

## Assignment 5-1: ARP, CLS, Command History, and DHCP Exercises

Name: \_\_\_\_\_

### Objective

In this exercise, you will display, clear, and establish a new ARP table and look at DHCP services using the IPCOFIG commands. **CLS** clears the command window.

### Scenario

This lab assumes you are using any version of Windows. This is a non-destructive lab, and you should be able to do it with your home computer without concern of changing your system configuration.

Mac users: The Mac **Terminal** application should allow you to accomplish similar results, but I have not tested it. A resource you might find useful in the conversion is: <http://krypted.com/mac-security/mac-network-commands-cheat-sheet/>

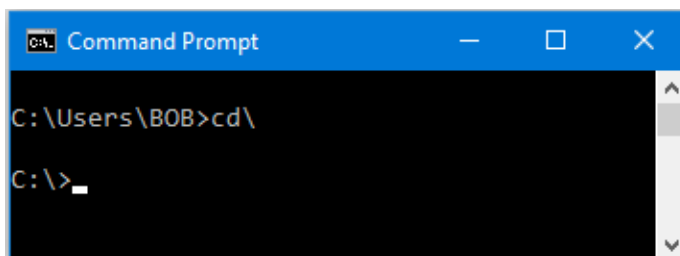
Ideally, this lab will be done in a classroom or other LAN connected to at least one other device. A home network with a couple devices will work as well. Try it in a couple of different locations and note your results.

### ARP – Address Resolution Protocol

#### Part 1

Open the command window as you did in the Module 1 exercises. **Start | Run** and type **cmd** and **Enter** should do it.

Use the **cd\** command to move the cursor to the root (main) directory. This is not necessary to run the commands, but it will make your output similar to the examples.



```

C:\Users\BOB>cd\
C:\>_

```

Type the **ARP** command and press **Enter** – the command is not case sensitive. Don't be alarmed; our command is incomplete, and the system is displaying a Help screen telling us that **switches** are required for the command.

Switches are codes telling the system what we want the ARP command to do. The switches are letters like **-a** and in some cases, might require additional information.

Take a moment and look at the output and you will see that there are six letter switches including **a**, **g**, **v**, **N**, **d**, and **s**. We also see that some commands require one or more of the following parameters.

**inet\_addr**      internet address (IP address).

**if\_addr**        network interface specified by if\_addr.

**eth\_addr**      physical address (MAC address).

If the parameter in the Help in square brackets [ ] it is optional. Otherwise it is required.

The good news, we only care about two of the switch options

## Part 2

Run the **arp -a** command and look over your results. Your results will vary from mine and in length depending on the number of devices active on the network. You should be able to identify your interface IP address, the network and all networks broadcast addresses (all fs **ff-ff-ff-ff-ff-ff**). Chances are your router IP address will end in .1 – the first usable IP address on the network as a best practice.

A computer will typically have just one interface, but routers and switches would have more.

```

C:\>arp -a

Interface: 192.168.7.105 --- 0x13
Internet Address      Physical Address      Type
192.168.7.1           ec-08-6b-ae-e6-c8    dynamic
192.168.7.5           00-90-a9-ec-54-ed    dynamic
192.168.7.6           9c-b6-54-ef-41-a4    dynamic
192.168.7.106         38-01-95-74-54-59    dynamic
192.168.7.255         ff-ff-ff-ff-ff-ff    static
224.0.0.2             01-00-5e-00-00-02    static
224.0.0.22            01-00-5e-00-00-16    static
224.0.0.251           01-00-5e-00-00-fb    static
224.0.0.252           01-00-5e-00-00-fc    static
239.255.255.250       01-00-5e-7f-ff-fa    static
255.255.255.255       ff-ff-ff-ff-ff-ff    static
  
```

The **dynamic** entries were learned by the interface; the **statics** were configured (by the system in most cases). The **arp -s** command would allow you to add static entries, but that is rare today.

The **224.** and **239.** addresses are reserved addresses for multicast traffic.

In the above example, the .105 and .106 are my laptop and tower. .1 is my router, .2 is my printer, and .5 is my Amazon Echo. The last three are outside of the DHCP assignment range (.100-.150) and are reserved, so they don't change.

Note that **arp -g** would yield the same result. Try it if you like.

**Note:** You can Google the 224. and 239. Addresses and often find out what service is using them. I found that:

- **224.0.0.251** was probably iTunes
- **224.0.0.252** is Windows' Link-Local Multicast Name Resolution (LLMNR) searching for local network computers
- **224.0.1.60** is used by HP printers to discover other printers or print servers
- **239.255.255.250** is Simple Service Discovery Protocol address an advertisement and discovery of network services and presence information

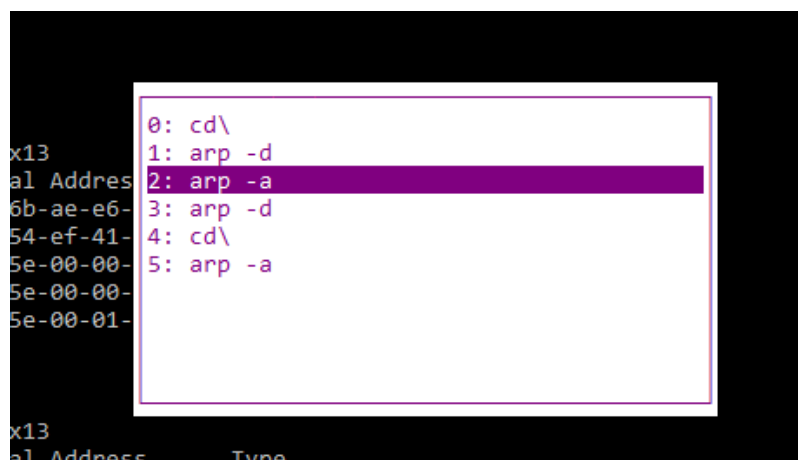
Or go to Wikipedia for **Multicast address** to see an extensive list of the common ones:

[https://en.wikipedia.org/wiki/Multicast\\_address](https://en.wikipedia.org/wiki/Multicast_address)

Remember that I told you that your computers and networks are pretty chatty devices, which is why switches and access points have no trouble keeping track of you.

### Part 3

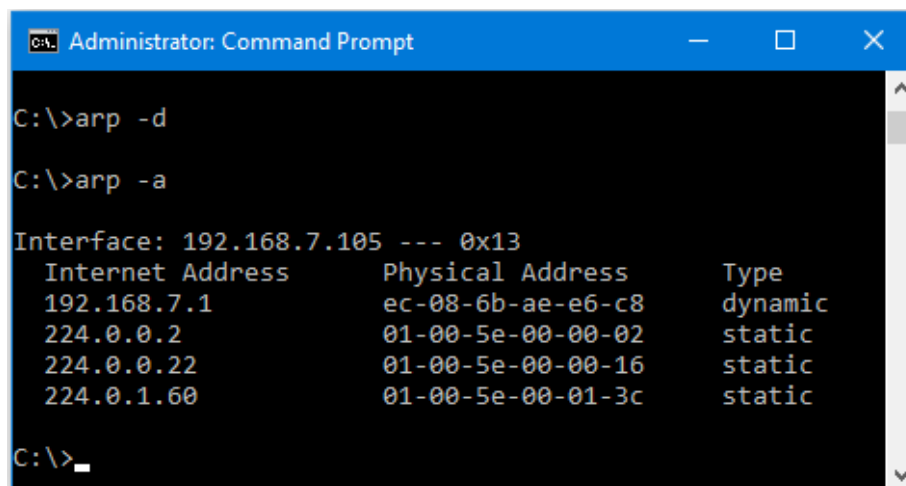
If the Command window is still open, press the up-arrow on your keyboard and notice that it brings back your last command. This is your **Command History**. Up and down arrows let you recall and reuse commands. Press **F7** to see your command history in a pop-up. Note only the arrow keys will work in the pop-up.



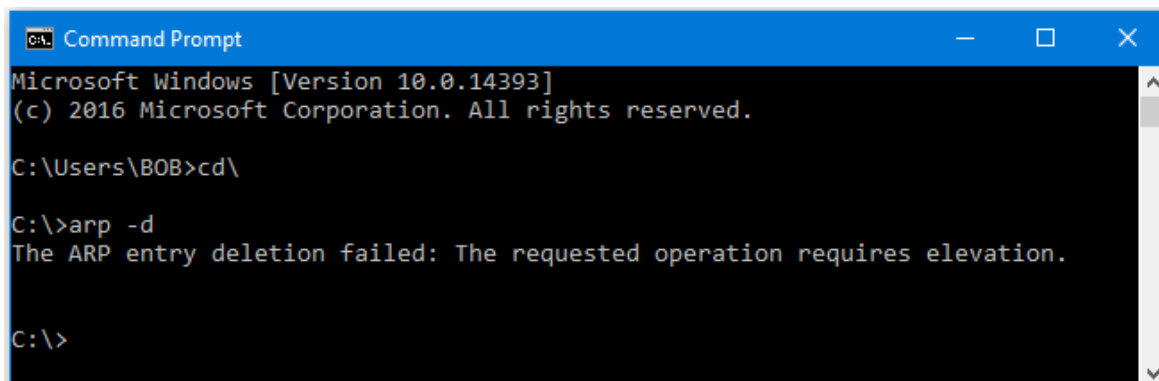
The **CLS** command will clear the command window, but not the history.

### Part 4

In the command window, run **arp -a** then use the up-arrow and change the command to run **arp -d**. Quickly use the up-arrow to rerun **arp -a** and notice the table is cleared of many entries although some of the static entries either never go away or repopulate very quickly. Repeat **arp -a** periodically and see how quickly your table rebuilds.

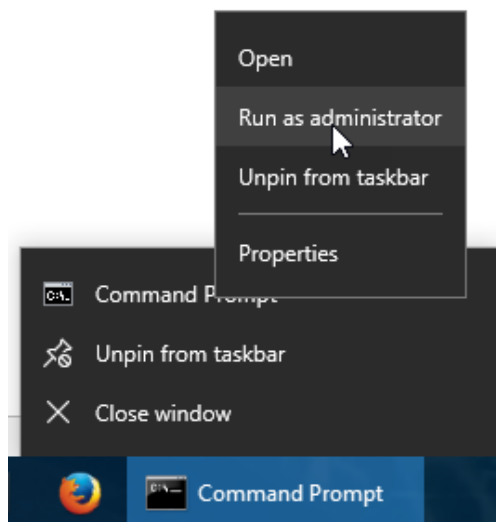


If you get the following message, don't panic.

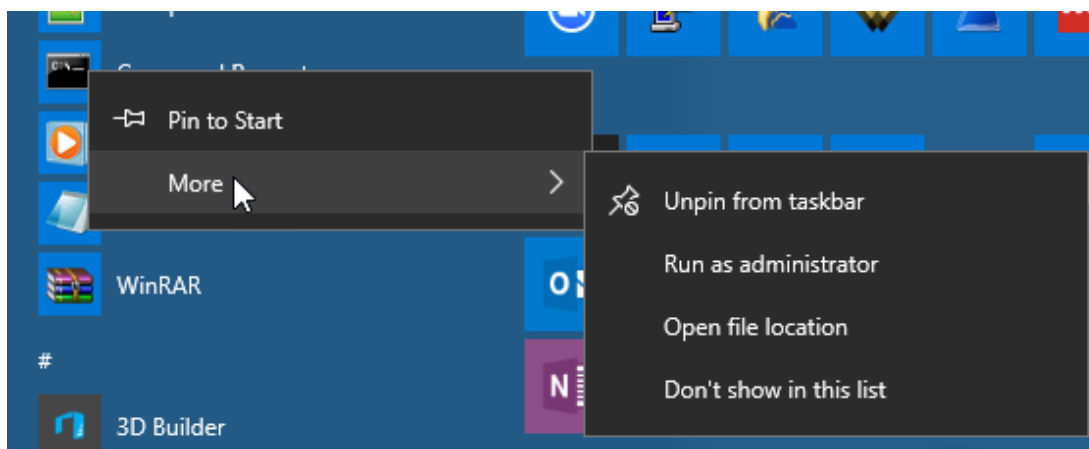


It means your user account doesn't have **Local Admin** privileges. That is not uncommon in the work environment, and some of us old timers still use two accounts. The **User account**, which can't install software or approve upgrades and an **Admin account** that can. It is a quite effective way to thwart virus and other online bad guys from installing problems on my computer.

So, how do we get around it? Right-click on the **Command Prompt** button and choose **Run as administrator**. You will be prompted for an Admin password.



If you do it on the Start menu, it is under the More option.



## DHCP – Dynamic Host Configuration Protocol

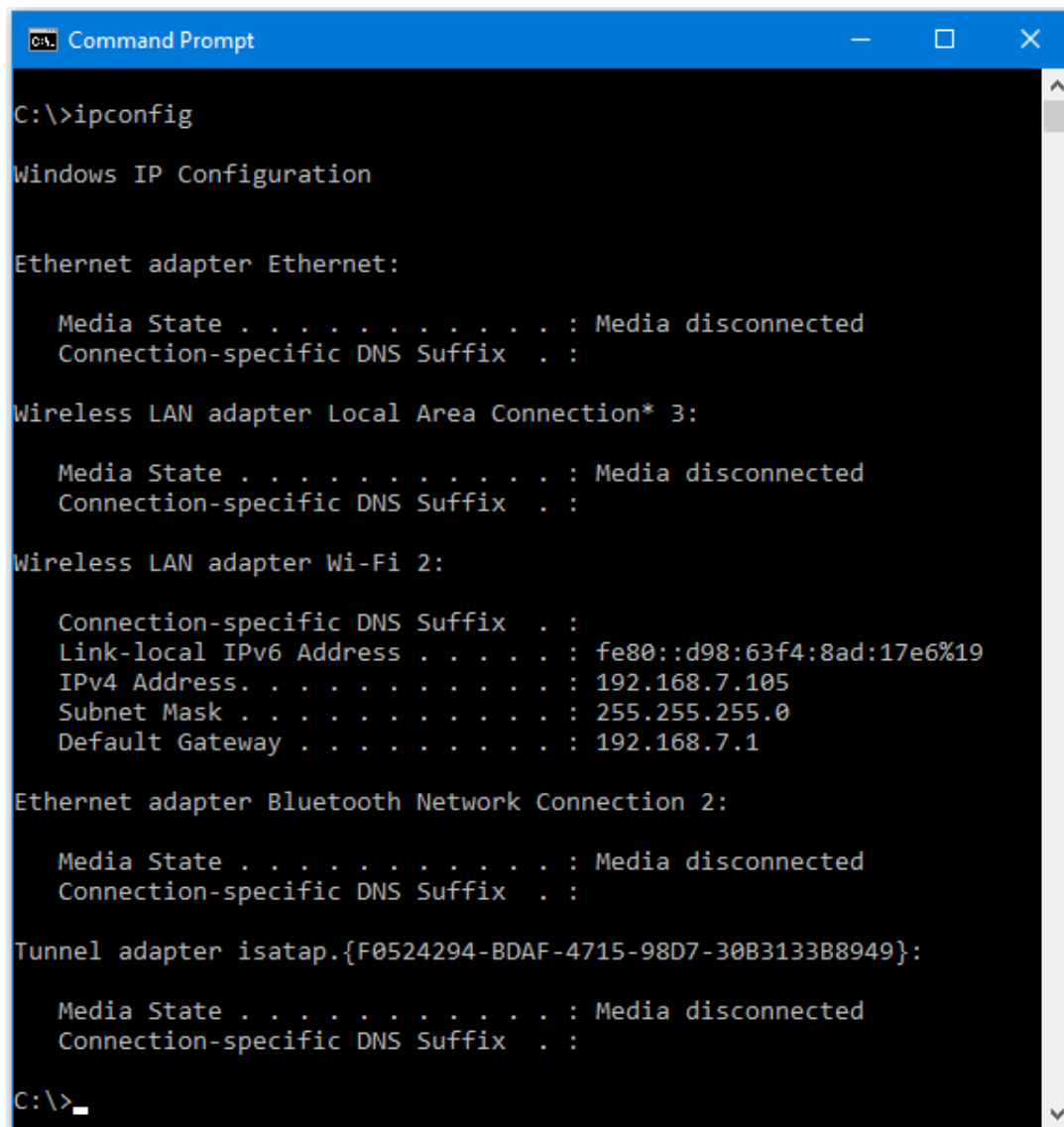
DHCP is a server-based protocol so we can't directly communicate with it from our computer like we did ARP, but we can use the IPCONFIG commands to change our computer's configuration and thereby see the results of DHCP.

**IPConfig** is a command-line tool that displays the current configuration of the installed IP stack on a networked computer. The configuration information can be done manually, but believe me there are many reasons you don't want to do that on most devices. The exception, if any, is networking devices like printers, switches, routers, and firewalls – devices that you do not want changing IP addresses. All other devices on the network rely on those devices not changing addresses.

Let's look at the ipconfig command.

## Part 1

In the command window, type **ipconfig** and press **Enter**. Note that you get a very limited display of the IP configuration. Yours will vary but note that any inactive interfaces or connection points show **Media disconnected**.



```

C:\>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 3:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi 2:

    Connection-specific DNS Suffix  . :
    Link-local IPv6 Address . . . . . : fe80::d98:63f4:8ad:17e6%19
    IPv4 Address. . . . . : 192.168.7.105
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.7.1

Ethernet adapter Bluetooth Network Connection 2:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Tunnel adapter isatap.{F0524294-BDAF-4715-98D7-30B3133B8949}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

C:\>_
  
```

Notice that we get only an IPv4 IP address, subnet mask, and default gateway (router interface) and an IPv6 Link-Local address.

To see the ipconfig options, run **ipconfig /?** Wow! That went fast.

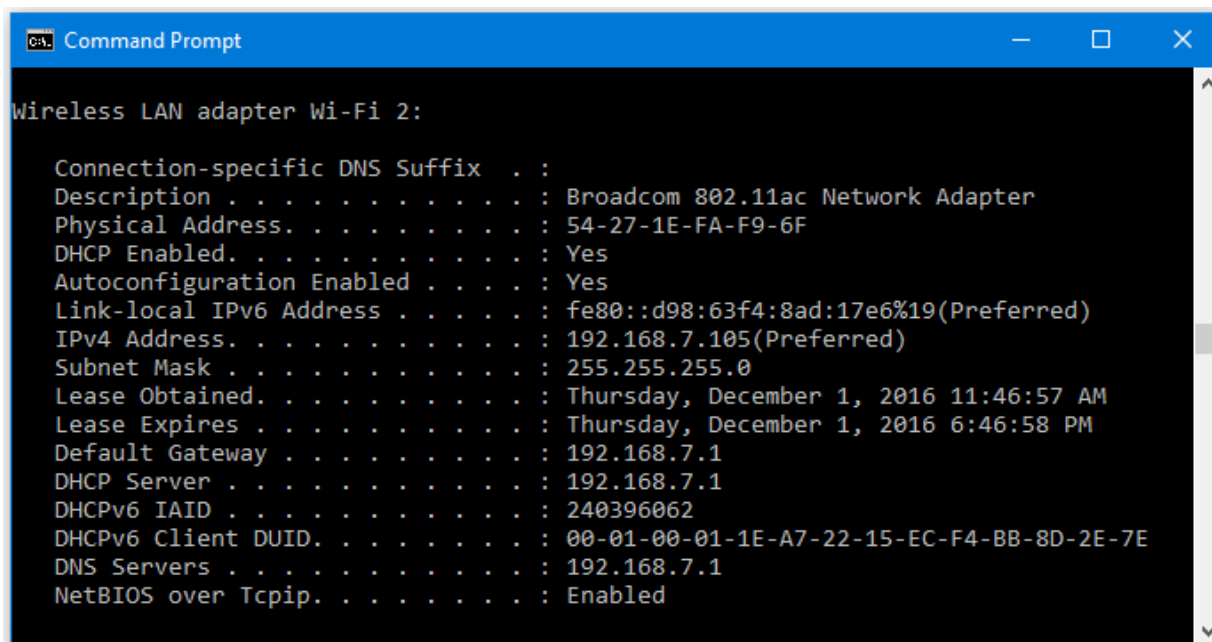
**Note:** **/?** is a common command switch for summoning help. It would have worked with ARP as well, except ARP automatically shows the Help any time it becomes obvious that you don't know what you are doing.

To slow the output down try this: **ipconfig /all | more**

The spacebar will now let you advance one screen at a time.

Scroll through until you find your active interface information.

I know that you looked at this in the Module 1 exercises so we won't go over everything again. Mine looked like this:



```

C:\>ipconfig /all

Wireless LAN adapter Wi-Fi 2:

    Connection-specific DNS Suffix  . : 
    Description . . . . . : Broadcom 802.11ac Network Adapter
    Physical Address. . . . . : 54-27-1E-FA-F9-6F
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes
    Link-local IPv6 Address . . . . . : fe80::d98:63f4:8ad:17e6%19(Preferred)
    IPv4 Address. . . . . : 192.168.7.105(Preferred)
    Subnet Mask . . . . . : 255.255.255.0
    Lease Obtained. . . . . : Thursday, December 1, 2016 11:46:57 AM
    Lease Expires . . . . . : Thursday, December 1, 2016 6:46:58 PM
    Default Gateway . . . . . : 192.168.7.1
    DHCP Server . . . . . : 192.168.7.1
    DHCPv6 IAID . . . . . : 240396062
    DHCPv6 Client DUID. . . . . : 00-01-00-01-1E-A7-22-15-EC-F4-BB-8D-2E-7E
    DNS Servers . . . . . : 192.168.7.1
    NetBIOS over Tcpip. . . . . : Enabled
  
```

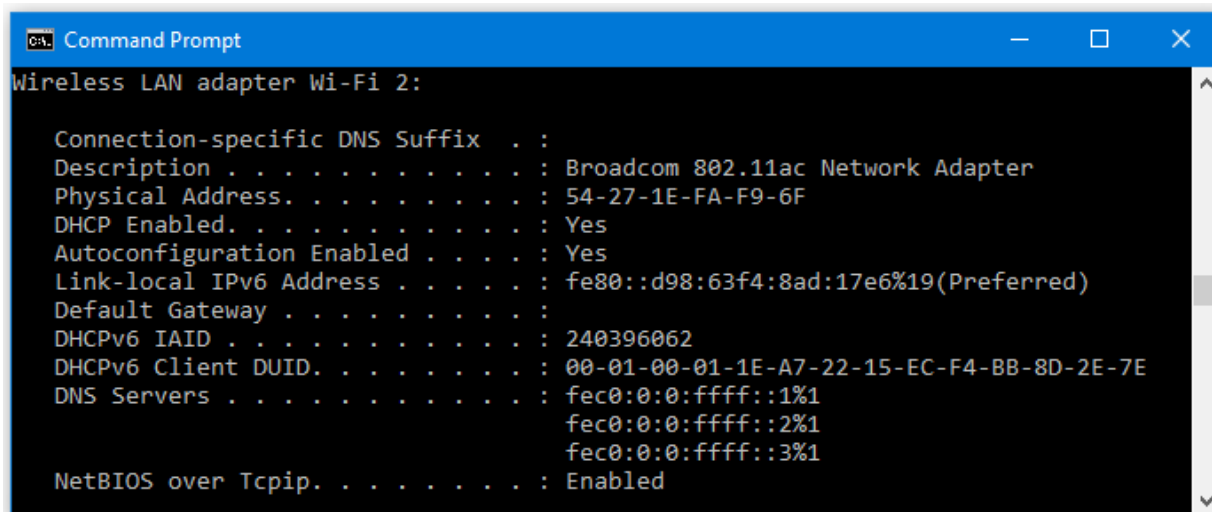
A couple notes: My DHCP and DNS are the same as my default gateway, which tells me my router is performing those functions. That would be the norm in a home, small office, public WiFi Hotspot, but probably not the case in a larger business network where servers would perform those functions.

DHCP and Autoconfiguration are both enabled – the norm today.

I also see that my IP address and configuration Lease is at seven hours. You might find that shorter in places where mobile devices come and go frequently, like at a public WiFi Hotspot, McDonald's, Starbucks, etc. Otherwise, they could run out IP addresses in the DHCP pool while many of the devices are no longer present.

## Part 2

Note your interface, and then run **ipconfig /release** followed by **ipconfig /all**



```

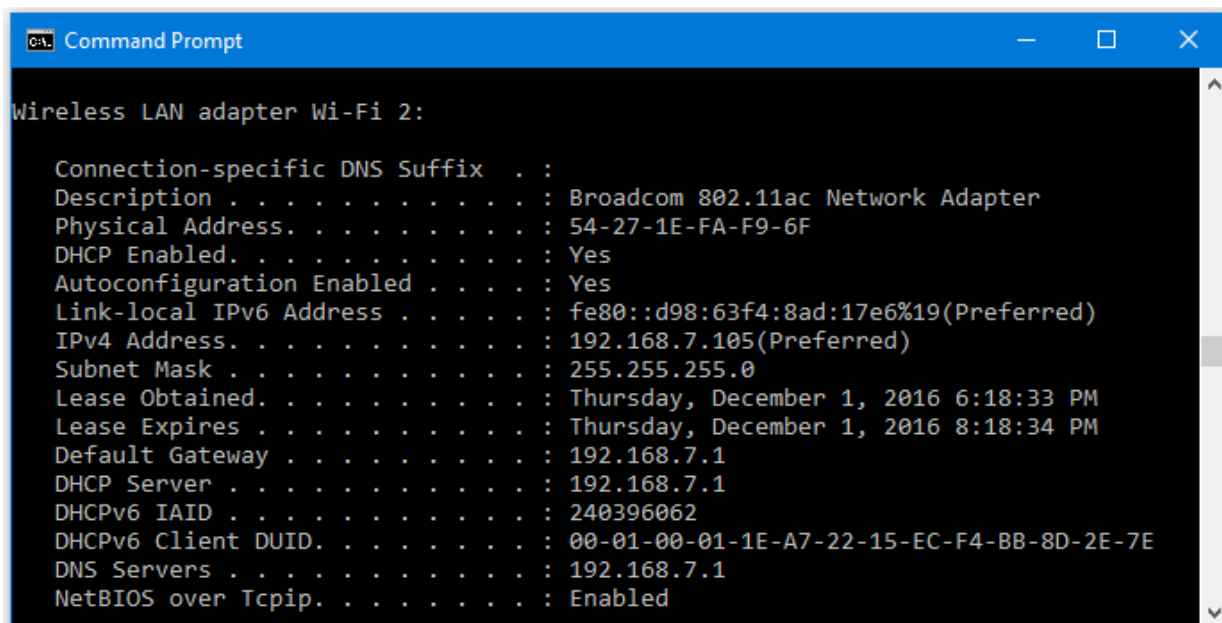
C:\>ipconfig /all

Wireless LAN adapter Wi-Fi 2:

    Connection-specific DNS Suffix  . : 
    Description . . . . . : Broadcom 802.11ac Network Adapter
    Physical Address. . . . . : 54-27-1E-FA-F9-6F
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes
    Link-local IPv6 Address . . . . . : fe80::d98:63f4:8ad:17e6%19(Preferred)
    Default Gateway . . . . . : 
    DHCPv6 IAID . . . . . : 240396062
    DHCPv6 Client DUID. . . . . : 00-01-00-01-1E-A7-22-15-EC-F4-BB-8D-2E-7E
    DNS Servers . . . . . : fec0:0:0:ffff::1%1
                           fec0:0:0:ffff::2%1
                           fec0:0:0:ffff::3%1
    NetBIOS over Tcpip. . . . . : Enabled
  
```

Pretty bleak huh? If you try your browser, you'll find that you have no Internet.

Bring up your last command and edit it to **ipconfig /renew** and then **ipconfig /all**



```

Wireless LAN adapter Wi-Fi 2:

    Connection-specific DNS Suffix  . : 
    Description . . . . . : Broadcom 802.11ac Network Adapter
    Physical Address. . . . . : 54-27-1E-FA-F9-6F
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes
    Link-local IPv6 Address . . . . . : fe80::d98:63f4:8ad:17e6%19(Preferred)
    IPv4 Address. . . . . : 192.168.7.105(Preferred)
    Subnet Mask . . . . . : 255.255.255.0
    Lease Obtained. . . . . : Thursday, December 1, 2016 6:18:33 PM
    Lease Expires . . . . . : Thursday, December 1, 2016 8:18:34 PM
    Default Gateway . . . . . : 192.168.7.1
    DHCP Server . . . . . : 192.168.7.1
    DHCPv6 IAID . . . . . : 240396062
    DHCPv6 Client DUID. . . . . : 00-01-00-01-1E-A7-22-15-EC-F4-BB-8D-2E-7E
    DNS Servers . . . . . : 192.168.7.1
    NetBIOS over Tcpip. . . . . : Enabled
  
```

Note it probably gave you the same IP and the other devices would be unchanged, but note the new **Lease Obtained** and **Lease Expires**. What we now know is that my DHCP initially gives out two-hour leases. At the mid-point of the lease, if my computer is still on it, it automatically requests and renewal. So, the seven hours we saw earlier was the total time the machine had been on the network.

## Copying Your Output

You can copy the output if you like. If it is all visible in the command window, you can just highlight it normally and press Enter. Then go to where you want it and do a paste. You will need to change the font to **Courier New** to get it to look right.

If what you want is more than command window, scroll up to the beginning. Right-click on the **Command Prompt icon** in the upper left corner and pick **Edit | Mark**. Then select by dragging over and down until everything you want is selected and press **Enter**. Paste and format as before.