Lab 4.2.4.5 Viewing Wireless and Wired NIC Information

1. Objectives

Part 1: Identify and Work with PC NICs

Part 2: Identify and Use the System Tray Network Icons

1. Background / Scenario

This lab requires you to determine the availability and status of the network interface cards (NICs) on the PC that you use. Windows provides a number of ways to view and work with your NICs.

In this lab, you will access the NIC information of your PC and change the status of these cards.

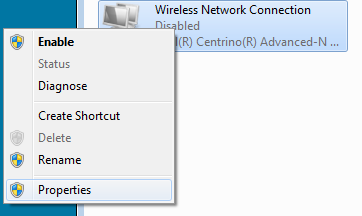
1. Identify and Work with PC NICs

In Part 1, you will identify the NIC types in the PC that you are using. You will explore different ways to extract information about these NICs and how to activate and deactivate them.

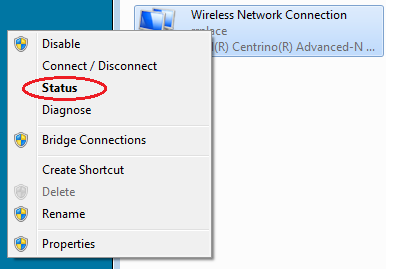
* 1. Use the Network and Sharing Center.
     1. Open the **Network and Sharing Center** by clicking the Windows **Start** button > **Control Panel** > **View network status and tasks** under Network and Internet heading in the Category View.
     2. In the left pane, click the **Change adapter settings** link.
     3. The Network Connections window displays, which provides the list of NICs available on this PC. Look for your Local Area Connection and Wireless Network Connection adapters in this window.



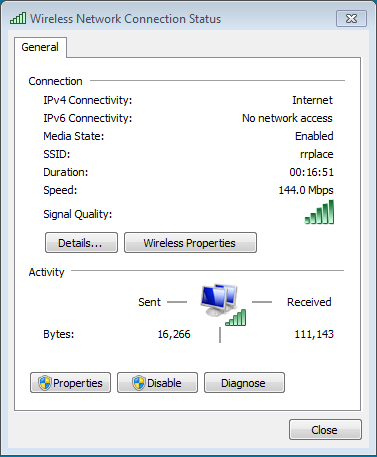
* 1. Work with your wireless NIC.
     1. Select the **Wireless Network Connection** option and right-click it to bring up a drop-down list. If your wireless NIC is disabled, you will have an option to **Enable** it. If your NIC was already enabled, then **Disable** would be the first option on this drop-down menu. If your **Wireless Network Connection** is currently disabled, then click **Enable**.



* + 1. Right-click the **Wireless Network Connection**, and then click **Status**.



* + 1. The Wireless Network Connection Status window displays where you can view information about your wireless connection.

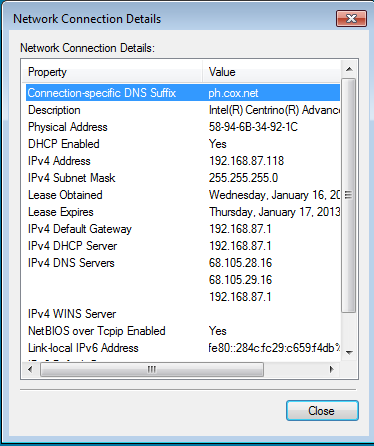


What is the Service Set Identifier (SSID) for the wireless router of your connection?\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

What is the speed of your wireless connection?\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**El SSID (Service Set IDentifier) es un nombre incluido en todos los paquetes de una red inalámbrica (**[**Wi-Fi**](http://es.wikipedia.org/wiki/Wi-Fi)**) para identificarlos como parte de esa red. Todos los dispositivos inalámbricos que intentan comunicarse entre sí deben compartir el mismo SSID.**

* + 1. Click **Details** to display the Network Connection Details window.



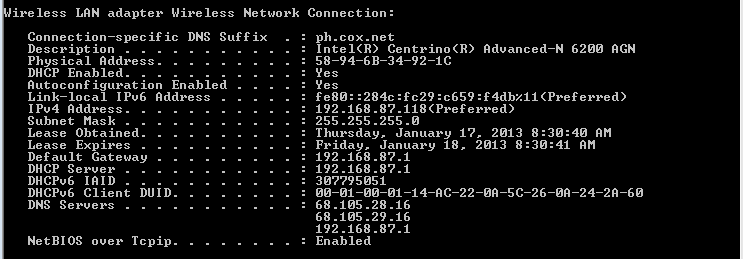
What is the MAC address of your wireless NIC?\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Do you have multiple IPv4 DNS Servers listed?\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Why would multiple DNS Servers be listed?

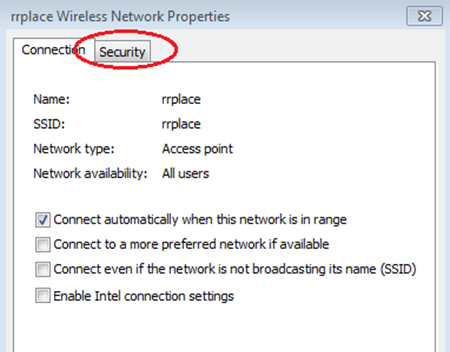
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* + 1. When you have reviewed the network connection details, click **Close**.
    2. Open a command window (**Windows + r > cmd**) prompt and type **ipconfig /all**.

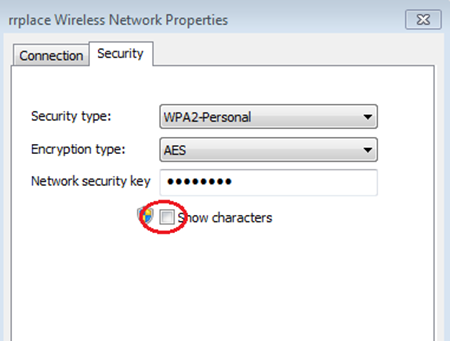


Notice that the information displayed here is the same information that was displayed in the Network Connection Details window in Step d.

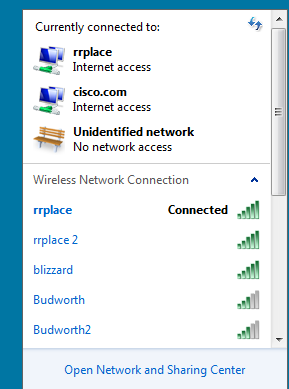
* + 1. Close the command window and the Network Connection Details windows. This should bring you back to the Wireless Network Connection Status window. Click **Wireless Properties**.
    2. In the **Wireless Network Properties** window, click the **Security** tab.



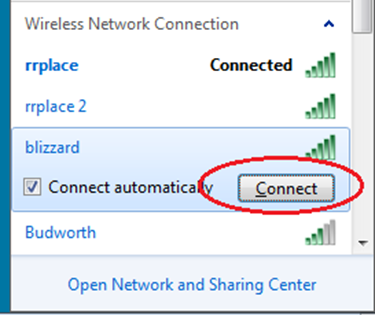
* + 1. The type of security the connected wireless router has implemented displays. Click the **Show characters** check box to display the actualNetwork security key, instead of the hidden characters, and then click **OK**.

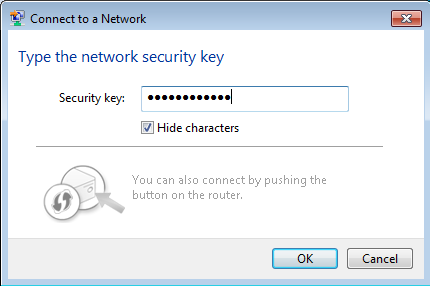
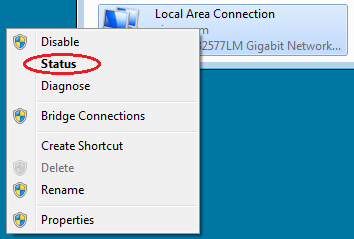


* + 1. Close the Wireless Network Properties and the Network Connection Status windows. Select and right-click the **Wireless Network Connection** option > **Connect/Disconnect**. A pop-up window should appear at the bottom right corner of your desktop that displays your current connections, along with a list of SSIDs that are in range of the wireless NIC of your PC. If a scrollbar appears on the right side of this window, you can use it to display additional SSIDs.



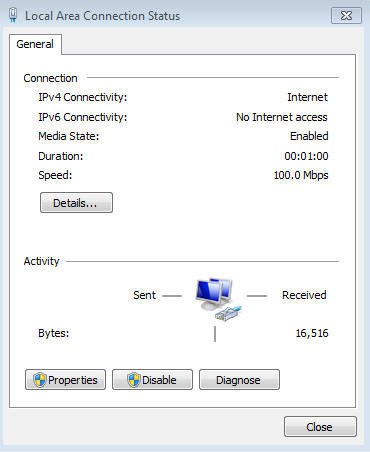
* + 1. To join one of the other wireless network SSIDs listed, click the SSID that you want to join, and then click **Connect**.



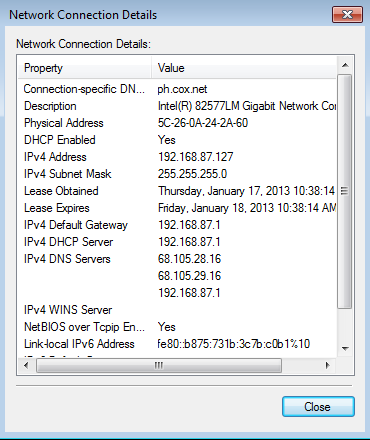
* + 1. If you have selected a secure SSID, you are prompted to enter the **Security key** for the SSID. Type the security key for that SSID and click **OK**. You can click the **Hide characters** check box to prevent people from seeing what you type in the **Security key** field.
  1. Work with your wired NIC.
     1. On the Network Connections window, select and right-click the **Local Area Connection** option to display the drop-down list. If the NIC is disabled, enable it, and then click the **Status** option.

**Note**: You must have an Ethernet cable attaching your PC NIC to a switch or similar device to see the status. Many wireless routers have a small 4-port Ethernet switch built-in. You can connect to one of the ports using a straight-through Ethernet patch cable.

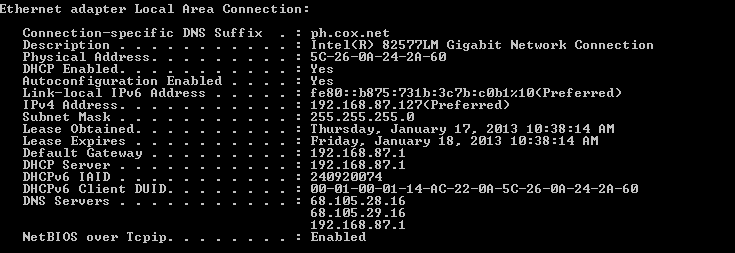
* + 1. The Local Area Connection Status window will open. This window displays information about your wired connection to the LAN.



* + 1. Click **Details…** to view the address information for your LAN connection.



* + 1. 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.



* + 1. Close all windows on your desktop.

1. Identify and Use the System Tray Network Icons

In Part 2, you will use the network icons in your system tray to determine and control the NICs on your PC.

Use the Wireless Network icon.

Click the system tray **Wireless Network** icon to view the pop-up window that displays the SSIDs that are in-range of your wireless NIC. When the system tray displays the Wireless Networkicon, the wireless NIC is active.



Lab 5.1.1.7 Using Wireshark to Examine Ethernet Frames



1. Background / Scenario

When upper layer protocols communicate with each other, data flows down the Open Systems Interconnection (OSI) layers and is encapsulated into a Layer 2 frame. The frame composition is dependent on the media access type. For example, if the upper layer protocols are TCP and IP and the media access is Ethernet, then the Layer 2 frame encapsulation will be Ethernet II. This is typical for a LAN environment.

When learning about Layer 2 concepts, it is helpful to analyze frame header information. In this lab, you will review the fields contained in an Ethernet II frame.

Examine the Header Fields in an Ethernet II Frame

* 1. Review the Ethernet II header field descriptions and lengths.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Preamble | Destination Address | Source Address | Frame Type | Data | FCS |
| 8 Bytes | 6 Bytes | 6 Bytes | 2 Bytes | 46 – 1500 Bytes | 4 Bytes |

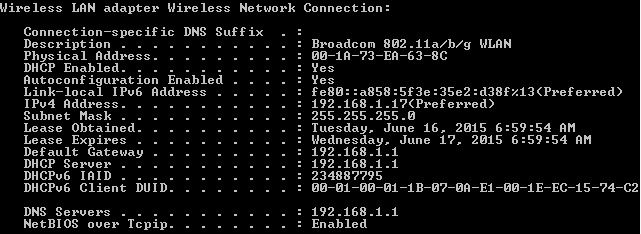
* 1. Examine the Ethernet II header contents of an ARP request.

The following table takes the first frame in the Wireshark capture and displays the data in the Ethernet II header fields.

|  |  |  |
| --- | --- | --- |
| Field | Value | Description |
| Preamble | Not shown in capture | This field contains synchronizing bits, processed by the NIC hardware. |
| Destination Address | Broadcast (ff:ff:ff:ff:ff:ff) | Layer 2 addresses for the frame. Each address is 48 bits long, or 6 octets, expressed as 12 hexadecimal digits, 0-9,A-F. A common format is 12:34:56:78:9A:BC.  The first six hex numbers indicate the manufacturer of the network interface card (NIC), the last six hex numbers are the serial number of the NIC.  The destination address may be a broadcast, which contains all ones, or a unicast. The source address is always unicast. |
| Source Address | GemtekTe\_ea:63:8c  (00:1a:73:ea:63:8c) |
| Frame Type | 0x0806 | For Ethernet II frames, this field contains a hexadecimal value that is used to indicate the type of upper-layer protocol in the data field. There are numerous upper-layer protocols supported by Ethernet II. Two common frame types are:  **Value Description**  0x0800 IPv4 Protocol  0x0806 Address resolution protocol (ARP) |
| Data | ARP | Contains the encapsulated upper-level protocol. The data field is between 46 – 1,500 bytes. |
| FCS | Not shown in capture | Frame Check Sequence, used by the NIC to identify errors during transmission. The value is computed by the sending machine, encompassing frame addresses, type, and data field. It is verified by the receiver. |

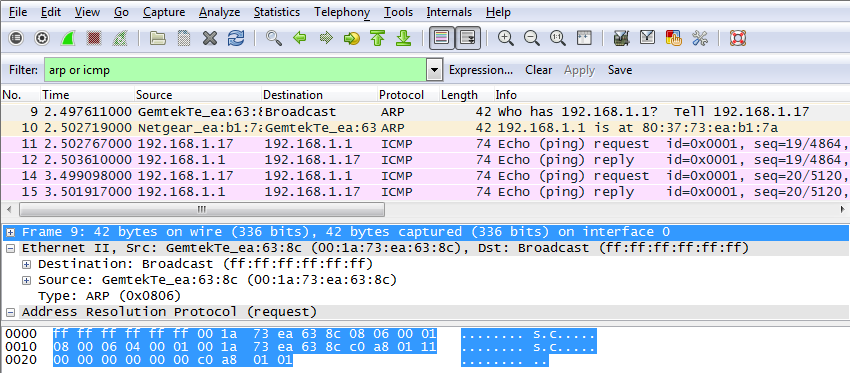
* 1. Examine the network configuration of the PC

This PC host IP address is 192.168.1.17 and the default gateway has an IP address of 192.168.1.1.



* 1. Examine Ethernet frames in a Wireshark capture.

The Wireshark capture below shows the packets generated by a **ping being issued from a PC host to its default gateway.** A filter has been applied to Wireshark to view the ARP and ICMP protocols only. The session begins with an ARP query for the MAC address of the gateway router, followed by four ping requests and replies.



What is significant about the contents of the destination address field?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Why does the PC send out a broadcast ARP prior to sending the first ping request?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

What is the MAC address of the source in the first frame? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

What is the Vendor ID (OUI) of the Source’s NIC? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

What is the Source’s NIC serial number? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Use Wireshark to Capture and Analyze Ethernet Frames

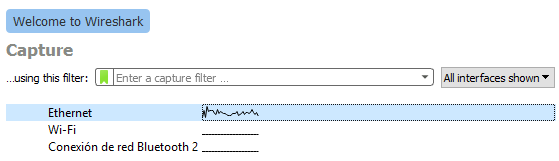
In Part 2, you will use Wireshark to capture local and remote Ethernet frames. You will then examine the information that is contained in the frame header fields.

* 1. Determine the IP address of the default gateway on your PC.

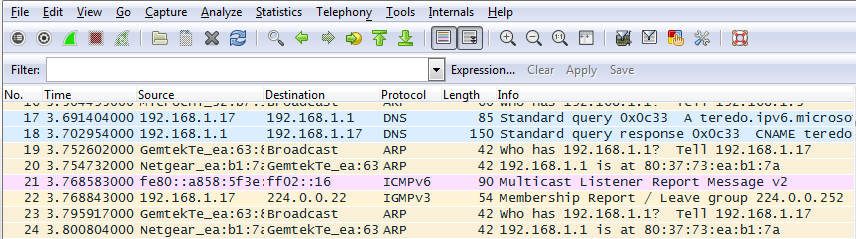
Open a command prompt window and issue the **ipconfig** command.

What is the IP Address of the PC Default Gateway? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* 1. Start capturing traffic on your PC’s NIC.
     1. Open Wireshark.
     2. In the **Wireshark: Capture Interfaces** window, click to the interface that is connected to your LAN.



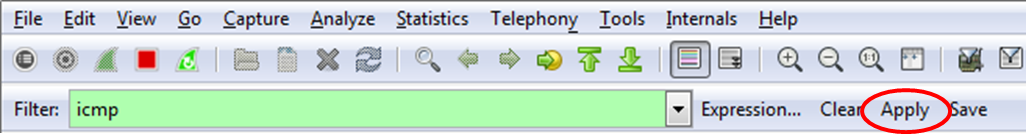
* + 1. Double click on the **Ethernet** interface.
    2. Observe the traffic that appears in the Packet List window.



* 1. Filter Wireshark to display only ICMP traffic.

You can use the filter in Wireshark to block visibility of unwanted traffic. The filter does not block the capture of unwanted data; it only filters what to display on the screen. For now, only ICMP traffic is to be displayed.

In the Wireshark **Filter** box, type **icmp**. The box should turn green if you typed the filter correctly. If the box is green, click **Apply** to apply the filter.

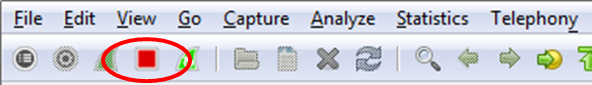


* 1. From the command prompt window, ping the default gateway of your PC.

From the command window, ping the default gateway using the IP address that you recorded in Step 1.

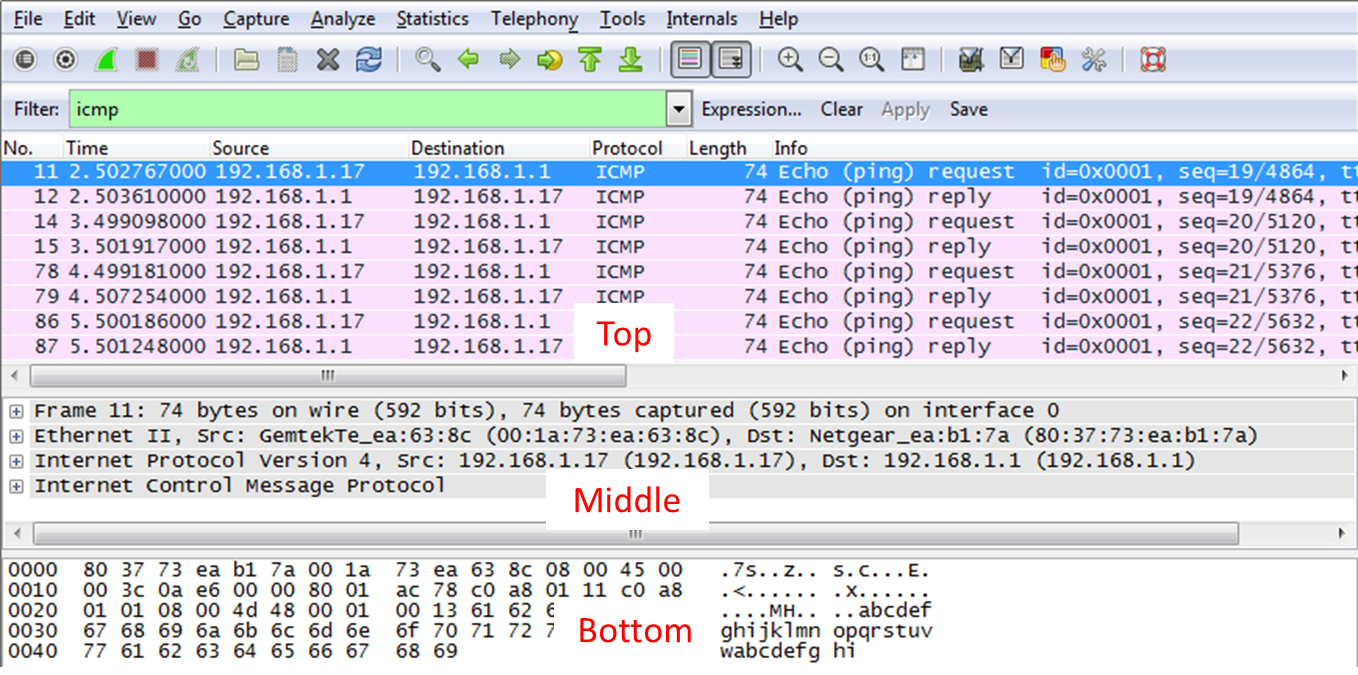
* 1. Stop capturing traffic on the NIC.

Click the **Stop Capture** icon to stop capturing traffic.



* 1. Examine the first Echo (ping) request in Wireshark.

The Wireshark main window is divided into three sections: the Packet List pane (top), the Packet Details pane (middle), and the Packet Bytes pane (bottom). If you selected the correct interface for packet capturing in Step 3, Wireshark should display the ICMP information in the Packet List pane of Wireshark, similar to the following example.



* + 1. In the Packet List pane (top section), click the first frame listed. You should see **Echo (ping) request** under the **Info** heading. This should highlight the line blue.
    2. Examine the first line in the Packet Details pane (middle section). This line displays the length of the frame; 74 bytes in this example.
    3. The second line in the Packet Details pane shows that it is an Ethernet II frame. The source and destination MAC addresses are also displayed.

What is the MAC address of the PC’s NIC? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

What is the default gateway’s MAC address? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* + 1. You can click the plus (+) sign at the beginning of the second line to obtain more information about the Ethernet II frame. Notice that the plus sign changes to a minus (-) sign.

What type of frame is displayed? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* + 1. The last two lines displayed in the middle section provide information about the data field of the frame. Notice that the data contains the source and destination IPv4 address information.

What is the source IP address? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

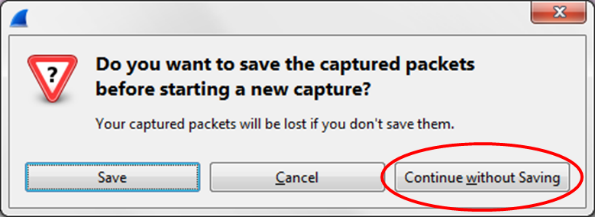
What is the destination IP address? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* + 1. Click the next frame in the top section and examine an Echo reply frame. Notice that the source and destination MAC addresses have reversed, because this frame was sent from the default gateway router as a reply to the first ping.

What device and MAC address is displayed as the destination address?\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* 1. Restart packet capture in Wireshark.

Click the **Start Capture** icon to start a new Wireshark capture. You will receive a popup window asking if you would like to save the previous captured packets to a file before starting a new capture. Click **Continue without Saving**.



* 1. In the command prompt window, ping [www.cisco.com](http://www.cisco.com).
  2. Stop capturing packets.
  3. Examine the new data in the packet list pane of Wireshark.

In the first echo (ping) request frame, what are the source and destination MAC addresses?

**Source**: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Destination**: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

What are the source and destination IP addresses contained in the data field of the frame?

**Source**: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Destination**: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Compare these addresses to the addresses you received in Step 6. The only address that changed is the destination IP address. Why has the destination IP address changed, while the destination MAC address remained the same?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_