**20PW14**

## 20XC46 COMPUTER NETWORKS LAB

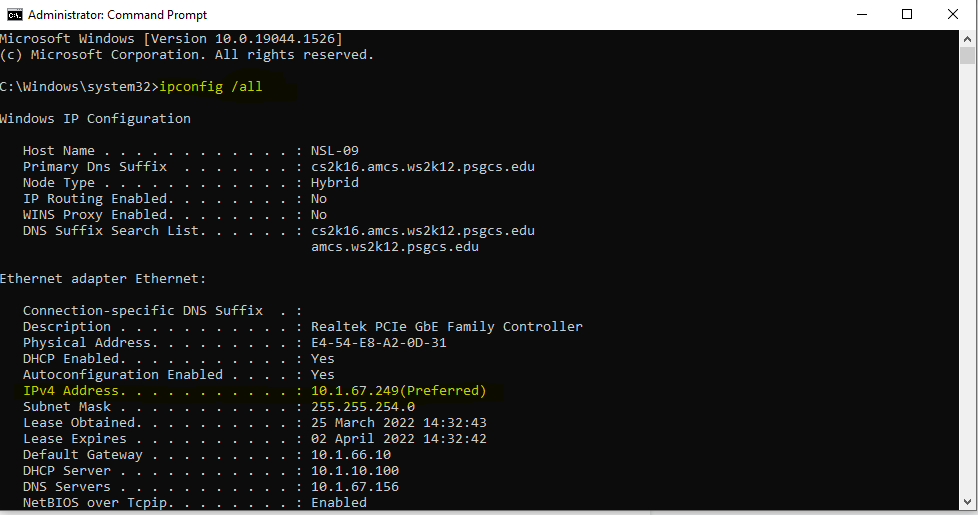
&

## 20XW46 COMPUTER NETWORKS AND TCP/IP LAB

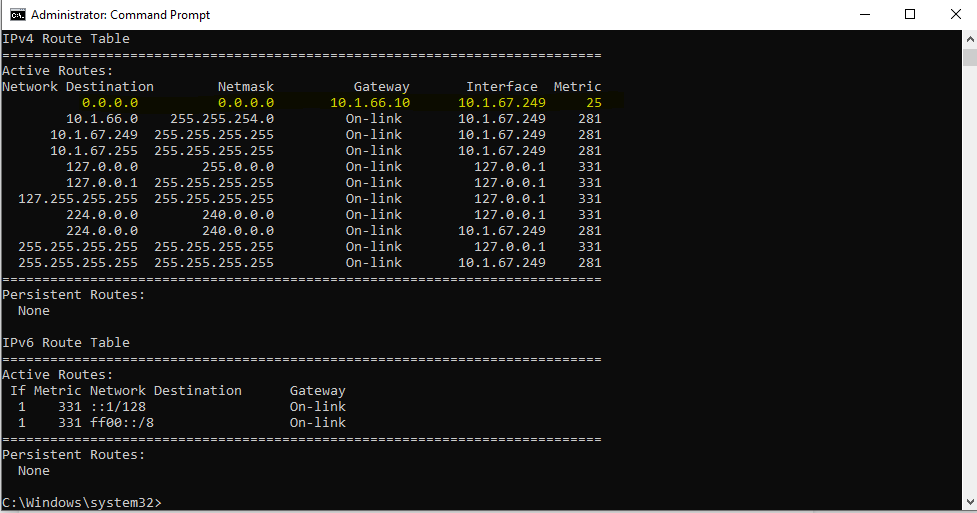
Wireshark Lab-ARP

# Step 1: Finding your IP address and Gateway address

1. Open a command prompt as an administrator as follows:
2. *Find the* ***Ethernet*** *address of the main network interface:*



1. *Find the IP address of the local router or default gateway that your computer uses to reach the rest of the Internet using the* netstat */* route *command.* You should be able to use the netstat -r command on Windows.



1. Now **run Wireshark** by typing “*wireshark*” in the bottom left search box in Windows
2. You should see the main Wireshark interface. **Click on the Ethernet OR Wireless interface** to start traffic analysis on that interface.
3. *Add a filter of* “arp”. Your capture window should be like the one pictured below.

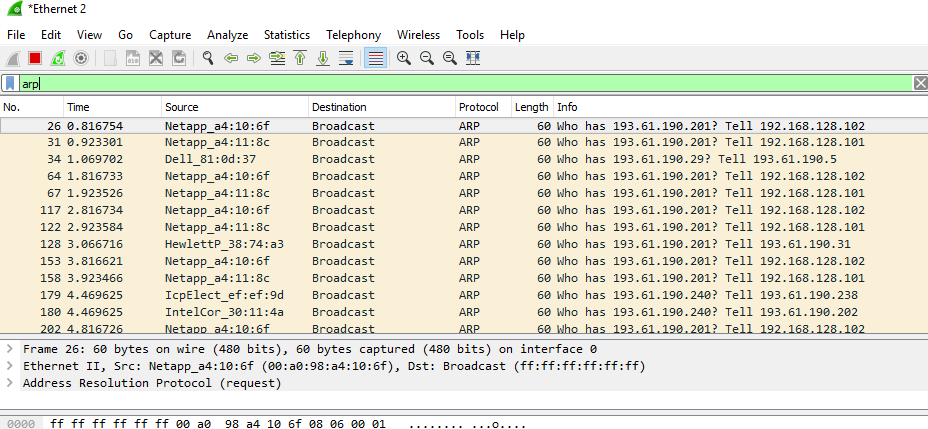
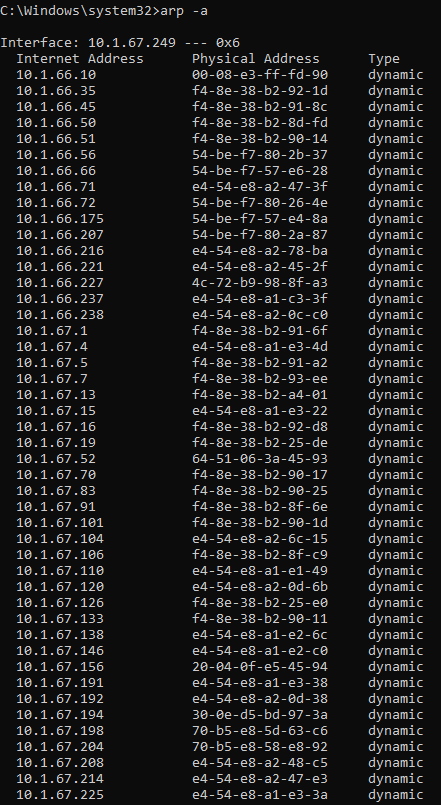


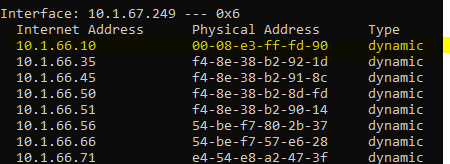
Figure 6: Setting up the capture options

1. *When the capture is started, use the “arp” command to clear the default gateway from the ARP cache.* Using the command “arp –a” will show you the contents of the ARP cache as a check that you can run “arp”.

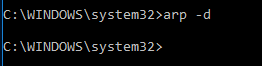
*Go to command prompt and type* **arp -a** as shown below.



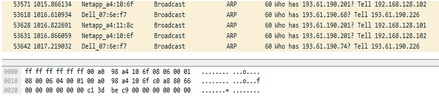
You should see an entry for the IP address of the default gateway as shown in image below. In this case it is 10 which is the default gateway on my office PC.



1. To clear this entry, use the arp command with different arguments (“arp –d” on Windows) as follows. Type **arp -d** in the command prompt.

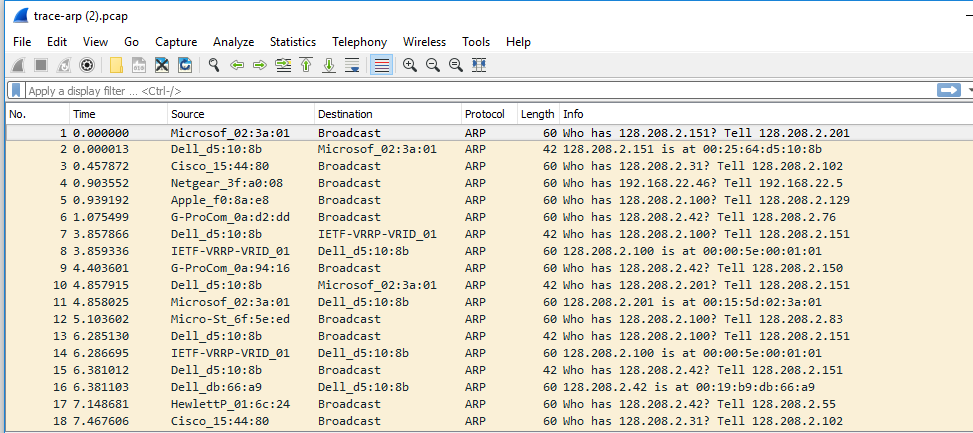


1. *Now that you have cleared your ARP cache,* ***fetch a remote page with your Web browser***. This will cause ARP to find the Ethernet address of the default gateway so that the packets can be sent.
2. You will see these packets flowing through your computer by scrolling down in the Wireshark window to the bottom as shown below.



# Step 2: Inspect the supplied ARP Trace

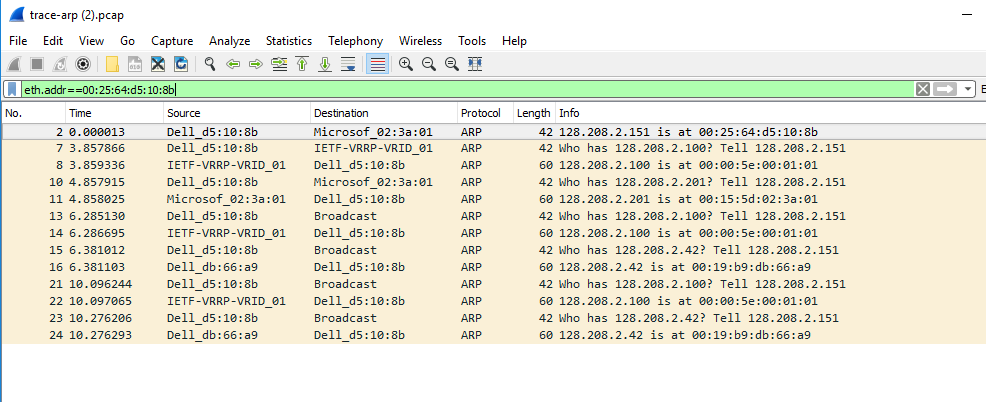
1. **Close** Wireshark.
2. Once Wireshark is closed, **open** the ARP trace here: You should see a screen as shown below.



1. Now we can look at an ARP exchange. Since there may be many ARP packets in your trace, we’ll first narrow our view to only the ARP packets that are sent directly from or to your computer.

*Set a display filter for packets with the Ethernet address of your computer which is this case is*

***00:25:64:d5:10:8***



# Step 3: Details of ARP over Ethernet

*(Please note that answers on next page to following 5 questions)*

*To look at further details of ARP, examine an ARP request and ARP reply to answer these questions:*

1. *What opcode is used to indicate a request? What about a reply?*

**opcode 1 indicates a request and opcode 2 indicates a reply.**

1. *What value is carried on a request for the unknown target MAC address?*

**Target MAC address: 00:00:00\_00:00:00 (00:00:00:00:00:00)**

1. *What Ethernet Type value which indicates that ARP is the higher layer protocol?*

**The Ethernet Type value for ARP is 0x806.**

1. *Is the ARP reply broadcast (like the ARP request) or not?*

**The ARP reply is normally not broadcast. It is sent directly to the target using its Ethernet address.**