PRIFYSGOL CYMRU
Y Drindod Dewi Sant
UNIVERSITY OF WALES
Trinity Saint David
SWANSEA - ABERTAWE

Applied Computing

Wales Institute of Science and Art (WISA)

Networks and Cybersecurity Essentials (ACCA4024)

Lab 2: Design a Simple Network with 2 PC's connected to a Switch.

Cisco | Networking Academy®
Mind Wide Open™

Warm-up

Based on your acquired skills from previous lab works, complete the following.

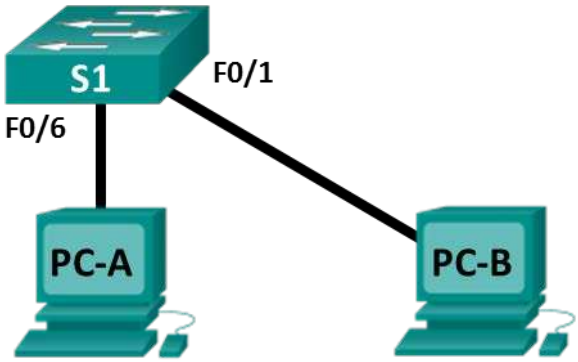
Build a Simple Network as per the topology given below

Configure the IP Address as per the addressing table

Use Ping Utility to check if the connection is successful.

(Save the file as Lab2_ Student_ID) and submit it via Moodle Link ONLY

Topology:



Addressing Table

Device	Interface	IP Address	Subnet Mask
PC-A	NIC	192.168.1.10	255.255.255.0
PC-B	NIC	192.168.1.11	255.255.255.0

Record your outcome: Is the Ping between PC- A and PC- B Successful?

Yes, I have had 4 successful pings

LAB Objectives

Every computer on an Ethernet local network has a Media Access Control (MAC) address that is burned into the Network Interface Card (NIC). Computer MAC addresses are usually displayed as 6 sets of two hexadecimal numbers separated by dashes or colons (example: 15-EF-A3-45-9B-57). The ipconfig /all command displays the computer MAC address.

1. Determine the MAC address of a Windows computer on an Ethernet network using the ipconfig /all command.
2. Analyze a MAC address to determine the manufacturer.
3. Analyze the Wired and Wireless Network connection.
4. Analyze Address Resolution Protocol (ARP).

Requirements

- PC running Windows 10 with at least one Ethernet network interface card (NIC) or the above created Topology in Packet Tracer.
- Connectivity to the Internet

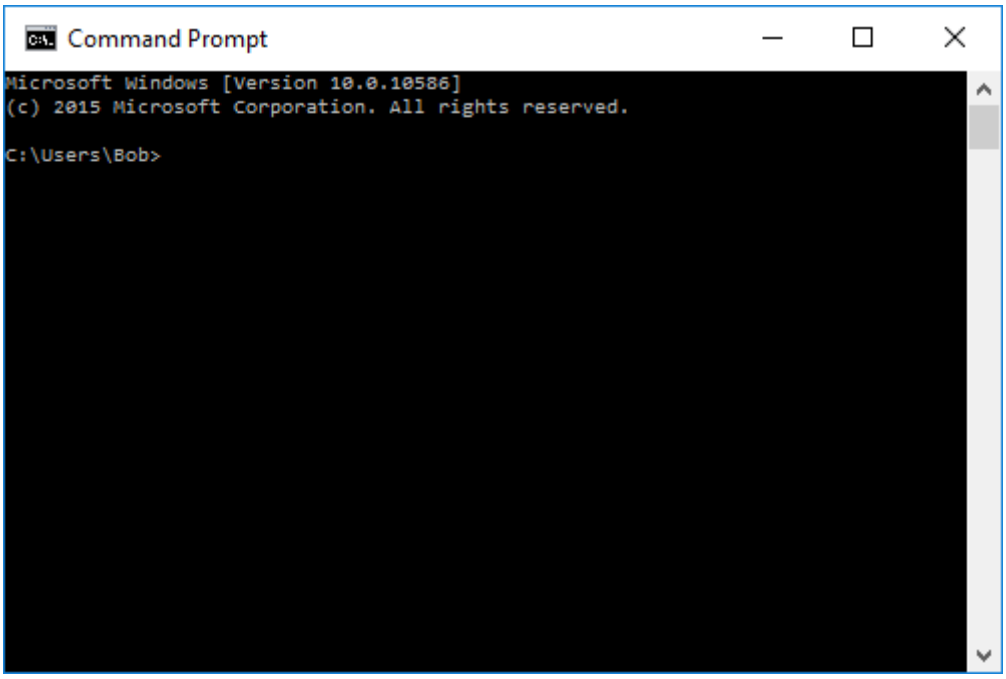
Task 1: Determine the MAC address of a Windows computer on an Ethernet network using the ipconfig /all command.

(From the previous lab, you should know the step-by-step procedure to execute a "PING"/ "TRACERT" command in a Packet Tracer) – Execute those steps, if you work with Packet Tracer.

In your PC

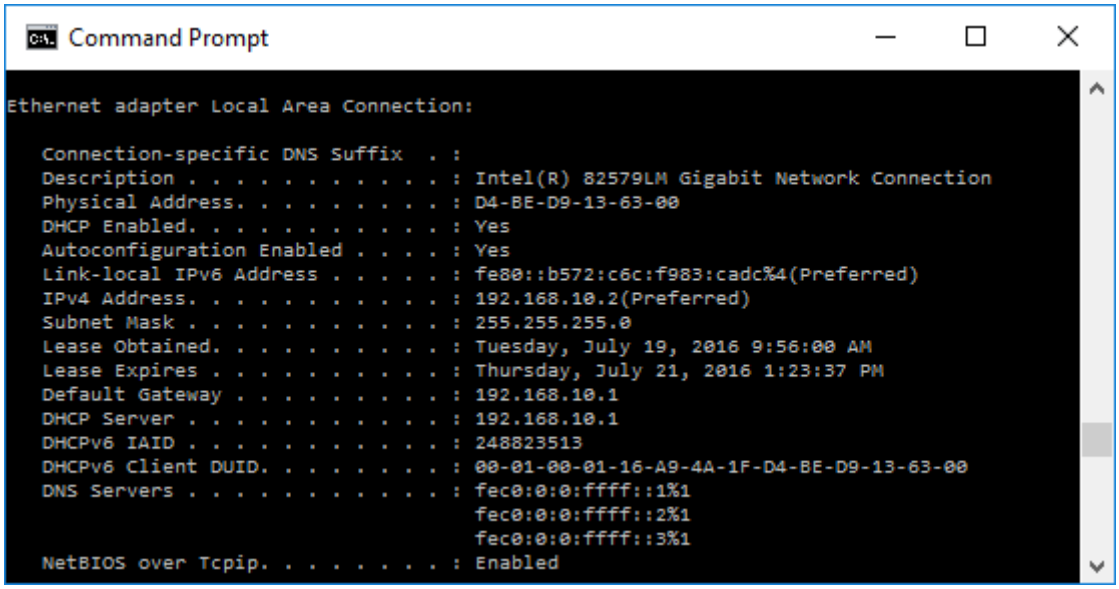
Step 1: Open a Windows command prompt window

Right-click on the **Start** button and select **Command Prompt**.



Step 2: Use the *ipconfig /all* command

Enter the **ipconfig /all** command at the command prompt. Press Enter. (Typical results are shown in the following figure, but your computer will display different information.)



Step 3: Locate the MAC (physical) address(es) in the output from the *ipconfig /all* command

Use the table below to fill in the description of the Ethernet adapter and the Physical (MAC) Address:

Description	Physical Address
Ethernet Adapter	04-92-26-58-DA-EA
Wireless LAN Adapter	64-5D-86-15-73-C7

How many MAC addresses did you discover in your PC? 5 - three of which are for Virtual Box

Task 2: Analyzing the Parts of a MAC Address

Every Ethernet network interface has a physical address assigned to it when it is manufactured. These addresses are 48 bit (6 bytes) long and are written in hexadecimal notation.

MAC addresses are made up of two parts.

One part of the MAC address, the first 3 bytes, represents the vendor who manufactured the network interface. This part of the MAC is called the OUI (Organizationally Unique Identifier). Each vendor who wants to make and sell Ethernet network interfaces must register with the IEEE in order to be assigned an OUI.

The second part of the address, the remaining 3 bytes are the unique ID for the interface. All MAC addresses that begin with the same OUI must have unique values in the last 3 bytes.

In the example shown in the lab, the physical MAC address for the Ethernet LAN interface is D4-BE-D9-13-63-00.

Manufacturer OUI	Unique Identifier for the Interface	Vendor Name
D4-BE-D9	13-63-00	Dell Incorporated

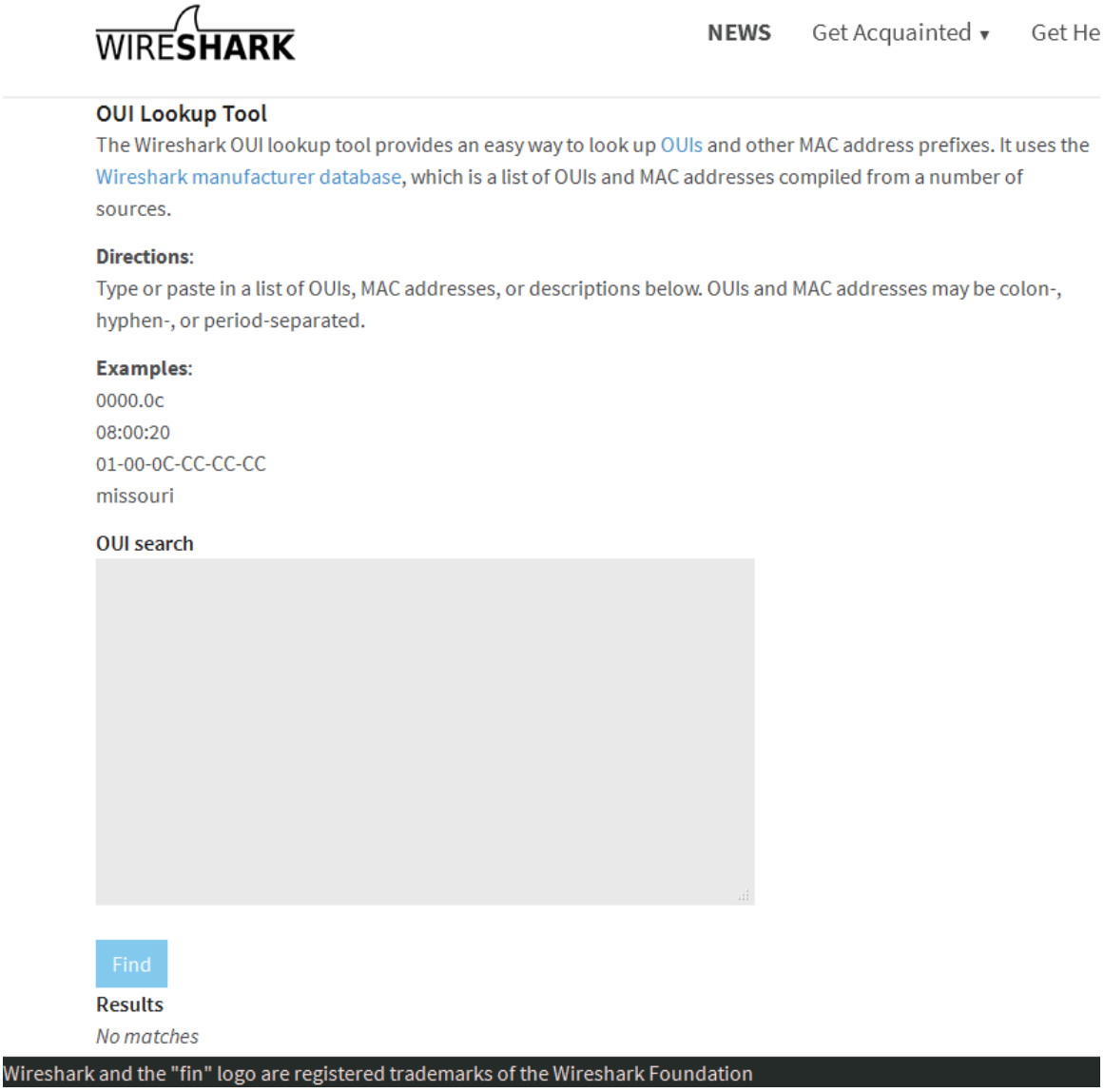
Step 4: List MAC addresses discovered by you in Part 1.

List the 3-byte Manufacturer OUI and the 3-byte unique interface identifier. You will fill in the Vendor name in Step 2.

Manufacturer OUI	Unique Identifier for the Interface	Vendor Name
D4-BE-D9	13-63-00	Dell Incorporated
04-92-26	58-DA-EA	ASUSTek Computing INC
64-5D-86	15-73-C7	Intel Corporate

Step 5: Lookup the vendors who are the registered owners of the OUI that you listed in the table.

a. Wireshark.org provides an easy to use lookup tool at https://www.wireshark.org/tools/oui-lookup.html. Use this tool, or use the Internet to search for other ways to identify an OUI.



b. Use the information that you found to update the vendor column in the chart in Step 1. How many different vendors did you discover? 2

I have discovered that my Ethernet has an ASUS vendor whilst my Wi-fi is registered as the from the Intel Vendor

Record your Reflection

1. Why might a computer have more than one MAC address?

   A computer might have more than one MAC address depending on the available connections e.g. (ethernet or Wi-fi) it might also show additional MAC addresses if Virtual Machines are used on the device as they create their own versions of the ethernet and Wi-fi Adapters

2. Try connecting and disconnecting the network cable(s) to your network adapter(s) and use the **ipconfig /all** again. What changes do you see? Does the MAC address still display? Will the MAC address ever change?

   The MAC address does not change when disconnected as it is the addess assigned to the NIC. It is possible to override this to change the MAC address but this is often only done during hacking. Another way to change the MAC address is to change the component as the MAC address is based on the NIC component

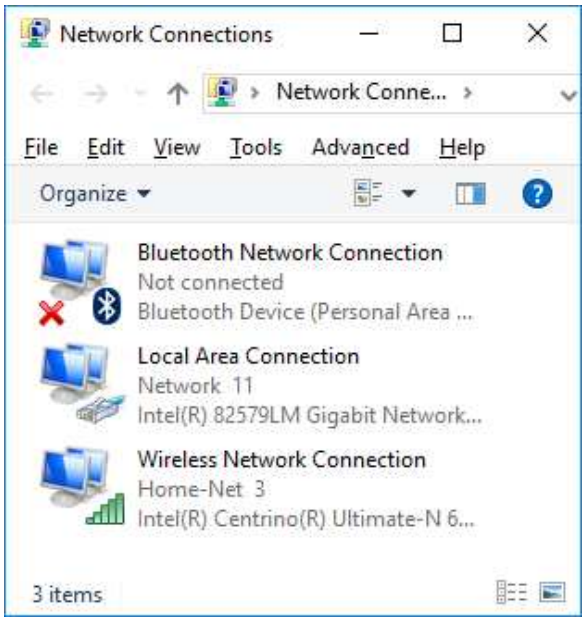
3. What are other names for the MAC address?

   The other name for a MAC address is the Physical Address

Task 3: Wired and Wireless Network Connection.

Step 6: Open the Network Connections window by right-clicking the Windows Start button > Network Connections.

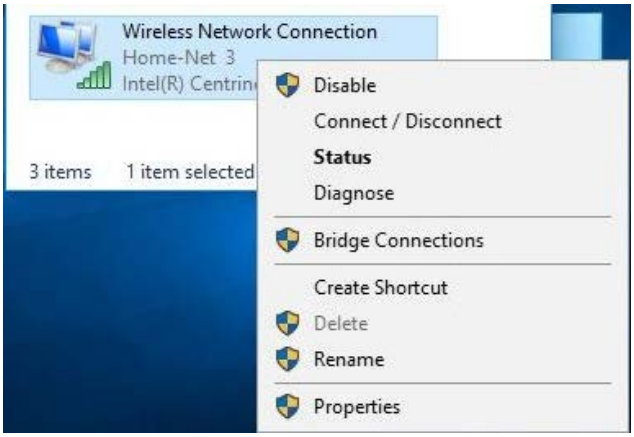
Step 7: The Network Connections window displays the list of NICs available on this PC. Look for your Local Area Connection and Wireless Network Connection adapters in this window.



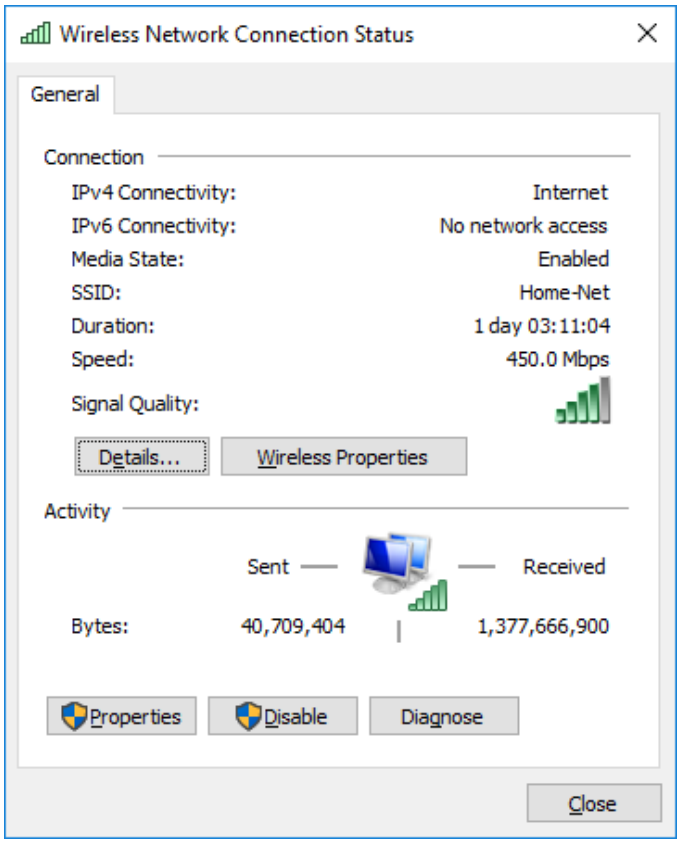
Note: Other types of network adapters, such as Bluetooth Network connection and Virtual Private Network (VPN) adapter, may also be displayed in this window.

Verify the wireless network connection settings

Step 8: Select the Wireless Network Connection option. Right-click on it to display a drop-down list. The first option displays if your wireless NIC is enabled or disabled. Currently, this NIC is enabled which is why the Disable option is displayed. If your wireless NIC is disabled, you will have an option to Enable it.



Step 9: Click Status to open the Wireless Network Connection Status window.



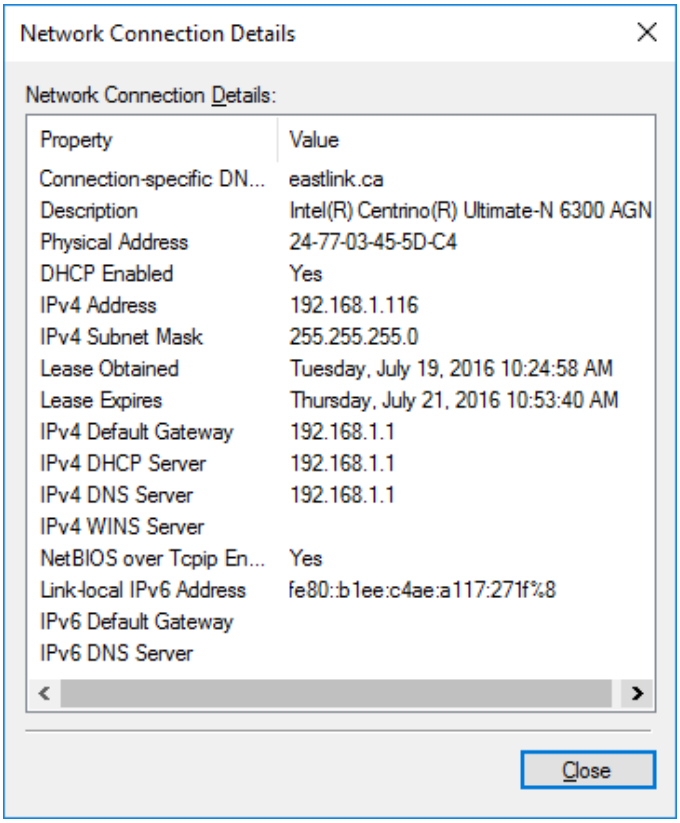
What is the Service Set Identifier (SSID) for the wireless router of your connection?

This is the Name of the Broadband, in my case it is VM6285099

What is the speed of your wireless connection?

The speed is 72.2Mbps

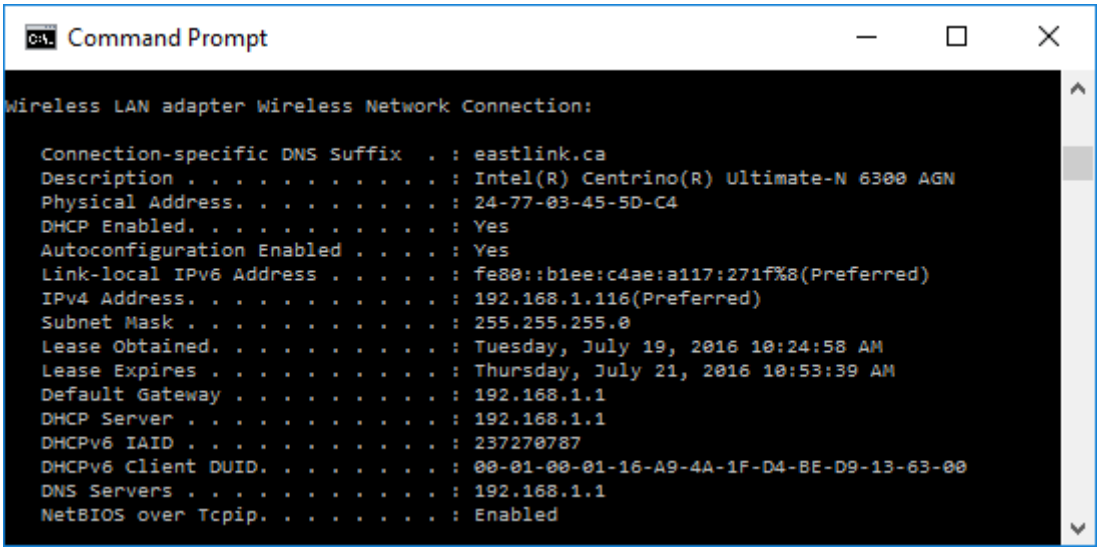
Step 10: Click Details to display the Network Connection Details window.



What is the MAC address of your wireless NIC?
64-5D-86-15-73-C7

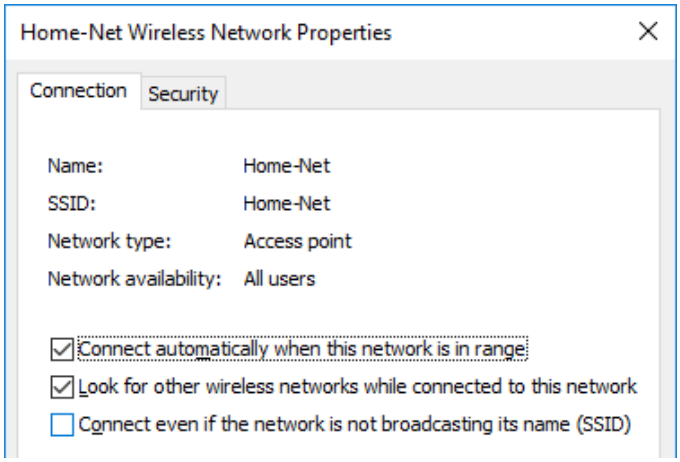
Step 11: Open a command window prompt and type ipconfig /all.

```
C:\Users\Bob> ipconfig /all
```

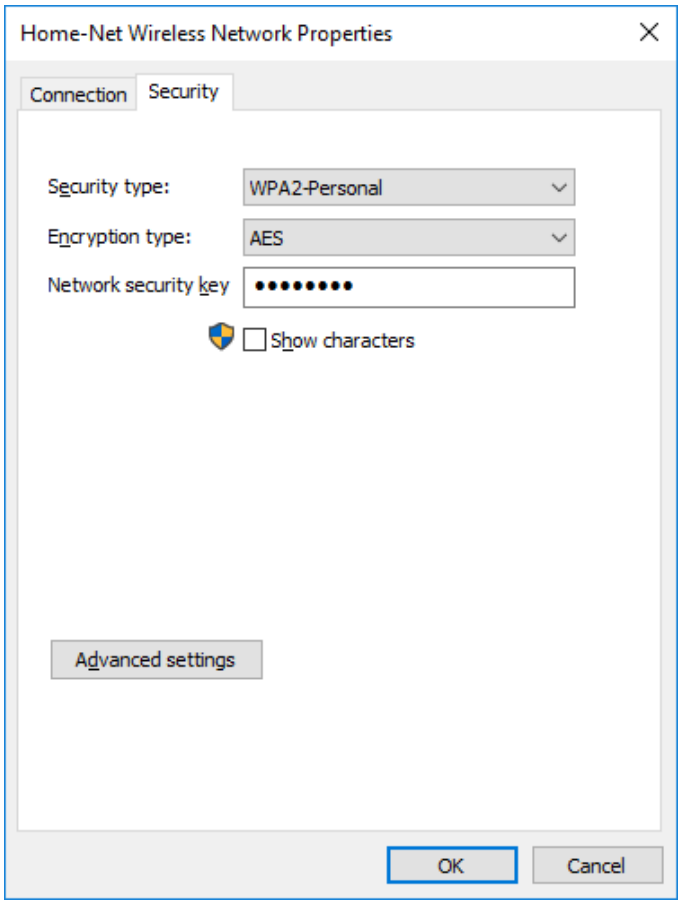


Notice the information displayed is similar to the Network Connection Details window information. When you have reviewed the details, click **Close** to return to the Wireless Network Connection Status window.

Step 12: Return to the Wireless Network Connection Status window. Click Wireless Properties to open the Wireless Network Properties window of the Home-Net network.



Step 13: You should always use wireless security whenever available. To verify (or configure) the wireless security options click on the Security tab.



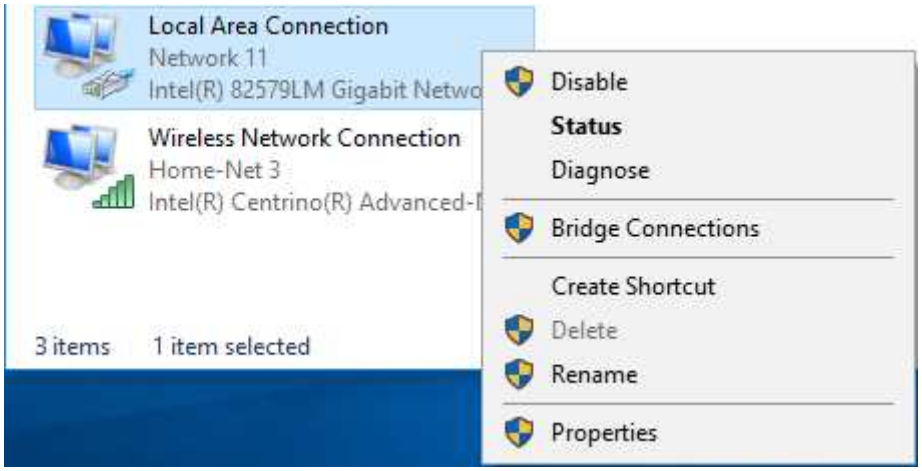
The window displays the type of security and encryption method enabled. You can also enter (or change) the security key in this window. Close all windows.

Work with your wired NIC.

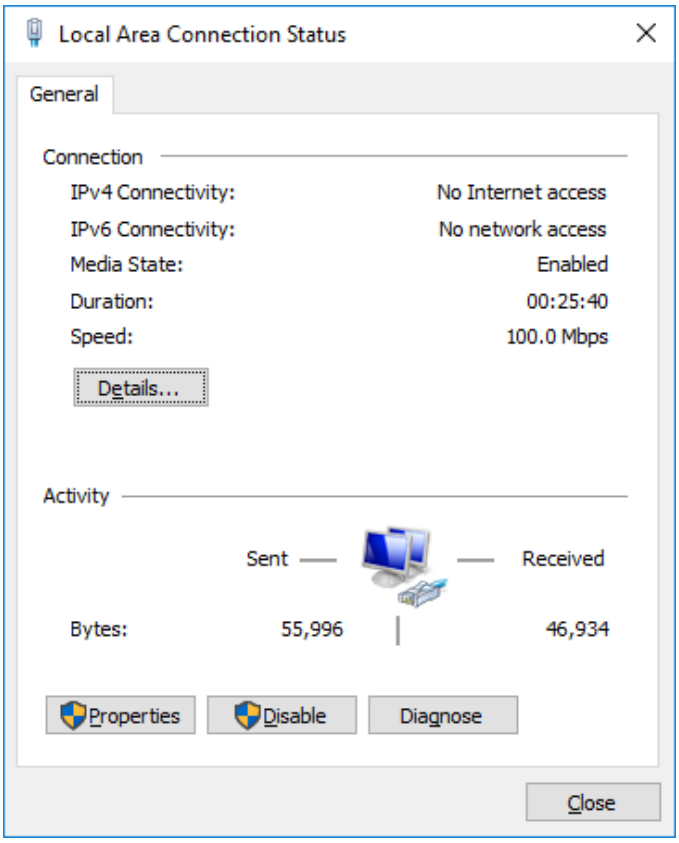
We will now verify the wired network connection settings.

Step 14: Open the Network Connections window by right-clicking Windows Start > Network Connections.

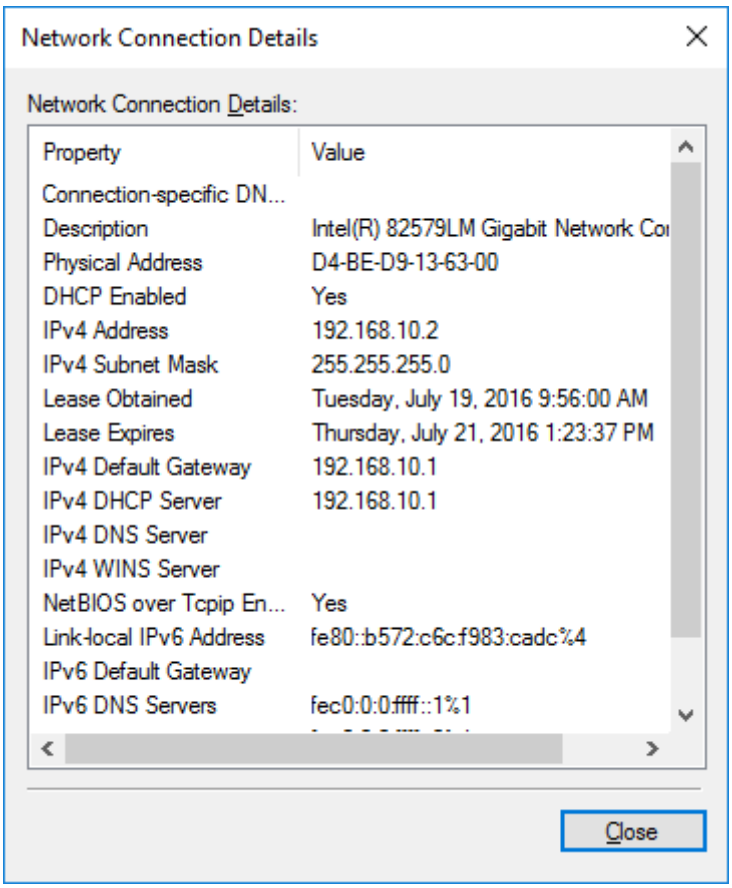
Step 15: Select and right-click the Local Area Connection option to display the drop-down list. If the NIC is disabled, enable it.



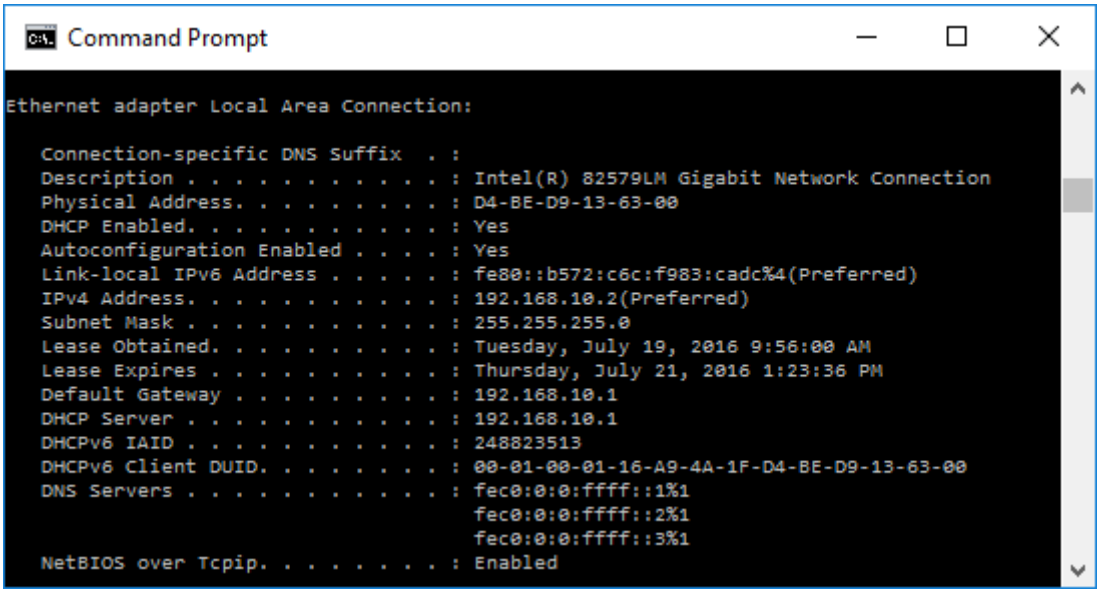
Step 16: Click the Status option to open the Local Area Connection Status window. This window displays information about your wired connection to the LAN.



Step 17: Click Details… to view the address information for your LAN connection.



Step 18: Open a command window prompt and type ipconfig /all. Find your Local Area Connection information and compare this with the information displayed in the Network Connection Details window.

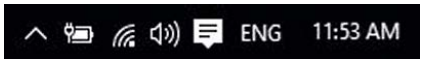


Step 19: Close all windows on your desktop.

Identify and Use the System Tray Network Icons

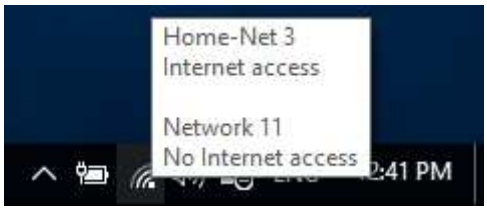
Use the Wireless Network icon.

Step 20: The bottom right-hand corner of the Windows 10 screen contains the system tray. Move your mouse to display the system tray as shown.

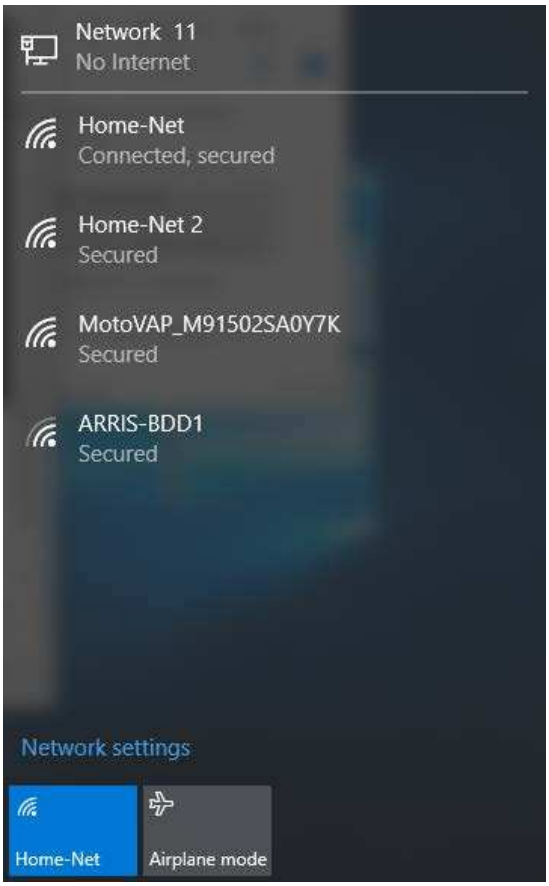


Note: If your wired network is enabled, a different network icon ( ) is displayed in the system tray.

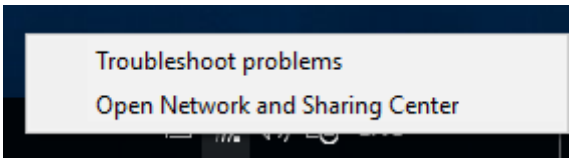
Step 21: In this example, the 3rd icon from the left is the wireless network icon. If you hover over it, it displays the currently connected networks.



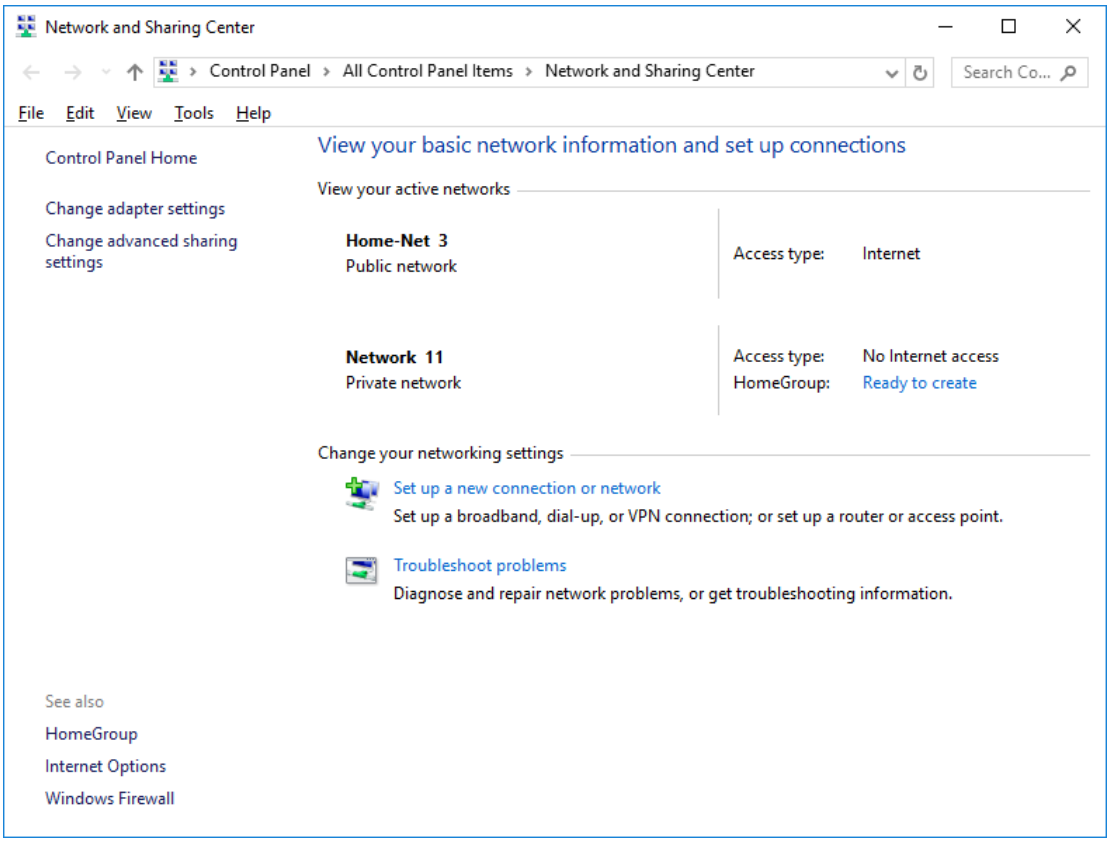
Step 22: Click the wireless network icon, and it displays the wired and wireless network SSIDs that are in range of your wireless NIC.



Step 23: Right-click the wireless network icon, and it displays a troubleshooting option and to open the Network and Sharing Center window.



Step 24: Click on the Open Network and Sharing Center option.



Step 25: The Network and Sharing Center is a central window that displays information about the active network or networks, the network type, the type of access.

Record your Reflection

Why would you activate more than one NIC on a PC?

This could be used as a fail over from wired to wireless or vice versa although this is dependant on the connections of the device

Task 4: Address Resolution Protocol (ARP).

Use your PC/ Laptop with Internet Connection to execute this Task.

Objectives

Download and Install Wireshark

Capture and Analyze ARP Data in Wireshark

- Start and stop data capture of ping traffic to remote hosts.
- Locate the IPv4 and MAC address information in captured PDUs.
- Analyze the content of the ARP messages exchanged between devices on the LAN.

View the ARP cache entries on the PC

- Access the Windows Command Prompt.
- Use the Windows **arp** command to view the local ARP table cache on the PC.

Background / Scenario

Address Resolution Protocol (ARP) is used by TCP/IP to map a Layer 3 IPv4 address to a Layer 2 MAC address. When an Ethernet frame is transmitted on the network, it must have a destination MAC address. To dynamically discover the MAC address of a known destination, the source device broadcasts an ARP request on the local network. The device that is configured with the destination IPv4 address responds to the request with an ARP reply and the MAC address is recorded in the ARP cache.

Every device on the LAN maintains its own ARP cache. The ARP cache is a small area in RAM that holds the ARP responses. Viewing an ARP cache on a PC displays the IPv4 address and the MAC address of each device on the LAN with which the PC has exchanged ARP messages.

Wireshark is a software protocol analyzer, or "packet sniffer" application, used for network troubleshooting, analysis, software and protocol development, and education. As data streams travel back and forth over the network, the sniffer "captures" each protocol data unit (PDU) and can decode and analyze its content according to the appropriate protocol specifications.

Wireshark is a useful tool for anyone working with networks and can be used with most labs in the Cisco courses for data analysis and troubleshooting. This lab provides instructions for downloading and installing Wireshark, although it may already be installed. In this lab, you will use Wireshark to capture ARP exchanges on the local network.

Required Resources

- 1 Windows 10 PC with Internet access

Download and Install Wireshark

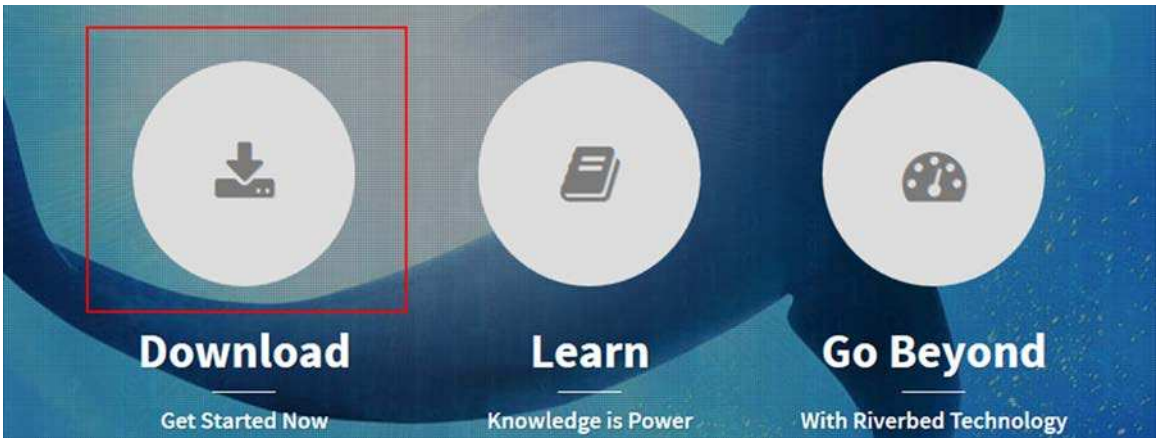
Wireshark has become the industry standard packet-sniffer program used by network engineers. This open source software is available for many different operating systems, including Windows, Mac, and Linux.

If Wireshark is already installed on your PC, you can skip Part 1 and go directly to Part 2. If Wireshark is not installed on your PC, check with your instructor about your academy's software download policy.

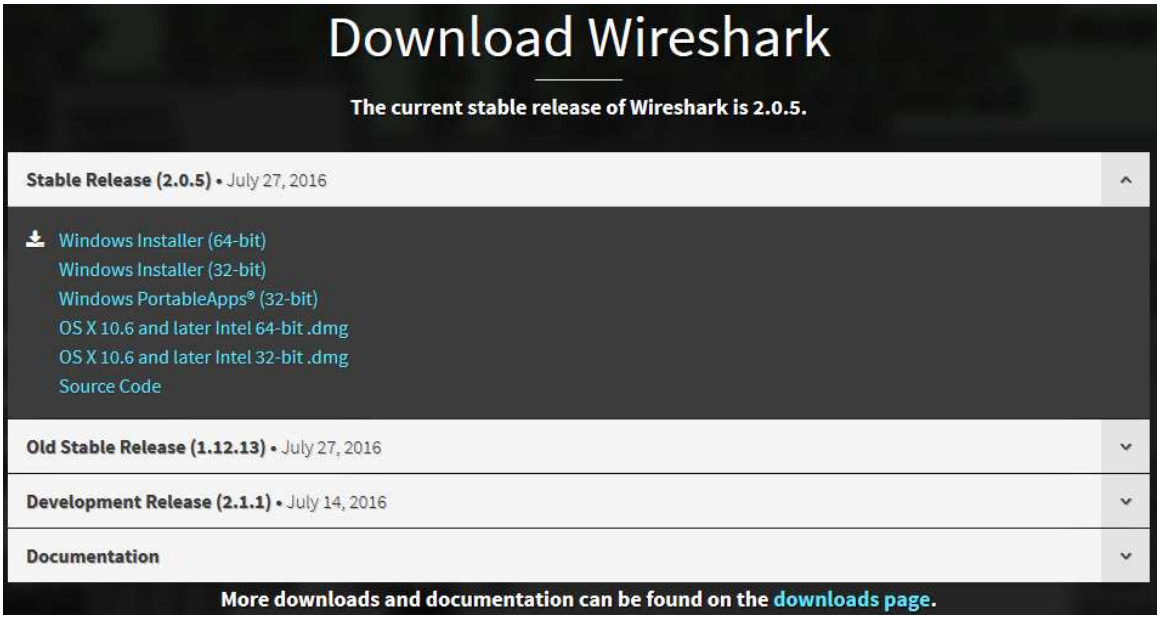
Step 26: Download Wireshark.

a. Wireshark can be downloaded from www.wireshark.org.

b. Click **Download**.



c. Choose the software version you need based on your PC's architecture and operating system. For instance, if you have a 64-bit PC running Windows, choose **Windows Installer (64-bit)**.



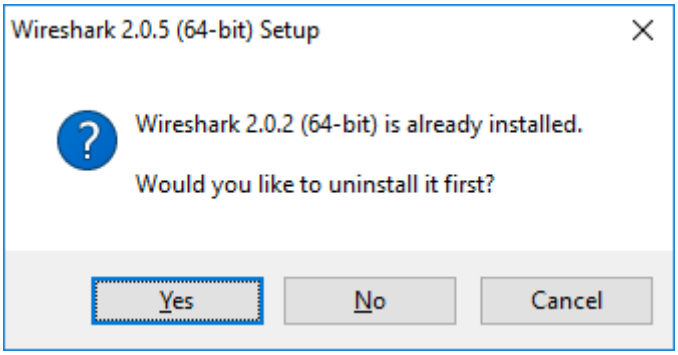
d. After making a selection, the download should start. Click **Save File** if prompted. The location of the downloaded file depends on the browser and operating

system that you use. For Windows users, the default location is the **Downloads** folder.

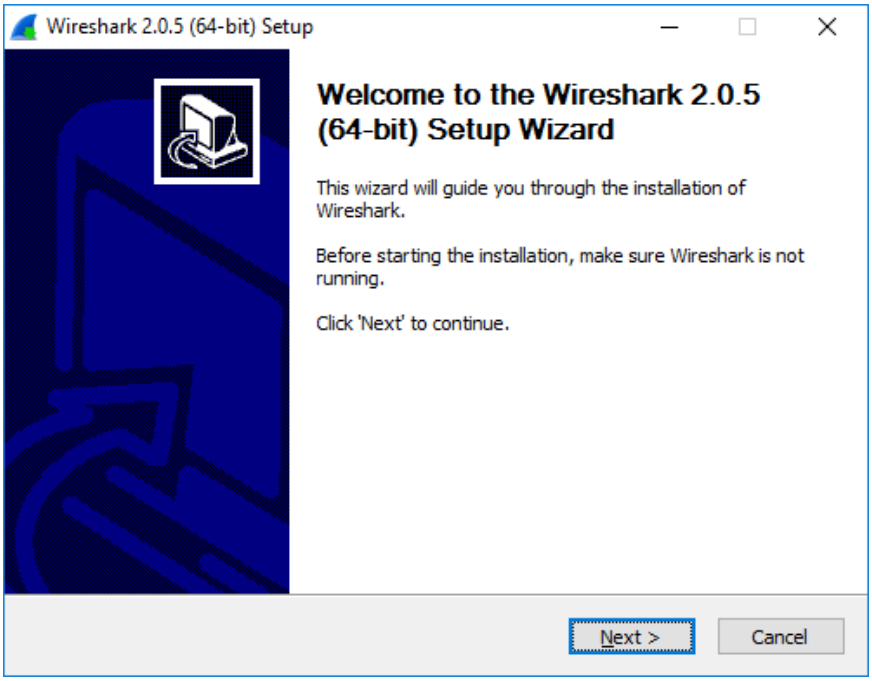
Step 27: Install Wireshark.

e. The downloaded file is named **Wireshark-win64-x.x.x.exe**, where **x** represents the version number. Double-click the file to start the installation process. It is version 2.0.5 in this example.

f. Respond to any security messages that may display on your screen. If you already have a copy of Wireshark on your PC, you will be prompted to uninstall the old version before installing the new version. It is recommended that you remove the old version of Wireshark prior to installing another version. Click **Yes** to uninstall the previous version of Wireshark.



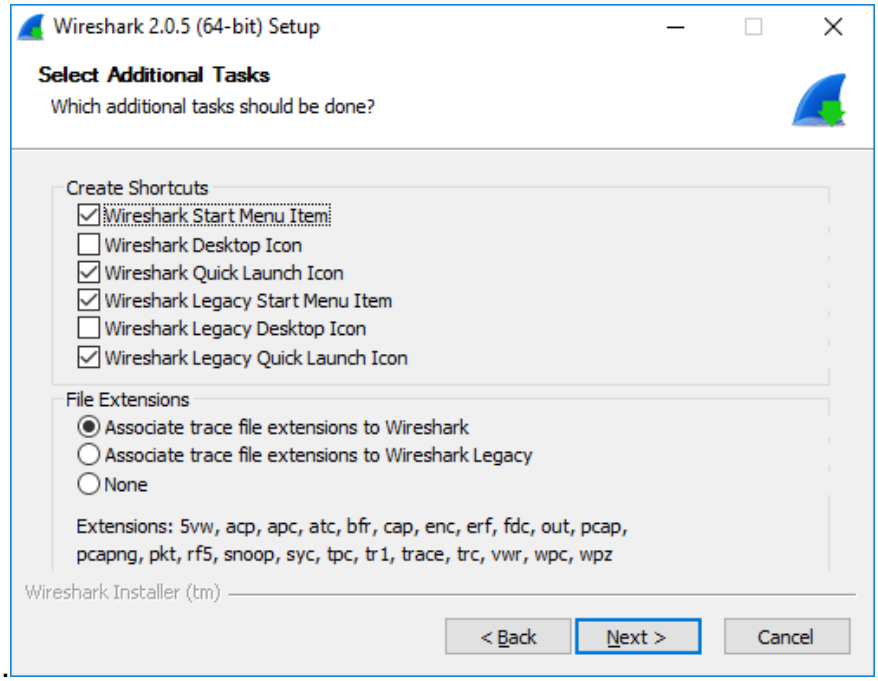
g. If this is the first time to install Wireshark, or after you have completed the uninstall process, you will navigate to the Wireshark Setup wizard. Click **Next**.



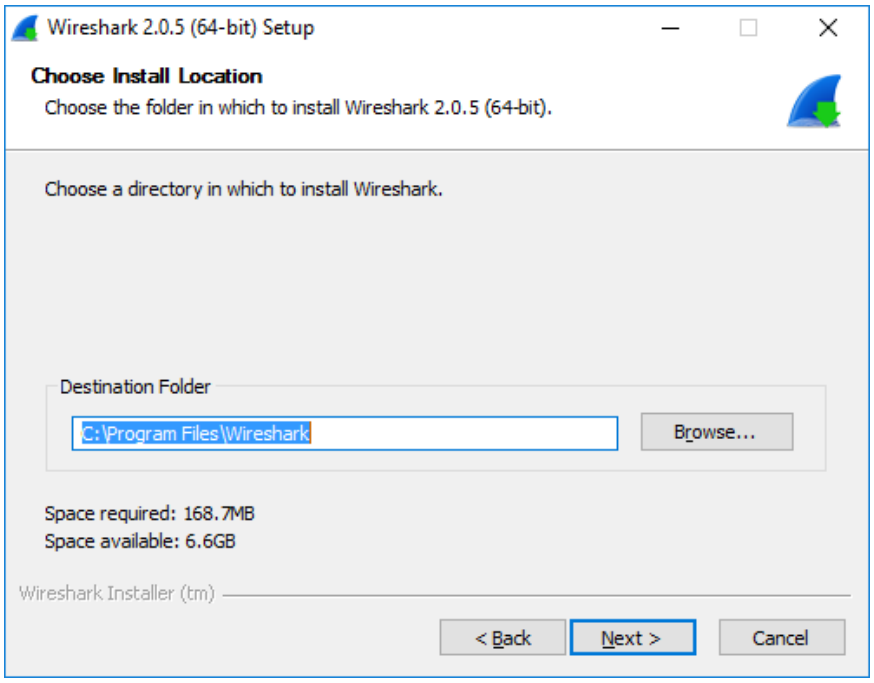
h. Continue advancing through the installation process. Click **I Agree** when the License Agreement window displays.

i. Keep the default settings on the Choose Components window and click **Next**.

j. Choose your desired shortcut options and click **Next**.

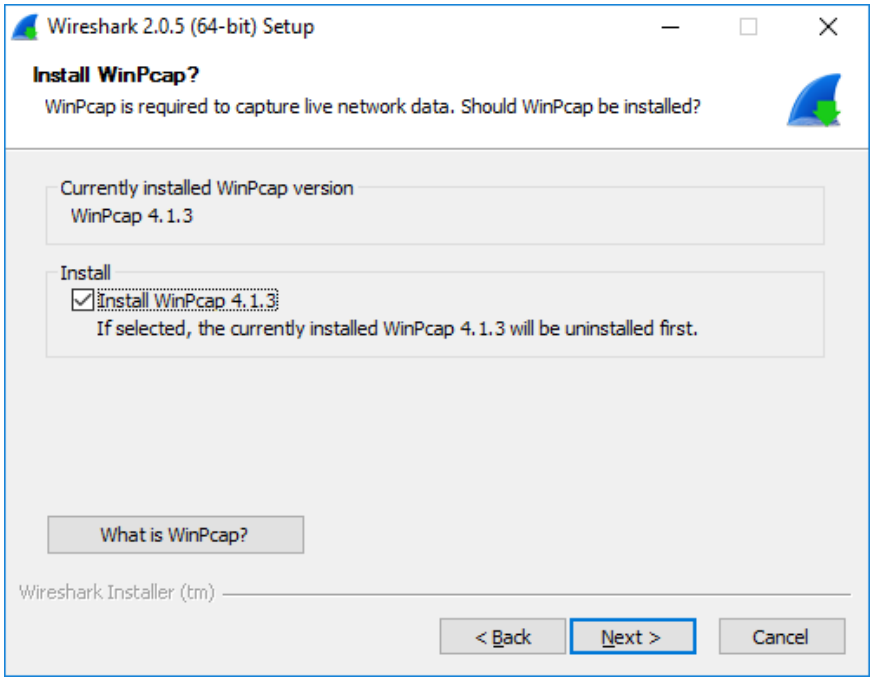


k. You can change the installation location of Wireshark, but unless you have limited disk space, it is recommended that you keep the default location.



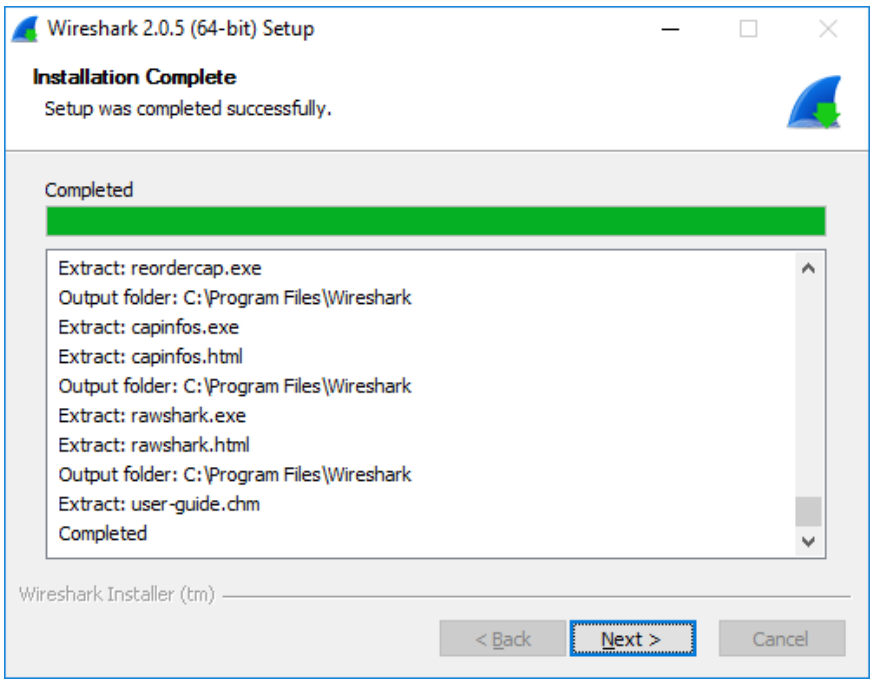
l. To capture live network data, WinPcap must be installed on your PC. If WinPcap is already installed on your PC, the Install check box will be unchecked. If your installed version of WinPcap is older than the version that comes with Wireshark, it is recommend that you allow the newer version to be installed by clicking the **Install WinPcap x.x.x** (version number) check box.

Finish the WinPcap Setup Wizard if installing WinPcap.

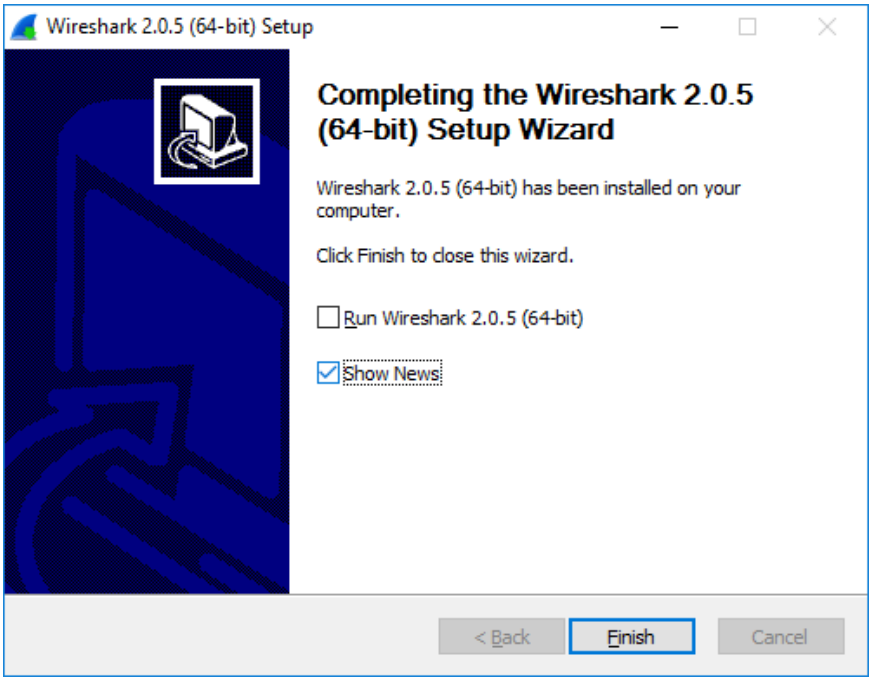


Note: You maybe prompted to install USBPcap. The installation of USBPcap is optional.

m. Wireshark starts installing its files and a separate window displays with the status of the installation. Click **Next** when the installation is complete.



n. Click **Finish** to complete the Wireshark install process.



Capture and Analyze Local ARP Data in Wireshark

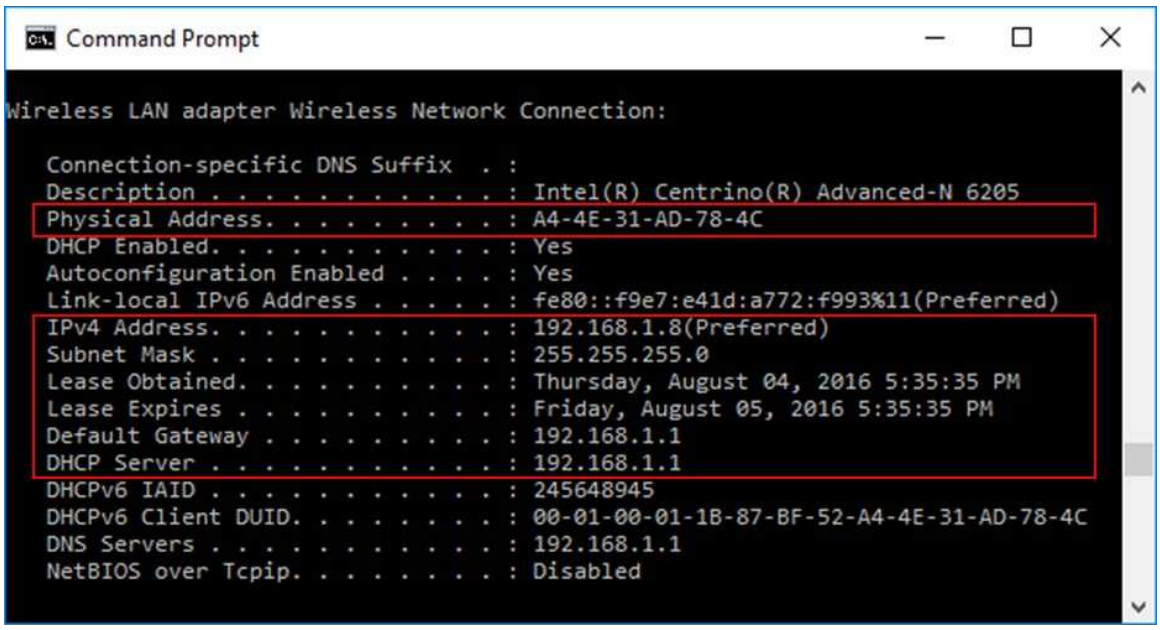
You will ping another PC on the LAN and capture ARP requests and replies in Wireshark. You will also look inside the frames captured for specific information. This analysis should help to clarify how packet headers are used to transport data to their destination.

Step 28: Retrieve your PC's interface addresses.

For this lab, you will need to retrieve your PC's IPv4 address and the MAC address.

o. Open a command window, type **ipconfig /all**, and then press Enter.

p. Note which network adapter that the PC is using to access the network. Record your PC interface's IPv4 address and MAC address (Physical Address).



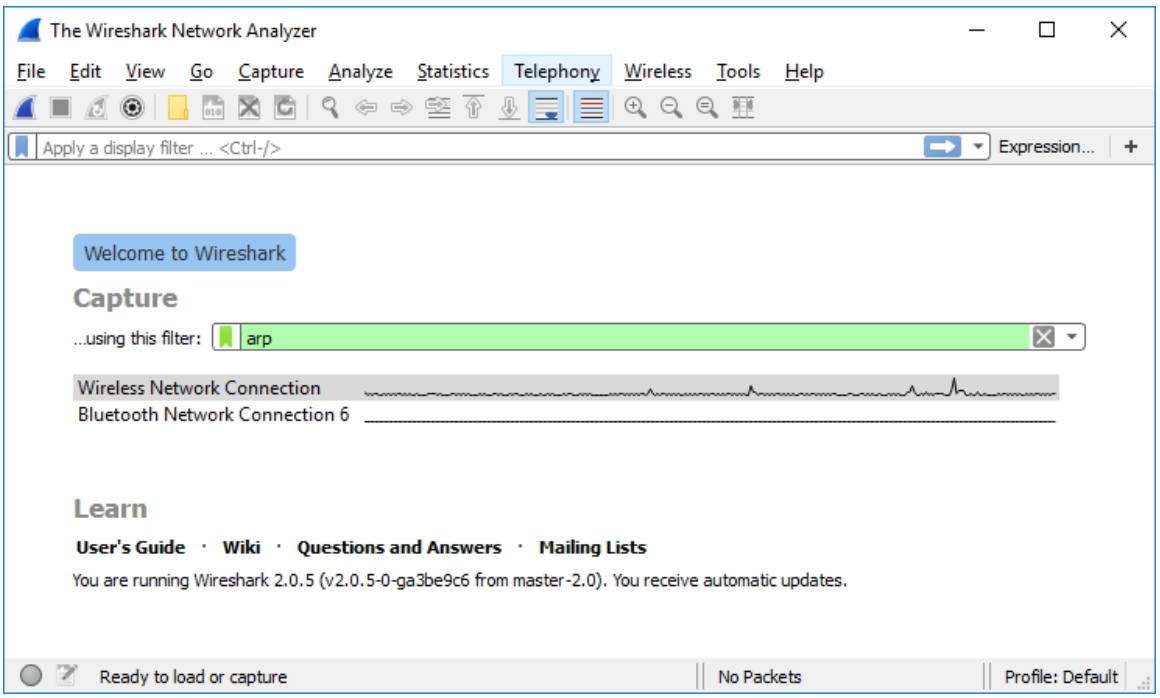
Step 29: Start Wireshark and begin capturing data.

q. On your PC, click **Start** and type **Wireshark**. Click **Wireshark Desktop App** when it appears in the search results window.

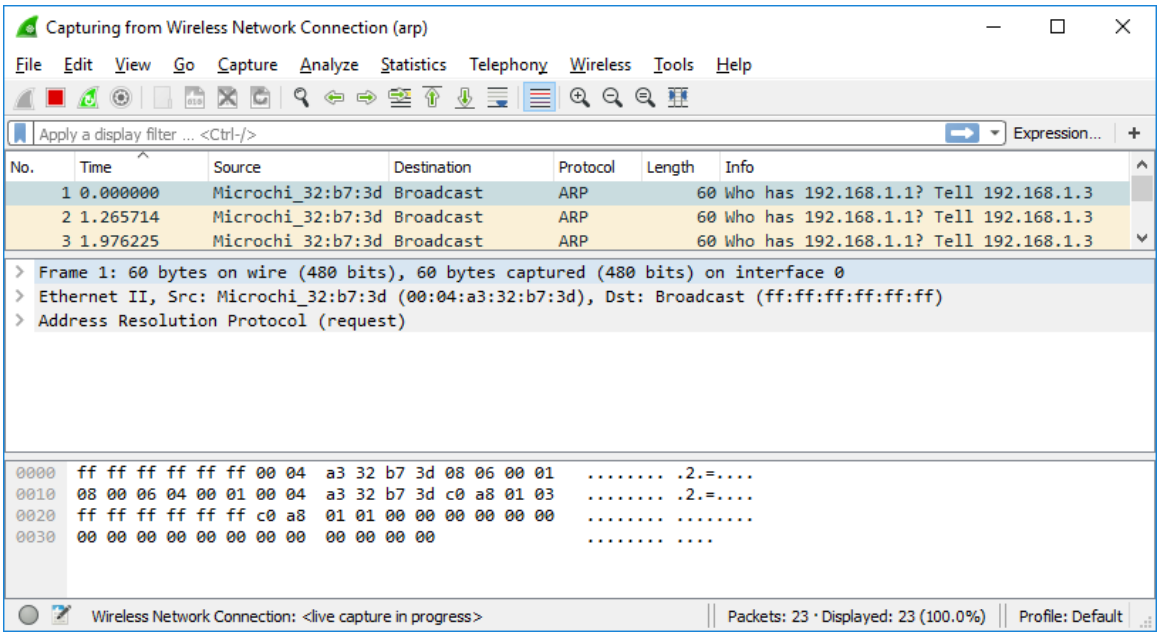
   Note: Alternatively, your installation of Wireshark may also provide a Wireshark Legacy option. This displays Wireshark in the older but widely recognized GUI. The remainder of this lab was completed using the newer Desktop App GUI.

r. After Wireshark starts, select the network interface that you identified with the **ipconfig** command. Enter **arp** in the filter box. This selection configures

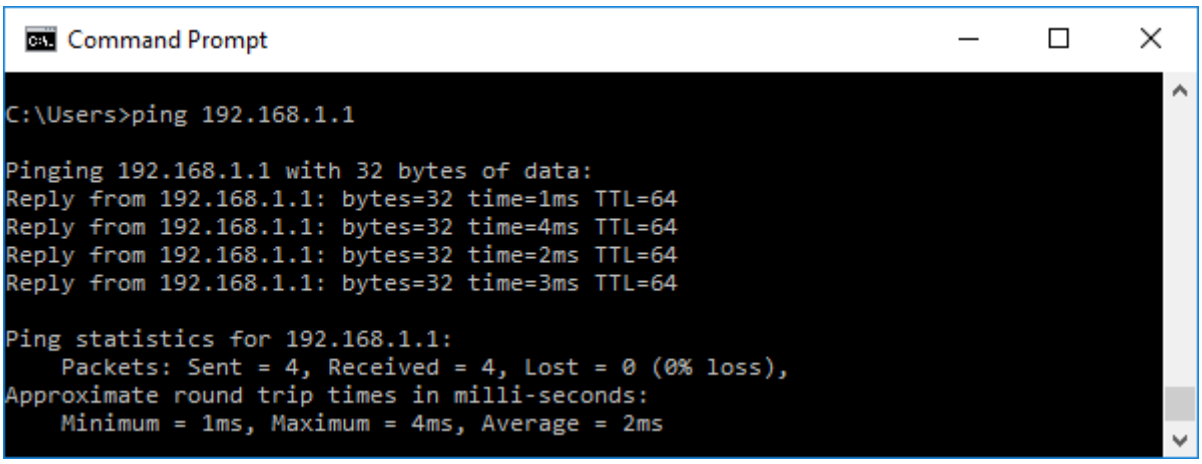
Wireshark to only display packets that are part of the ARP exchanges between the devices on the local network.



s. After you have selected the correct interface and entered the filter information, click **Start** ( ) to begin the data capture. Information will start scrolling down the top section in Wireshark. Each line represents a message being sent between a source and destination device on the network.



t. Open a command prompt window. Use the **ping** command to test connectivity to the default gateway address that you identified in Part 2, step 1c.

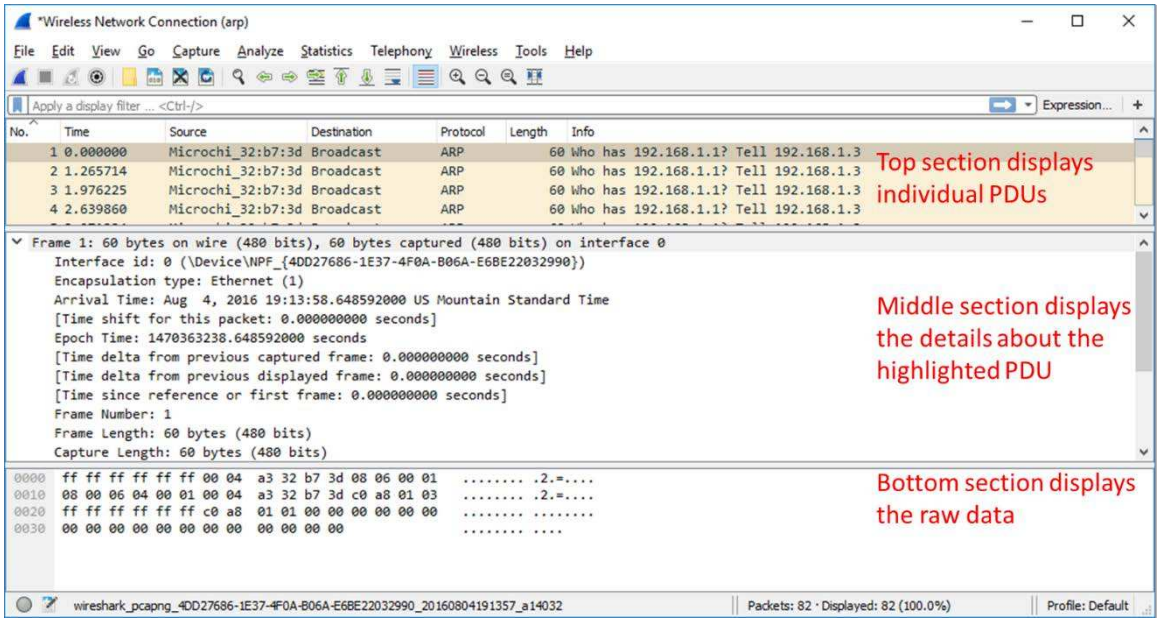


u. Stop capturing data by clicking **Stop Capture (** **)** on the toolbar.

Step 30: Examine the captured data.

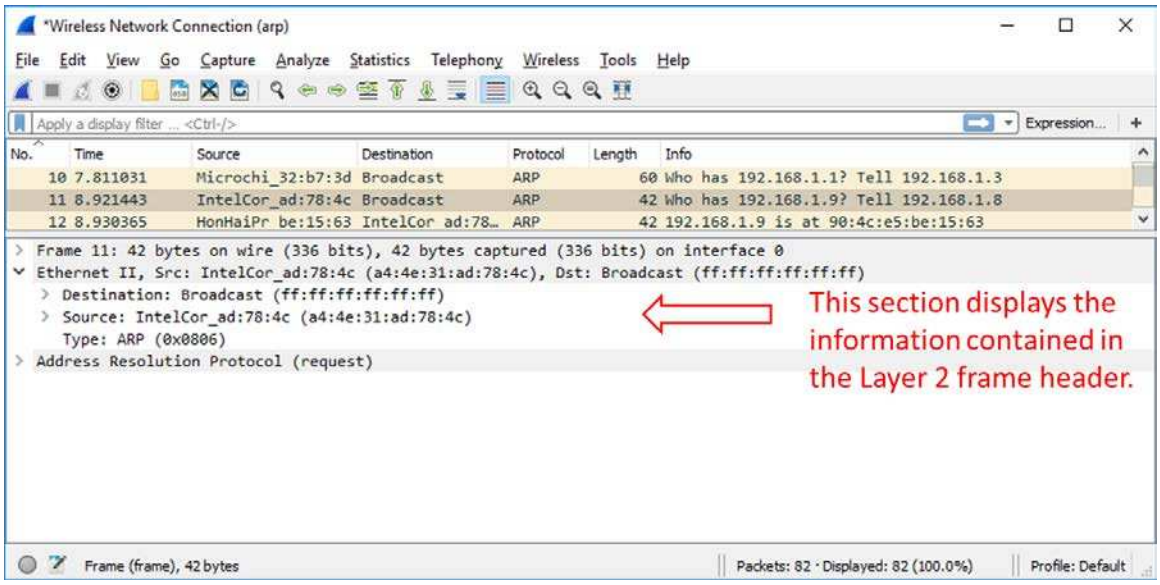
In Step 3, examine the data that was generated by the **ping** requests, Wireshark data is displayed in three sections:

1) The top section displays the list of PDU frames captured with a summary of the IPv4 packet information listed.
2) The middle section lists PDU information for the frame selected in the top part of the screen and separates a captured PDU frame by its protocol layers.
3) The bottom section displays the raw data of each layer. The raw data is displayed in both hexadecimal and decimal form.



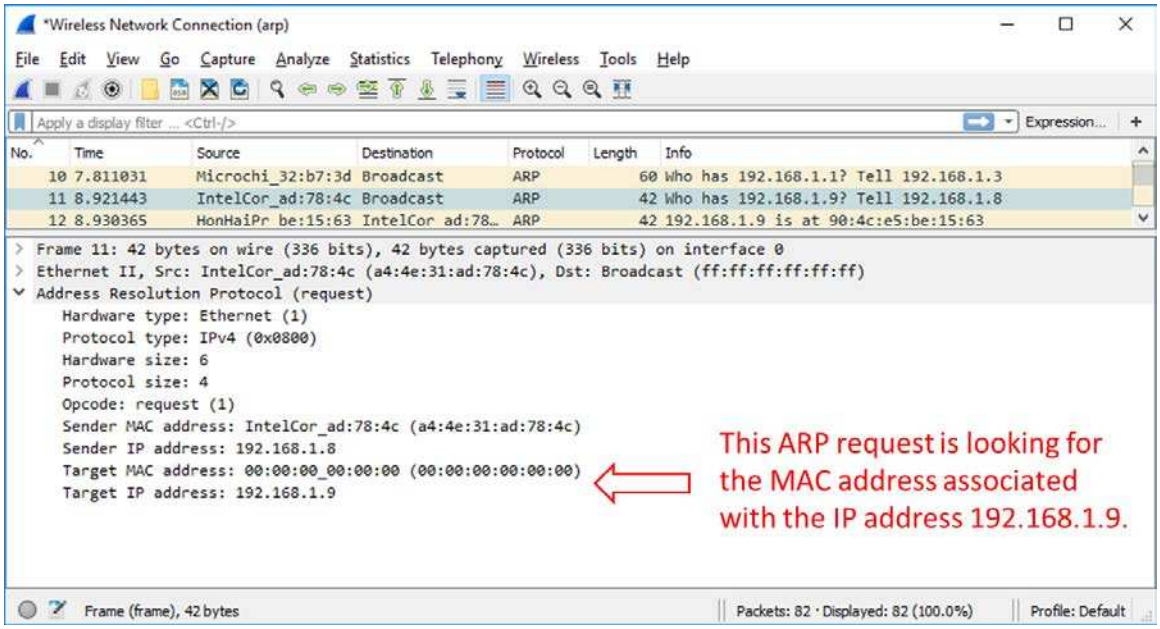
a. Click one of the ARP frames in the top section that has your PC MAC address as the source address in the frame and “broadcast” as the destination of the frame.

b. With this PDU frame still selected in the top section, navigate to the middle section. Click the arrow to the left of the Ethernet II row to view the Destination and Source MAC addresses.



Does the Source MAC address match your PC’s interface?
No, the source MAC address is shown as 18:35:d1:4f:04:30 which is different to the one assigned to my devices NIC

c. Click the arrow to the left of the Address Resolution Protocol (request) row to view the content of the ARP request.



Step 31: View ARP cache entries on a Windows PC.

a. Open a command prompt window on the PC. At the prompt, enter **arp –a** and press enter.

```
Command Prompt

C:\>arp -a

Interface: 192.168.1.8 --- 0xb
  Internet Address      Physical Address      Type
  192.168.1.1           80-37-73-ea-b1-7a     dynamic
  192.168.1.9           90-4c-e5-be-15-63     dynamic
  192.168.1.13          a4-4e-31-ad-78-4c     dynamic
  224.0.0.5             01-00-5e-00-00-05     static
  224.0.0.6             01-00-5e-00-00-06     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.252           01-00-5e-00-00-fc     static
  224.0.0.253           01-00-5e-00-00-fd     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

C:\>
```

The output of the **arp –a** command displays the entries that are in the cache on the PC. In the example, the PC has entries for the default gateway (192.168.1.1) and for two PCs that are located on the same LAN (192.168.1.9 and 192.168.1.13).

What is the result of executing the **arp –a** command on your PC?

it shows the IP and the Internet Address, Physical Address and the Type (Dynamic/Static)

I can see the default gateway as well as two other dynamic devices which I suspect are laptops

b. The **arp** command on the Windows PC has another functionality. Enter **arp /?** at the command prompt and press enter. The **arp** command options enable you to view, add and remove ARP table entries if necessary.

```
Command Prompt

C:\>arp /?

Displays and modifies the IP-to-Physical address translation tables used by
address resolution protocol (ARP).

ARP -s inet_addr eth_addr [if_addr]
ARP -d inet_addr [if_addr]
ARP -a [inet_addr] [-N if_addr] [-v]

  -a            Displays current ARP entries by interrogating the current
                protocol data.  If inet_addr is specified, the IP and Physical
                addresses for only the specified computer are displayed.  If
                more than one network interface uses ARP, entries for each ARP
                table are displayed.
  -g            Same as -a.
  -v            Displays current ARP entries in verbose mode.  All invalid
                entries and entries on the loop-back interface will be shown.
  inet_addr     Specifies an internet address.
  -N if_addr    Displays the ARP entries for the network interface specified
                by if_addr.
  -d            Deletes the host specified by inet_addr. inet_addr may be
                wildcarded with * to delete all hosts.
  -s            Adds the host and associates the Internet address inet_addr
                with the Physical address eth_addr.  The Physical address is
                given as 6 hexadecimal bytes separated by hyphens. The entry
                is permanent.
  eth_addr      Specifies a physical address.
  if_addr       If present, this specifies the Internet address of the
                interface whose address translation table should be modified.
                If not present, the first applicable interface will be used.
Example:
  > arp -s 157.55.85.212   00-aa-00-62-c6-09  .... Adds a static entry.
  > arp -a                                    .... Displays the arp table.
```

Which option deletes an entry from the ARP cache?

arp -d

What would be the result of issuing the **arp –d** * command?

It would delete all hosts

Record your Reflection

1. What is a benefit of keeping ARP cache entries in memory on the source computer?

   The device will not have to relearn the MAC addresses and associate them to an IP Address, this means that devices can be contacted faster

   It also prevents needlessly broadcasting ARP requests

2. If the destination IPv4 address is not located on the same network as the source host, what MAC address will be used as the destination target MAC address in the frame?

   The device will use teh MAC address of the default gateway

Learnings from this lab:

- ✓ ***Build a Simple Network***
- ✓ ***Configure the IP Address***
- ✓ ***Use Ping/ Trace route Utility to check the connection status***
- ✓ ***Use ipconfig /all command to determine the MAC address of a Windows computer on an Ethernet network.***
- ✓ ***Analyze a MAC address to determine the manufacturer.***
- ✓ ***Analyze the Wired and Wireless Network connection.***
- ✓ ***Analyze Address Resolution Protocol (ARP).***