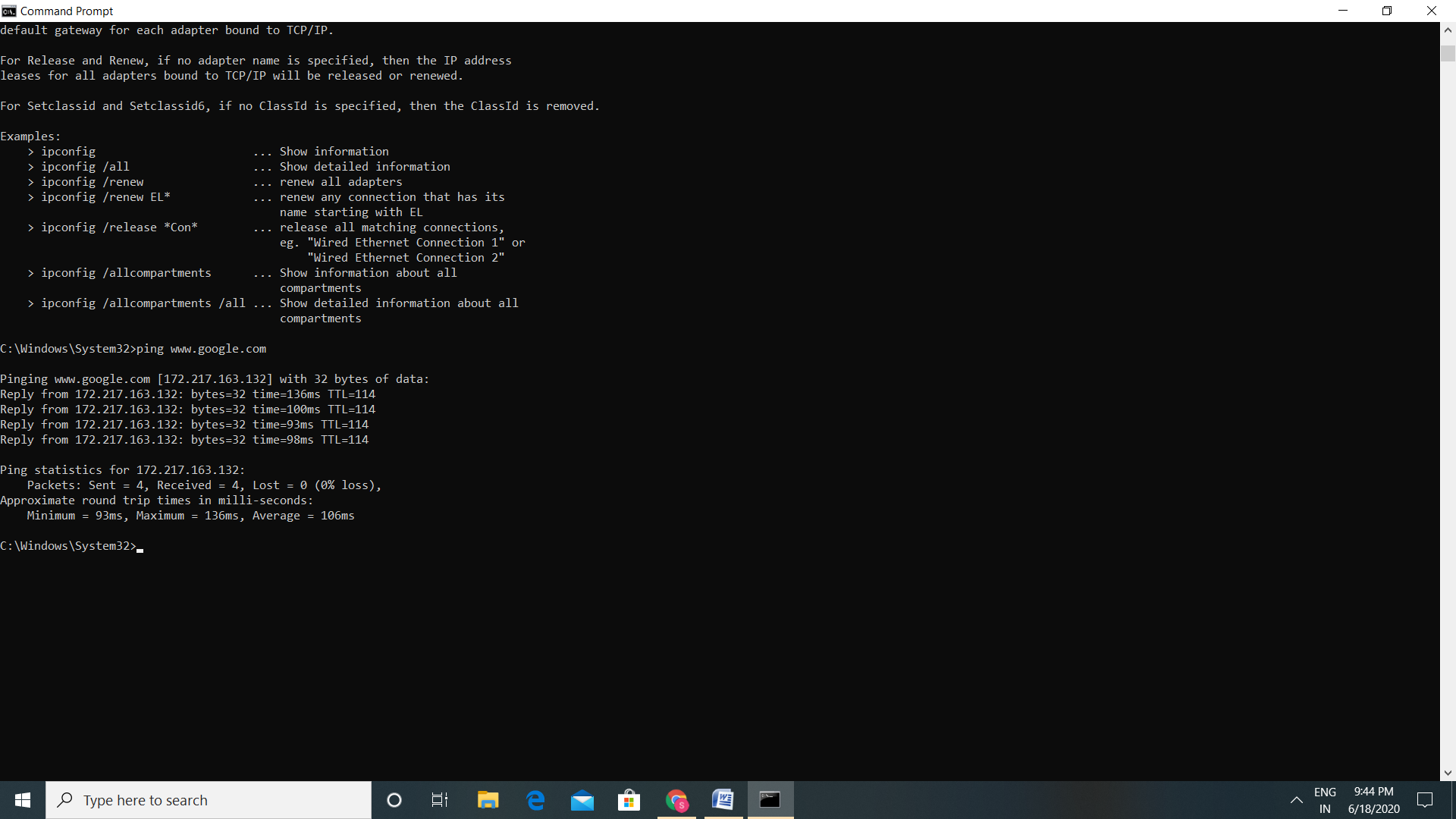
This command gives us information about our connection to a network (or to the Internet). Most importantly, we find out our own IP address. The command also has the IP address for our default gateway, which is our connection to the outside world. Running the ipconfig command is a first step in determining our system’s network configuration. Most commands including ipconfig have a number of parameters, or flags, which can be passed to the commands to make the computer behave in a certain way. we can find out what these commands are by typing in the command, followed by a space, and then typing in hyphen question mark: -?.The most commonly used method would probably be ipconfig/all.





**Ping**

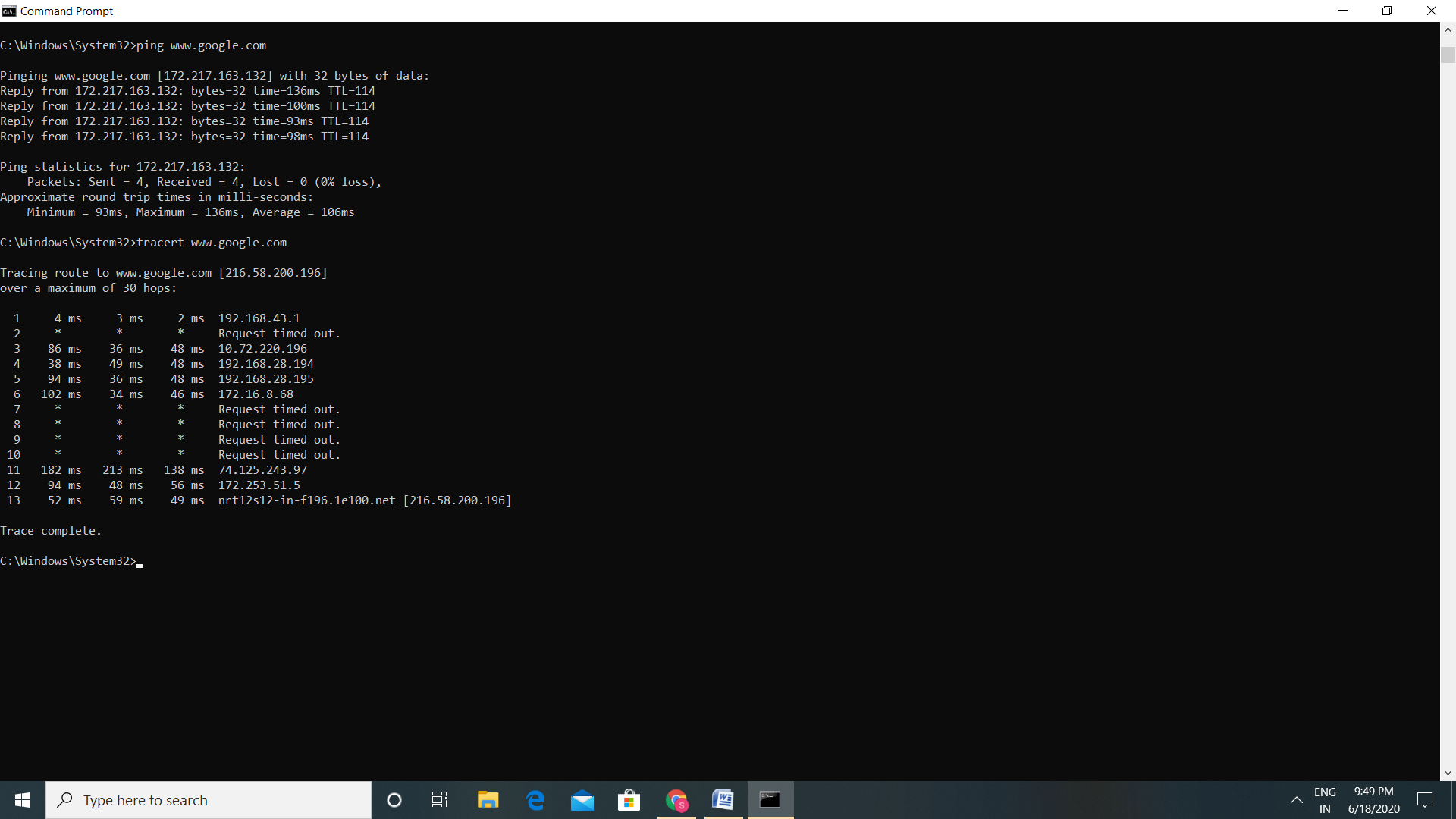
Another common used command is ping. Ping is used to send a test packet, or echo packet, to a machine to find out whether the machine is reachable and how long the packet takes to reach the machine. This useful diagnostic tool can be employed in elementary hacking techniques.



The above command shows that a 32-byte echo packet was sent to the destination and returned. The TTL means “time to live.” That time unit is how many intermediary steps, or hops, the packet should take to the destination before giving up. Remember that the Internet is a vast conglomerate of interconnected networks. our packet probably won’t go straight to its destination. It will have to take several hops to get there. As with ipconfig, we can type in ping -? to find out various ways we can refine our ping.

**Tracert**

The next command is tracert. This command is a sort of “ping deluxe.” Tracert not only tells you whether the packet got there and how long it took, but it also tells you all the intermediate hops it took to get there. (This same command can be executed in Linux or UNIX, but it is called traceroute rather than tracert.)



With tracert, we can see (in milliseconds) the time the IP addresses of each intermediate step listed, and how long it took to get to that step. Knowing the steps required to reach a destination can be very important.

**Netstat**

Netstat is another interesting command. It is an abbreviation for Network Status. Essentially, this command tells us what connections our computer currently has. Don’t panic if one see several connections; that does not mean a hacker is in their computer. We will see many private IP addresses. This means our network has internal communication going on. Certainly, other utilities can be used when working with network communications. However, the four we just examined are the core utilities. These four (ipconfig, ping, tracert, and netstat) are absolutely essential to any network administrator.

