Alan Palayil
ECE 407

ECE 407
Introduction to Computer Networks Laboratory

Practice 1 – Introduction to Wireshark and Cisco Packet Tracer

Objectives

The goal of this experiment is to:

1. Familiarize students with packet sniffing using Wireshark.
2. Familiarize students with Cisco Packet Tracer.

Part 1: Packet Sniffing using Wireshark

Background

The basic tool for observing the messages exchanged between executing protocol entities is called a packet sniffer. As the name suggests, a packet sniffer captures ("sniffs") messages being sent/received from/by your computer; it will also typically store and/or display the contents of the various protocol fields in these captured messages. A packet sniffer itself is passive. It observes messages being sent and received by applications and protocols running on your computer, but never sends packets itself. Similarly, received packets are never explicitly addressed to the packet sniffer. Instead, a packet sniffer receives a copy of packets that are sent/received from/by application and protocols executing on your machine. A packet sniffer consists of two parts: 1) the packet capture library, which receives a copy of every link-layer frame that is sent from or received by your computer (Note: all messages exchanged by higher layer protocols such as HTTP, FTP, TCP, UDP, DNS, or IP all are eventually encapsulated in link-layer frames that are transmitted over physical media such as an Ethernet cable), 2) The second component of a packet sniffer is the packet analyzer, which displays the contents of all fields within a protocol message. In order to do so, the packet analyzer must "understand" the structure of all messages exchanged by protocols.

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

Exercise 1: Using Wireshark to View Network Traffic (3.4.1.2)

Exercises in this experiment are based on Cisco NetAcad Labs

A. Capture and Analyze Local ICMP Data in Wireshark

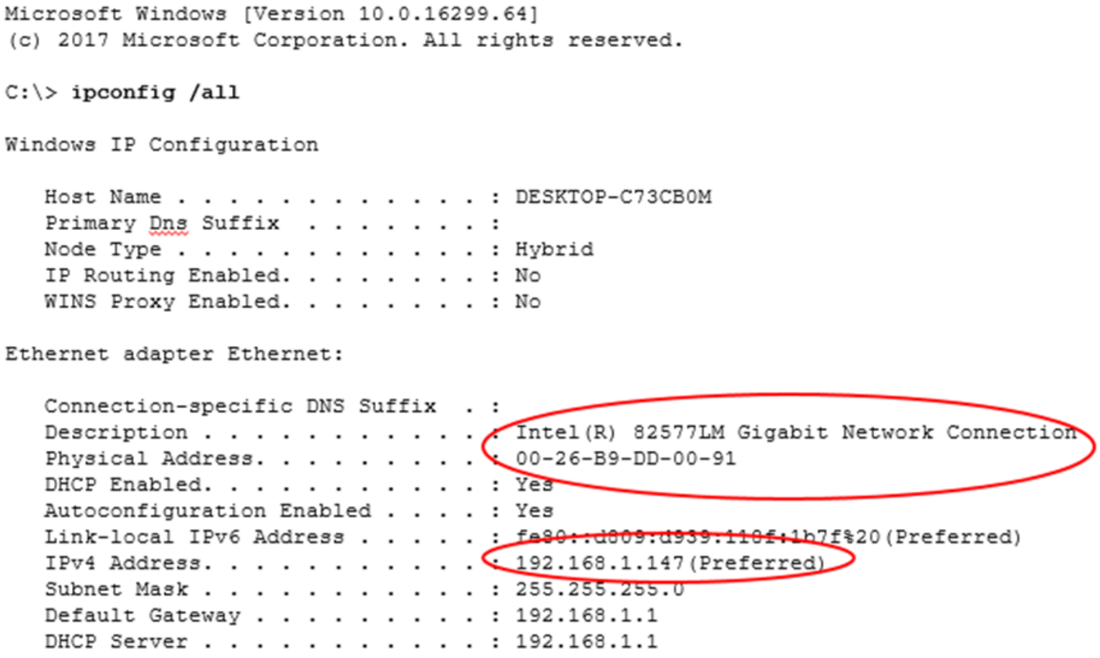
In this exercise, you will ping another PC on the LAN and capture ICMP requests and replies in Wireshark. You will also look inside the frames captured for specific information. This analysis should help to clarify how packet headers are used to transport data to their destination.

Step 1: Retrieve your PC interface addresses.

For this lab, you will need to retrieve your PC IP address and its network interface card (NIC) physical address, also called the MAC address.

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

b. Note the IP address



```
Microsoft Windows [Version 10.0.16299.64]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\> ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : DESKTOP-C73CB0M
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) 82577LM Gigabit Network Connection
   Physical Address. . . . . . . . . : 00-26-B9-DD-00-91
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::d809:d939:110f:1b7f%20(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.147(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1
   DHCP Server . . . . . . . . . . . : 192.168.1.1
```

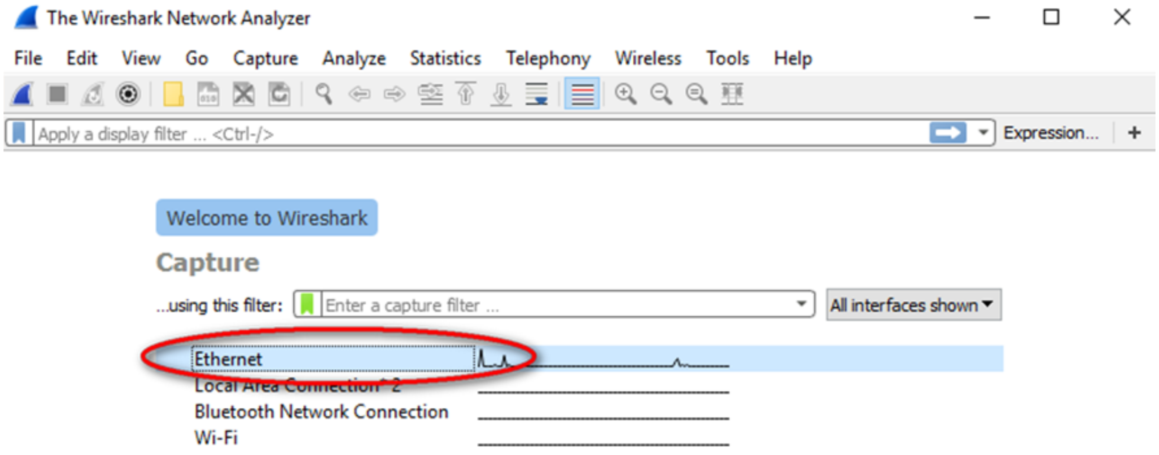
of your PC interface, its description, and its MAC (physical) address.

c. Ask a team member or team members for their PC IP address and provide your PC IP address to them. Do not provide them with your MAC address at this time.

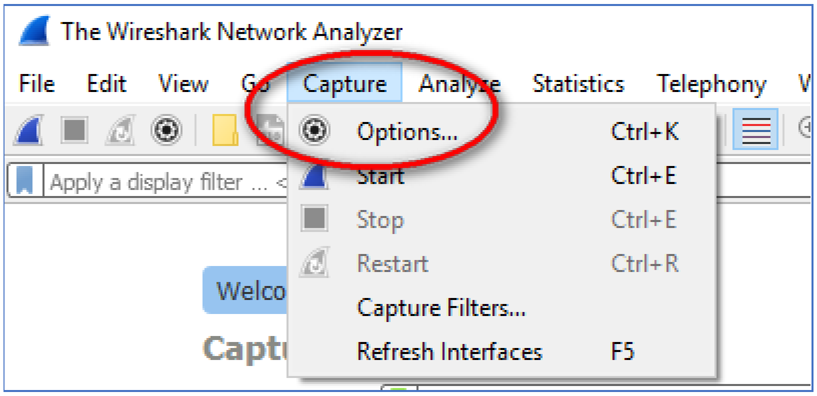
Step 2: Start Wireshark and begin capturing data.

a. On your PC, click the Windows **Start** button to see Wireshark listed as one of the programs on the pop-up menu. Double-click **Wireshark**.

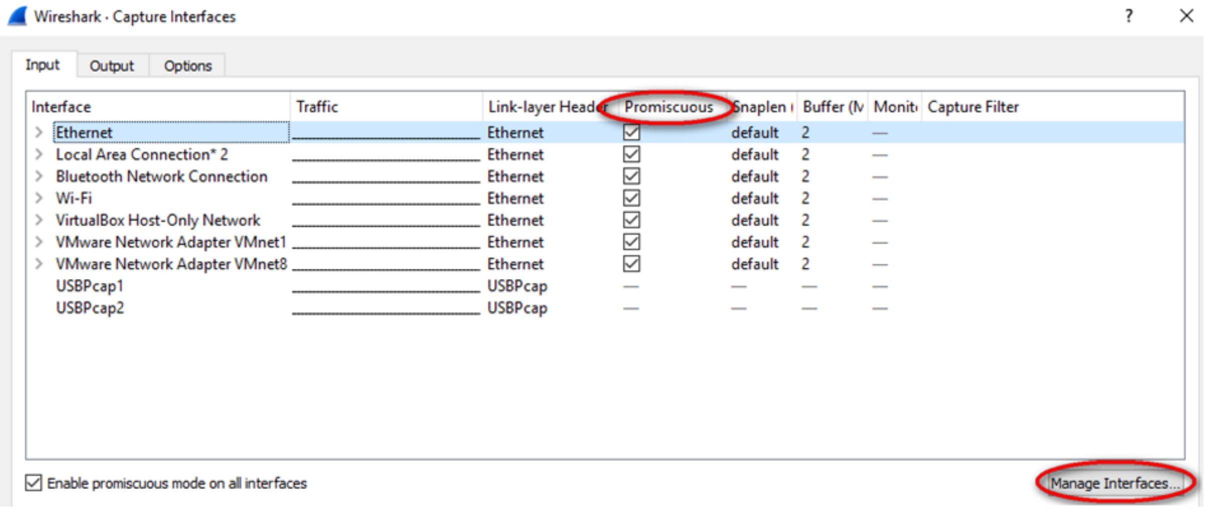
b. After Wireshark starts, click the capture interface to be used. Because we are using the wired Ethernet connection on the PC, make sure the Ethernet option is on the top of the list.


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
Welcome to Wireshark
Capture
...using this filter:
Enter a capture filter ...
All interfaces shown
Ethernet
Local Area Connection* 2
Bluetooth Network Connection
Wi-Fi

You can manage the capture interface by clicking **Capture** and **Options**:


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony
Apply a display filter ...
Options... Ctrl+K
Start Ctrl+E
Stop Ctrl+E
Restart Ctrl+R
Capture Filters...
Refresh Interfaces F5
Welco
Captu

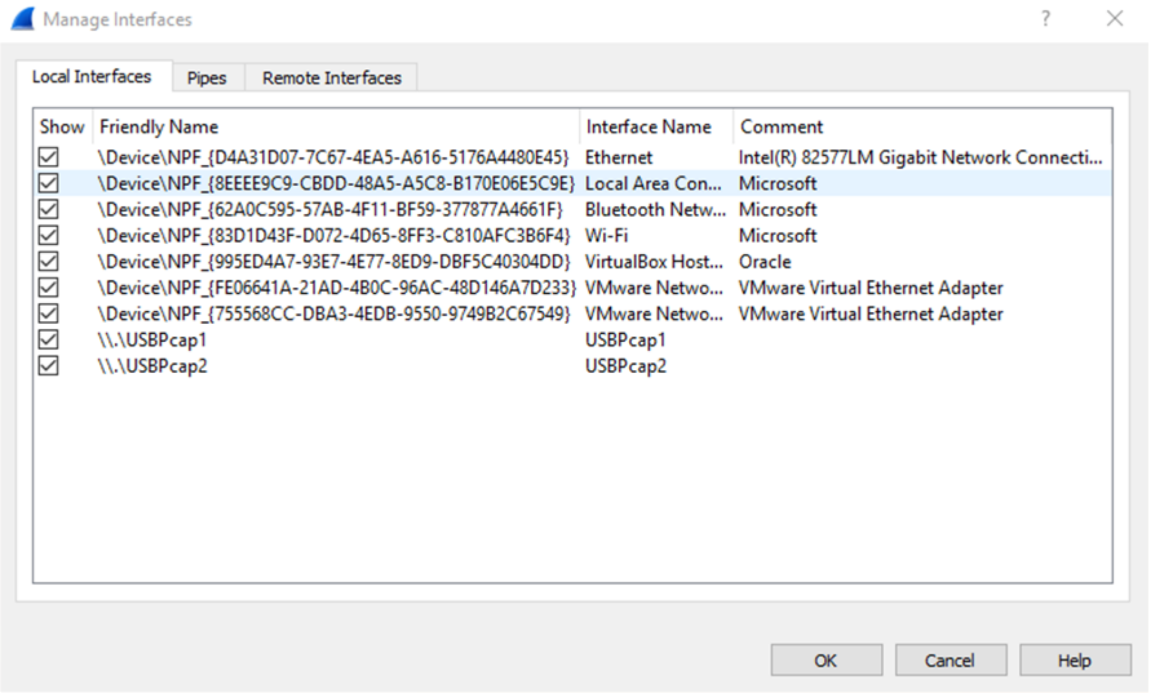
c. A list of interfaces will display. Make sure the capture interface is checked under **Promiscuous**.



Interface	Traffic	Link-layer Header	Promiscuous	Snaplen (	Buffer (M	Monit	Capture Filter
Ethernet		Ethernet	☑	default	2	—	
Local Area Connection* 2		Ethernet	☑	default	2	—	
Bluetooth Network Connection		Ethernet	☑	default	2	—	
Wi-Fi		Ethernet	☑	default	2	—	
VirtualBox Host-Only Network		Ethernet	☑	default	2	—	
VMware Network Adapter VMnet1		Ethernet	☑	default	2	—	
VMware Network Adapter VMnet8		Ethernet	☑	default	2	—	
USBPcap1		USBPcap	—	—	—	—	
USBPcap2		USBPcap	—	—	—	—	

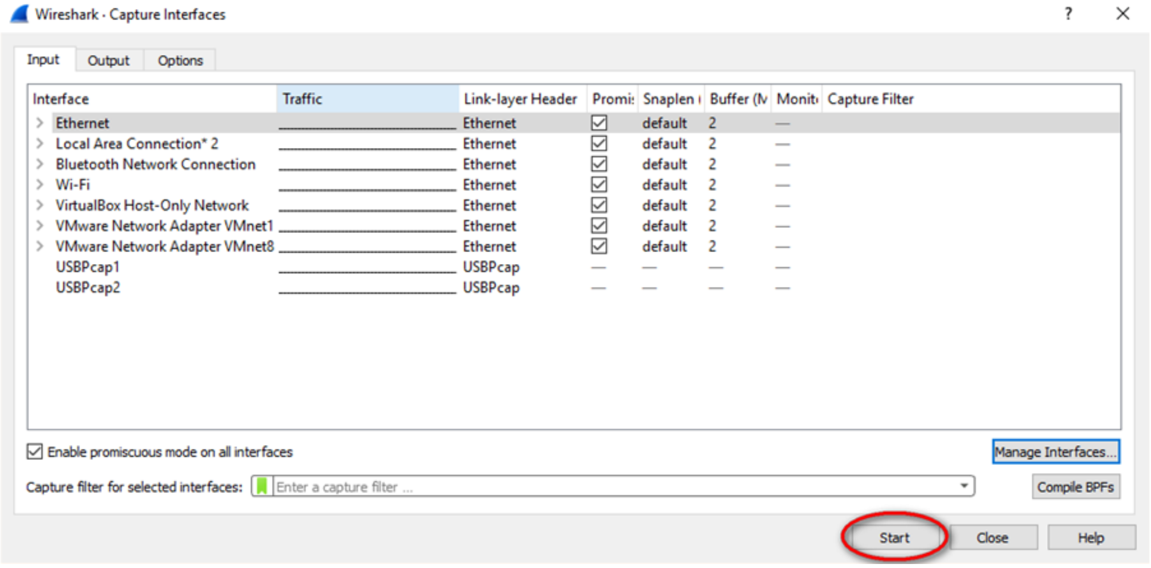
☑ Enable promiscuous mode on all interfaces

Note: We can further manage the interfaces on the PC by clicking **Manage Interfaces**. Verify that the description matches what you noted in Step 1b. Close the **Manage Interfaces** window after verifying the correct interface.



Show	Friendly Name	Interface Name	Comment
☑	\Device\NPF_{D4A31D07-7C67-4EA5-A616-5176A4480E45}	Ethernet	Intel(R) 82577LM Gigabit Network Connecti...
☑	\Device\NPF_{8EEEE9C9-CBDD-48A5-A5C8-B170E06E5C9E}	Local Area Con...	Microsoft
☑	\Device\NPF_{62A0C595-57AB-4F11-BF59-377877A4661F}	Bluetooth Netw...	Microsoft
☑	\Device\NPF_{83D1D43F-D072-4D65-8FF3-C810AFC3B6F4}	Wi-Fi	Microsoft
☑	\Device\NPF_{995ED4A7-93E7-4E77-8ED9-DBF5C40304DD}	VirtualBox Host...	Oracle
☑	\Device\NPF_{FE06641A-21AD-4B0C-96AC-48D146A7D233}	VMware Netwo...	VMware Virtual Ethernet Adapter
☑	\Device\NPF_{755568CC-DBA3-4EDB-9550-9749B2C67549}	VMware Netwo...	VMware Virtual Ethernet Adapter
☑	\\.\USBPcap1	USBPcap1	
☑	\\.\USBPcap2	USBPcap2	

d. After you have checked the correct interface, click **Start** to start the data capture.

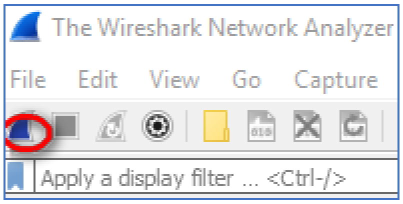


Interface	Traffic	Link-layer Header	Promi:	Snaplen	Buffer (M	Monit	Capture Filter
Ethernet		Ethernet	☑	default	2	—	
Local Area Connection* 2		Ethernet	☑	default	2	—	
Bluetooth Network Connection		Ethernet	☑	default	2	—	
Wi-Fi		Ethernet	☑	default	2	—	
VirtualBox Host-Only Network		Ethernet	☑	default	2	—	
VMware Network Adapter VMnet1		Ethernet	☑	default	2	—	
VMware Network Adapter VMnet8		Ethernet	☑	default	2	—	
USBPcap1		USBPcap	—	—	—	—	
USBPcap2		USBPcap	—	—	—	—	

☑ Enable promiscuous mode on all interfaces

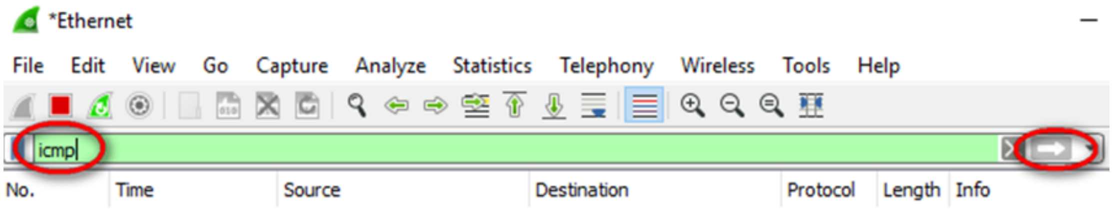
Capture filter for selected interfaces: Enter a capture filter ...

Note: You can also start the data capture by clicking the **Wireshark** icon in the main interface.


The Wireshark Network Analyzer
File
Edit
View
Go
Capture
Apply a display filter ... <Ctrl-/>

Information will start scrolling down the top section in Wireshark. The data lines will appear in different colors based on protocol.

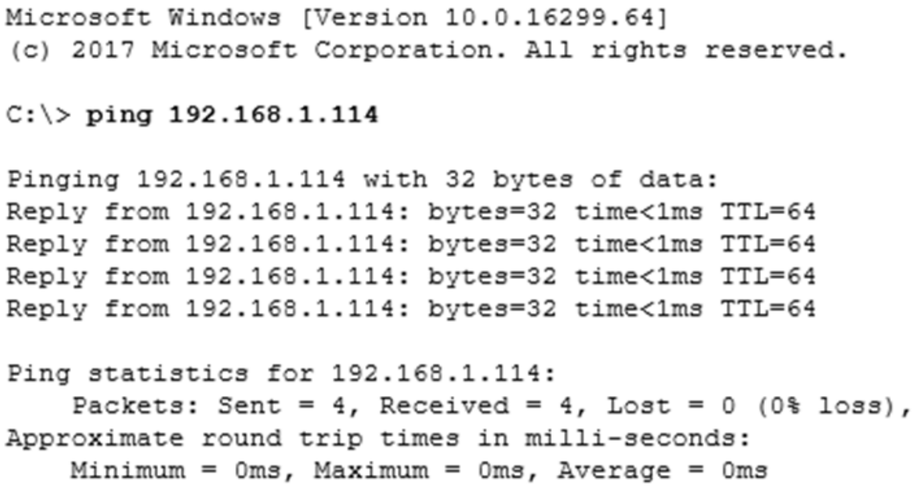
e. This information can scroll by very quickly depending on what communication is taking place between your PC and the LAN. We can apply a filter to make it easier to view and work with the data that is being captured by Wireshark. For this lab, we are only interested in displaying ICMP (ping) PDUs. Type **icmp** in the **Filter** box at the top of Wireshark and press **Enter** or click on the **Apply** button (arrow sign) to view only ICMP (ping) PDUs.



icmp

Exercises in this experiment are based on Cisco NetAcad Labs

f. This filter causes all data in the top window to disappear, but you are still capturing the traffic on the interface. Bring up the command prompt window that you opened earlier and ping the IP address that you received from your team member.

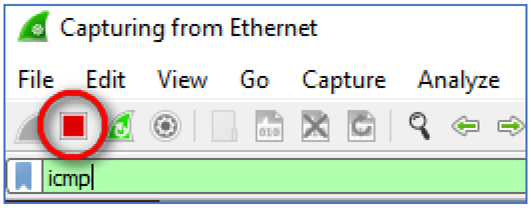


```
Microsoft Windows [Version 10.0.16299.64]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\> ping 192.168.1.114

Pinging 192.168.1.114 with 32 bytes of data:
Reply from 192.168.1.114: bytes=32 time<1ms TTL=64
Reply from 192.168.1.114: bytes=32 time<1ms TTL=64
Reply from 192.168.1.114: bytes=32 time<1ms TTL=64
Reply from 192.168.1.114: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.1.114:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Notice that you start seeing data appear in the top window of Wireshark again.

Note: If the PC of your team member does not reply to your pings, this may be because the PC firewall of the team member is blocking these requests. Please see Appendix A: Allowing ICMP Traffic Through a Firewall for information on how to allow ICMP traffic through the firewall using Windows 7.

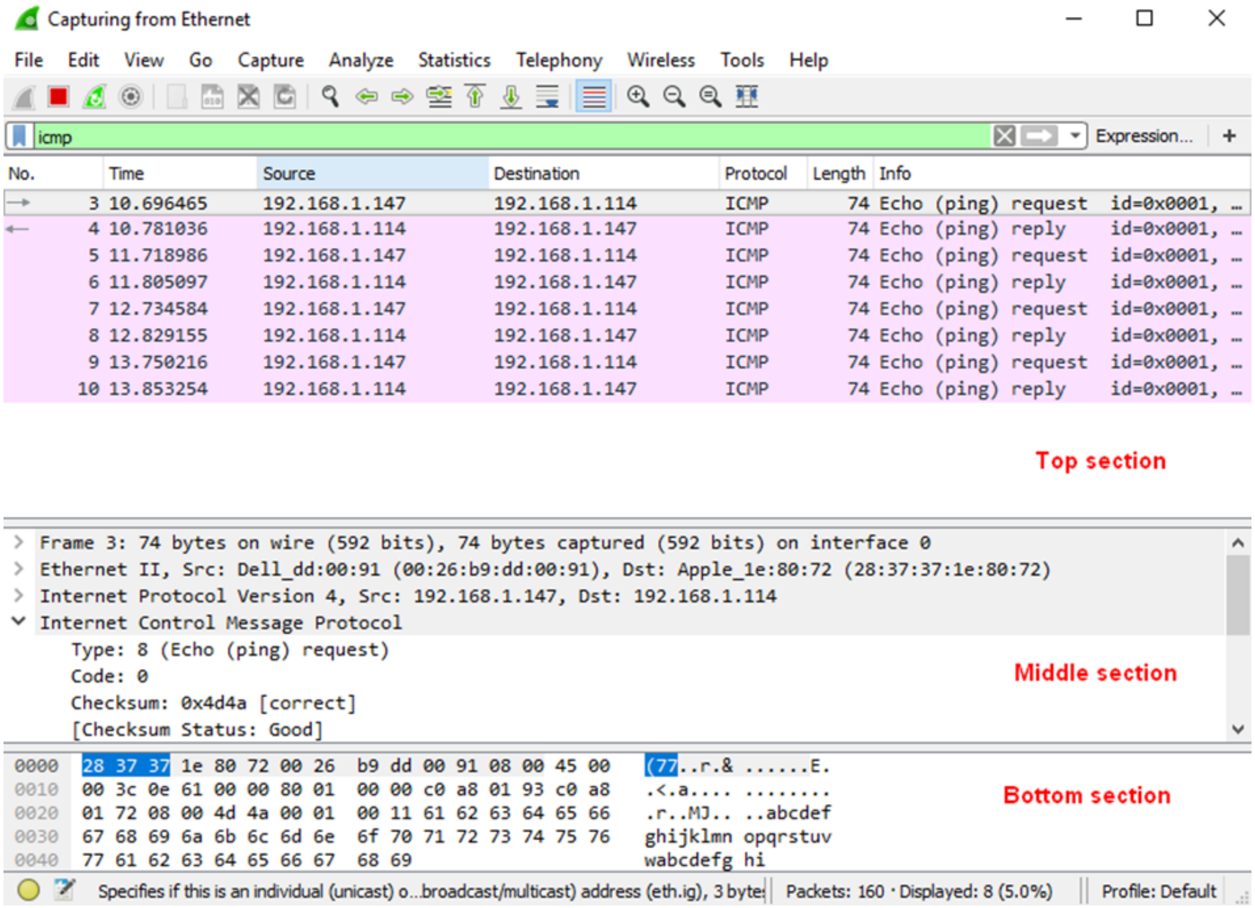
g. Stop capturing data by clicking the **Stop Capture** icon.



icmp

Step 3: Examine the captured data.

In Step 3, examine the data that was generated by the ping requests of your team member PC. Wireshark data is displayed in three sections: 1) The top section displays the list of PDU frames captured with a summary of the IP 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; and 3) the bottom section displays the raw data of each layer. The raw data is displayed in both hexadecimal and decimal form.


Capturing from Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression…
+
Top section
Middle section
Bottom section

icmp

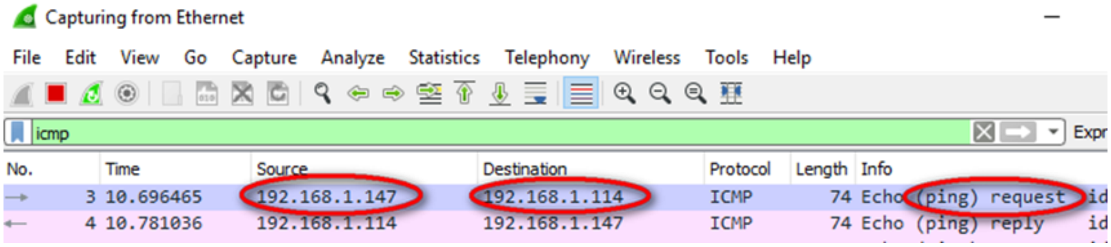
No.	Time	Source	Destination	Protocol	Length	Info
3	10.696465	192.168.1.147	192.168.1.114	ICMP	74	Echo (ping) request id=0x0001, …
4	10.781036	192.168.1.114	192.168.1.147	ICMP	74	Echo (ping) reply id=0x0001, …
5	11.718986	192.168.1.147	192.168.1.114	ICMP	74	Echo (ping) request id=0x0001, …
6	11.805097	192.168.1.114	192.168.1.147	ICMP	74	Echo (ping) reply id=0x0001, …
7	12.734584	192.168.1.147	192.168.1.114	ICMP	74	Echo (ping) request id=0x0001, …
8	12.829155	192.168.1.114	192.168.1.147	ICMP	74	Echo (ping) reply id=0x0001, …
9	13.750216	192.168.1.147	192.168.1.114	ICMP	74	Echo (ping) request id=0x0001, …
10	13.853254	192.168.1.114	192.168.1.147	ICMP	74	Echo (ping) reply id=0x0001, …

```
> Frame 3: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
> Ethernet II, Src: Dell_dd:00:91 (00:26:b9:dd:00:91), Dst: Apple_1e:80:72 (28:37:37:1e:80:72)
> Internet Protocol Version 4, Src: 192.168.1.147, Dst: 192.168.1.114
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x4d4a [correct]
    [Checksum Status: Good]
```

```
0000  28 37 37 1e 80 72 00 26  b9 dd 00 91 08 00 45 00   (77..r.& ......E.
0010  00 3c 0e 61 00 00 80 01  00 00 c0 a8 01 93 c0 a8   .<.a.... ........
0020  01 72 08 00 4d 4a 00 01  00 11 61 62 63 64 65 66   .r..MJ.. ..abcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67  68 69                     wabcdefg hi
```

Specifies if this is an individual (unicast) o...broadcast/multicast) address (eth.ig), 3 byte | Packets: 160 · Displayed: 8 (5.0%) | Profile: Default

a. Click the first ICMP request PDU frames in the top section of Wireshark. Notice that the **Source** column has your PC IP address, and the **Destination** column contains the IP address of the teammate PC that you pinged.

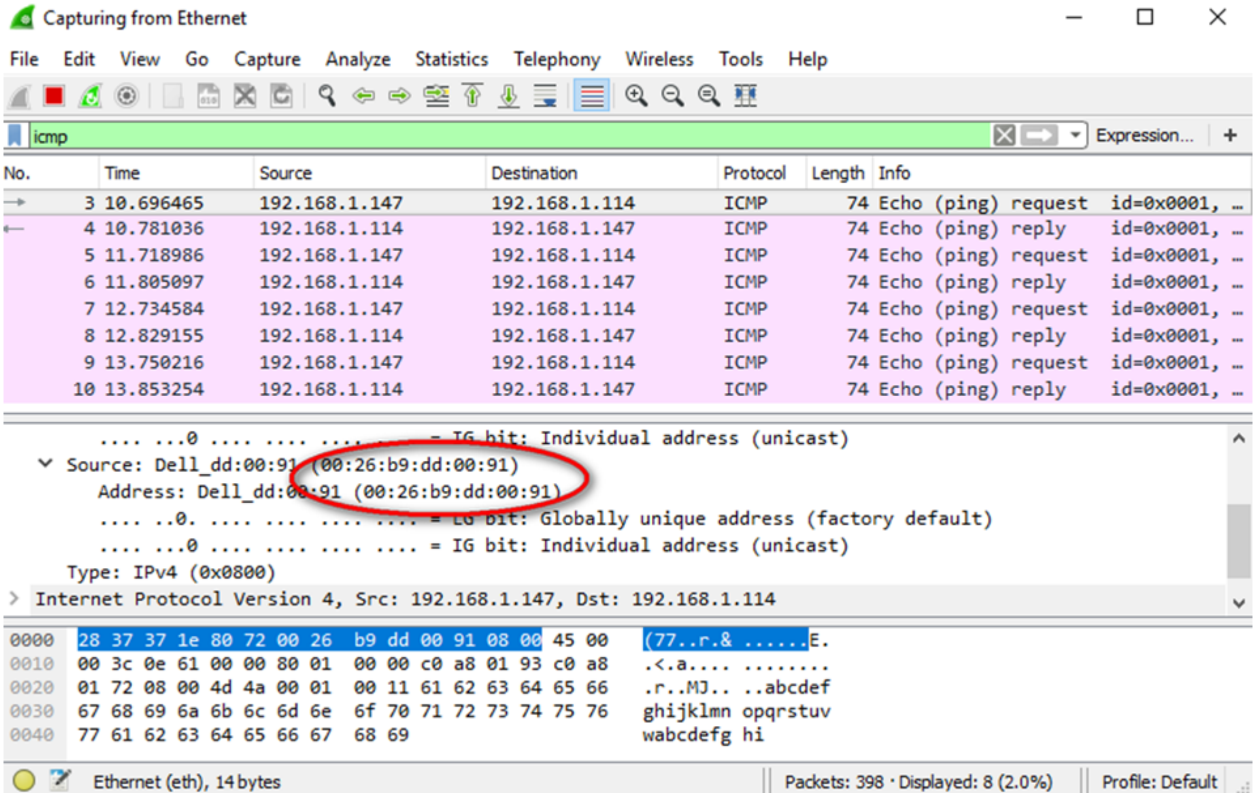

Capturing from Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expr

icmp

No.	Time	Source	Destination	Protocol	Length	Info
3	10.696465	192.168.1.147	192.168.1.114	ICMP	74	Echo (ping) request id
4	10.781036	192.168.1.114	192.168.1.147	ICMP	74	Echo (ping) reply id

Exercises in this experiment are based on Cisco NetAcad Labs

b. With this PDU frame still selected in the top section, navigate to the middle section. Click the plus sign to the left of the Ethernet II row to view the destination and source MAC addresses.


Capturing from Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression... +

icmp

No.	Time	Source	Destination	Protocol	Length	Info
3	10.696465	192.168.1.147	192.168.1.114	ICMP	74	Echo (ping) request id=0x0001, …
4	10.781036	192.168.1.114	192.168.1.147	ICMP	74	Echo (ping) reply id=0x0001, …
5	11.718986	192.168.1.147	192.168.1.114	ICMP	74	Echo (ping) request id=0x0001, …
6	11.805097	192.168.1.114	192.168.1.147	ICMP	74	Echo (ping) reply id=0x0001, …
7	12.734584	192.168.1.147	192.168.1.114	ICMP	74	Echo (ping) request id=0x0001, …
8	12.829155	192.168.1.114	192.168.1.147	ICMP	74	Echo (ping) reply id=0x0001, …
9	13.750216	192.168.1.147	192.168.1.114	ICMP	74	Echo (ping) request id=0x0001, …
10	13.853254	192.168.1.114	192.168.1.147	ICMP	74	Echo (ping) reply id=0x0001, …

```
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  ˅ Source: Dell_dd:00:91 (00:26:b9:dd:00:91)
      Address: Dell_dd:00:91 (00:26:b9:dd:00:91)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 192.168.1.147, Dst: 192.168.1.114
```

```
0000  28 37 37 1e 80 72 00 26  b9 dd 00 91 08 00 45 00   (77..r.& ......E.
0010  00 3c 0e 61 00 00 80 01  00 00 c0 a8 01 93 c0 a8   .<.a.... ........
0020  01 72 08 00 4d 4a 00 01  00 11 61 62 63 64 65 66   .r..MJ.. ..abcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67  68 69                     wabcdefg hi
```

Ethernet (eth), 14 bytes | Packets: 398 · Displayed: 8 (2.0%) | Profile: Default

Does the source MAC address match your PC interface (shown in Step 1.b)?

- **Yes**

Does the destination MAC address in Wireshark match your team member MAC address?

- **Yes**

How is the MAC address of the pinged PC obtained by your PC?

- **It is obtained through an ARP request.**

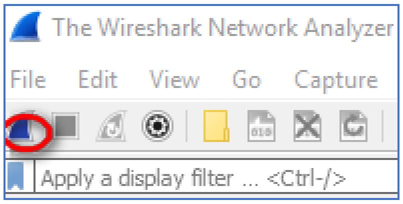
Note: In the preceding example of a captured ICMP request, ICMP data is encapsulated inside an IPv4 packet PDU (IPv4 header) which is then encapsulated in an Ethernet II frame PDU (Ethernet II header) for transmission on the LAN.

B. Capture and Analyze Remote ICMP Data in Wireshark

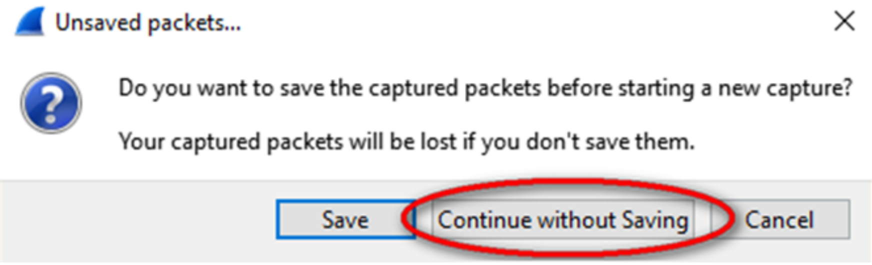
In this exercise, you will ping remote hosts (hosts not on the LAN) and examine the generated data from those pings. You will then determine what is different about this data from the data examined in exercise A.

a. Start capturing data on the interface.

i. Start the data capture again.


The Wireshark Network Analyzer
File Edit View Go Capture
Apply a display filter ... <Ctrl-/>

ii. A window prompts you to save the previously captured data before starting another capture. It is not necessary to save this data. Click **Continue without Saving**.


Unsaved packets...

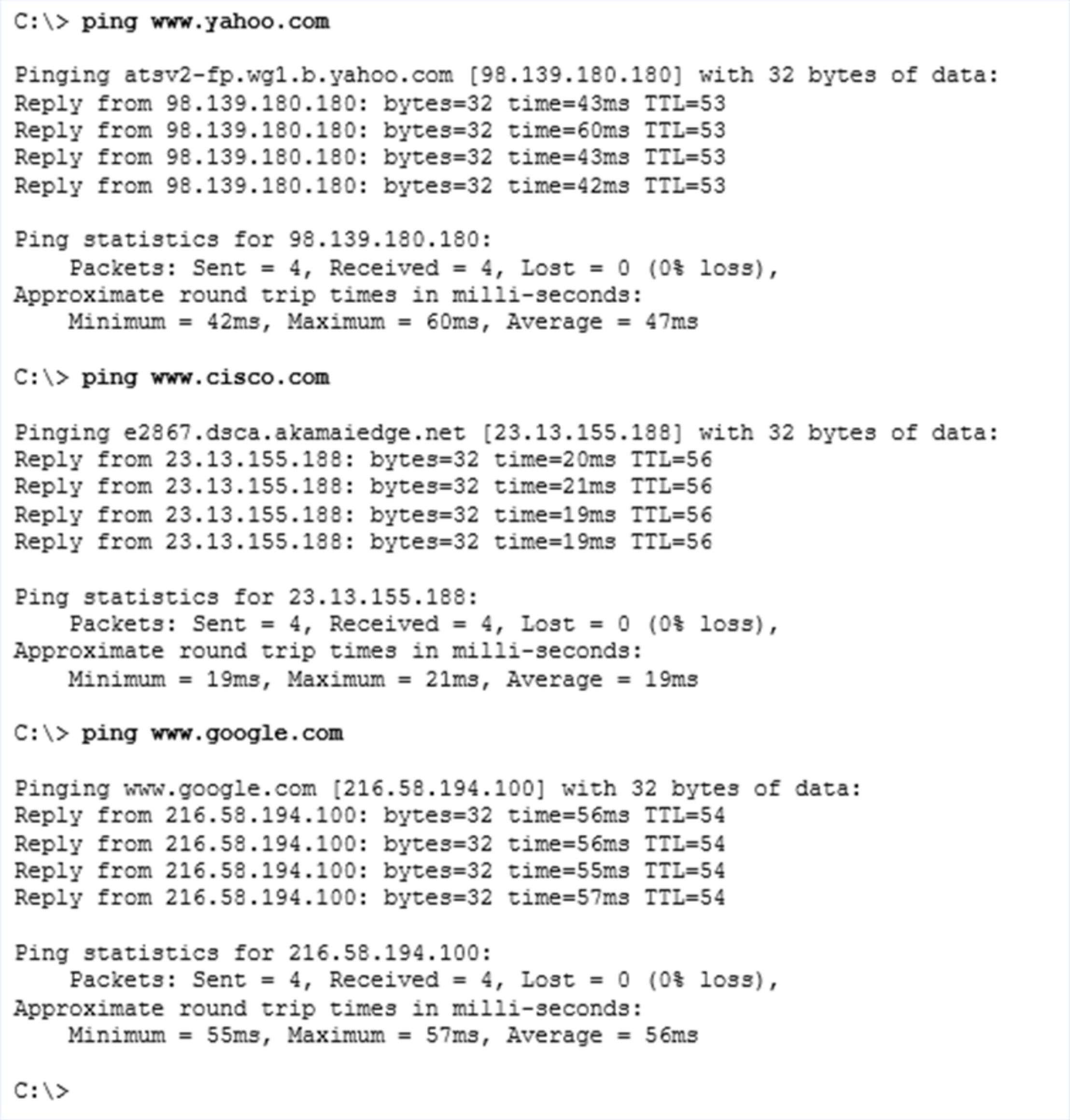
Do you want to save the captured packets before starting a new capture?

Your captured packets will be lost if you don't save them.

iii. With the capture active, ping the following three website URLs:

1. www.yahoo.com
2. www.cisco.com

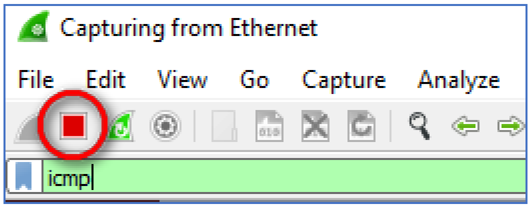
3. www.google.com



```
C:\> ping www.yahoo.com

Pinging atsv2-fp.wg1.b.yahoo.com [98.139.180.180] with 32 bytes of data:
Reply from 98.139.180.180: bytes=32 time=43ms TTL=53
Reply from 98.139.180.180: bytes=32 time=60ms TTL=53
Reply from 98.139.180.180: bytes=32 time=43ms TTL=53
Reply from 98.139.180.180: bytes=32 time=42ms TTL=53

Ping statistics for 98.139.180.180:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 42ms, Maximum = 60ms, Average = 47ms

C:\> ping www.cisco.com

Pinging e2867.dsca.akamaiedge.net [23.13.155.188] with 32 bytes of data:
Reply from 23.13.155.188: bytes=32 time=20ms TTL=56
Reply from 23.13.155.188: bytes=32 time=21ms TTL=56
Reply from 23.13.155.188: bytes=32 time=19ms TTL=56
Reply from 23.13.155.188: bytes=32 time=19ms TTL=56

Ping statistics for 23.13.155.188:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 19ms, Maximum = 21ms, Average = 19ms

C:\> ping www.google.com

Pinging www.google.com [216.58.194.100] with 32 bytes of data:
Reply from 216.58.194.100: bytes=32 time=56ms TTL=54
Reply from 216.58.194.100: bytes=32 time=56ms TTL=54
Reply from 216.58.194.100: bytes=32 time=55ms TTL=54
Reply from 216.58.194.100: bytes=32 time=57ms TTL=54

Ping statistics for 216.58.194.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 55ms, Maximum = 57ms, Average = 56ms

C:\>
```

Note: When you ping the URLs listed, notice that the Domain Name Server (DNS) translates the URL to an IP address. Note the IP address received for each URL.

iv. You can stop capturing data by clicking the **Stop Capture** icon.



icmp

Exercises in this experiment are based on Cisco NetAcad Labs

b. Examining and analyzing the data from the remote hosts.

i. Review the captured data in Wireshark and examine the IP and MAC addresses of the three locations that you pinged. List the destination IP and MAC addresses for all three locations in the space provided.

● **<u>www.yahoo.com</u>**	**IP: 74.6.231.20**	**MAC: e0 : 9d : 31 : f4 : bf : 32**
● **<u>www.cisco.com</u>**	**IP: 96.17.51.173**	**MAC: cc : 40 : d0 : 6f : 3d : 69**
● **<u>www.google.com</u>**	**IP: 142.250.190.4**	**MAC: e0 : 9d : 31 : f4 : bf : 32**

ii. What is significant about this information?

- **The MAC address is the physical address while IP is the identifier of the connection to the network**

iii. How does this information differ from the local ping information you received in Part A?

- **It differs because Part A involves a local network**

Reflection

Why does Wireshark show the actual MAC address of the local hosts, but not the actual MAC address for the remote hosts?

- **This is due to the fact that MAC addresses of the remote hosts is not known to the local network**

<u>Exercise 2: Using Wireshark to Examine Ethernet Frames (5.1.1.7)</u>

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 exercise, you will use Wireshark to capture and analyze Ethernet II frame header fields for local and remote traffic.

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

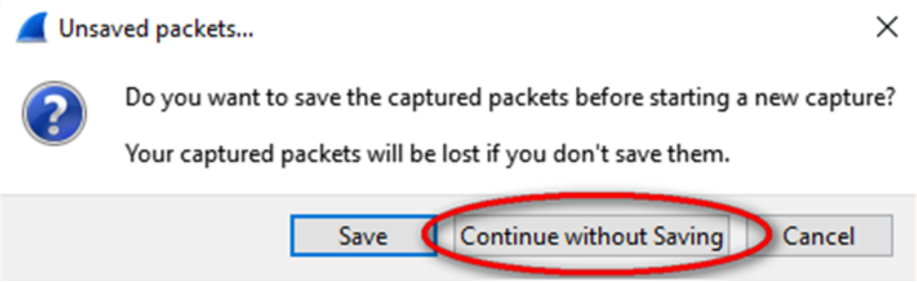
Open a command prompt window and issue the **ipconfig** command.

What is the IP address of the PC default gateway?

- **10.0.0.139**

Step 2: Start capturing traffic on your PC NIC.

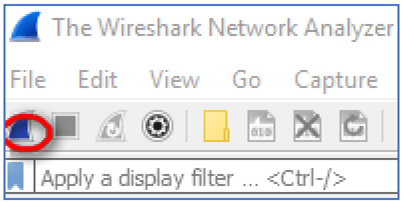
a. Close Wireshark. No need to save the captured data.


Unsaved packets...

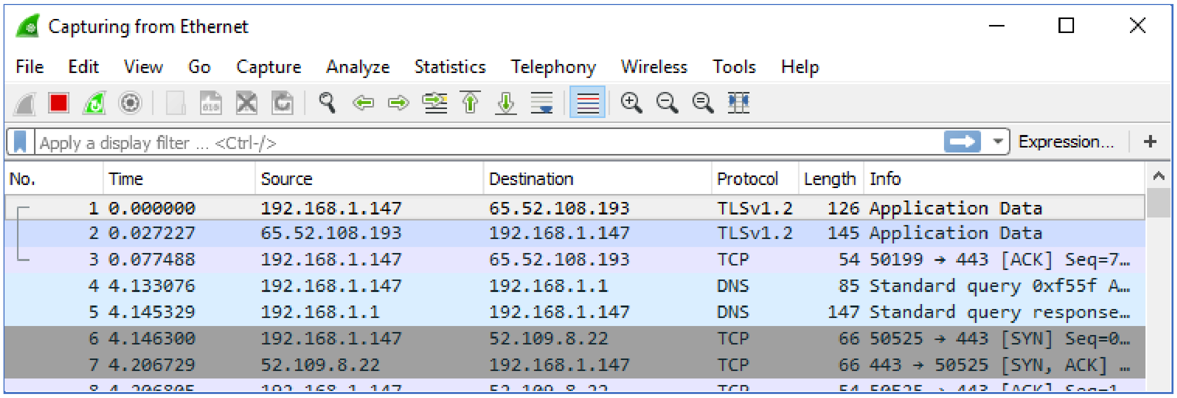
Do you want to save the captured packets before starting a new capture?

Your captured packets will be lost if you don't save them.

b. Open Wireshark, start data capture.


The Wireshark Network Analyzer
File
Edit
View
Go
Capture
Apply a display filter ... <Ctrl-/>

c. Observe the traffic that appears in the packet list window.

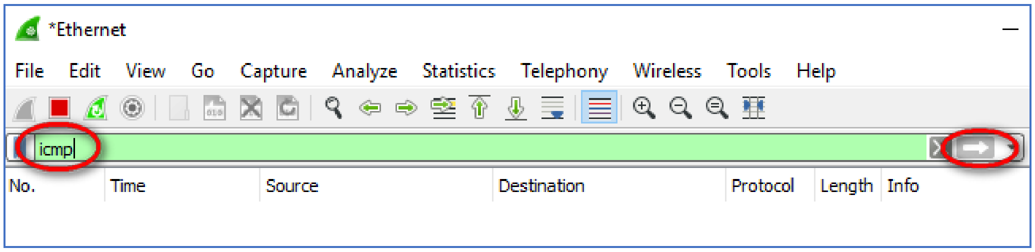


No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.147	65.52.108.193	TLSv1.2	126	Application Data
2	0.027227	65.52.108.193	192.168.1.147	TLSv1.2	145	Application Data
3	0.077488	192.168.1.147	65.52.108.193	TCP	54	50199 → 443 [ACK] Seq=7…
4	4.133076	192.168.1.147	192.168.1.1	DNS	85	Standard query 0xf55f A…
5	4.145329	192.168.1.1	192.168.1.147	DNS	147	Standard query response…
6	4.146300	192.168.1.147	52.109.8.22	TCP	66	50525 → 443 [SYN] Seq=0…
7	4.206729	52.109.8.22	192.168.1.147	TCP	66	443 → 50525 [SYN, ACK] …
8	4.206805	192.168.1.147	52.109.8.22	TCP	54	50525 → 443 [ACK] Seq=1

Step 3: 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** (the right arrow) to apply the filter.

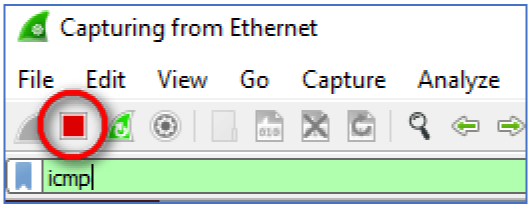

*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
icmp
No. Time Source Destination Protocol Length Info

Step 4: 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.

Step 5: Stop capturing traffic on the NIC.

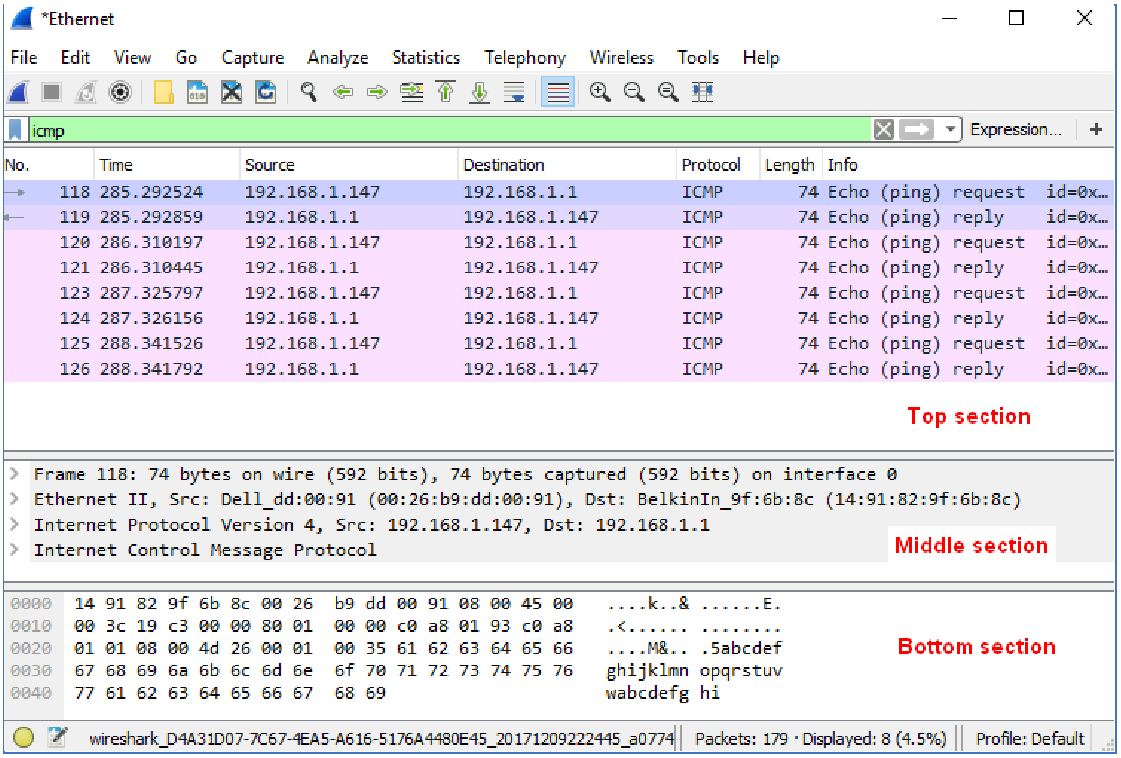
Click the **Stop Capture** icon to stop capturing traffic.



Exercises in this experiment are based on Cisco NetAcad Labs

Step 6: 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.


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
icmp
Expression…
+

```
No.    Time        Source         Destination    Protocol  Length Info
118 285.292524  192.168.1.147  192.168.1.1    ICMP      74 Echo (ping) request  id=0x…
119 285.292859  192.168.1.1    192.168.1.147  ICMP      74 Echo (ping) reply    id=0x…
120 286.310197  192.168.1.147  192.168.1.1    ICMP      74 Echo (ping) request  id=0x…
121 286.310445  192.168.1.1    192.168.1.147  ICMP      74 Echo (ping) reply    id=0x…
123 287.325797  192.168.1.147  192.168.1.1    ICMP      74 Echo (ping) request  id=0x…
124 287.326156  192.168.1.1    192.168.1.147  ICMP      74 Echo (ping) reply    id=0x…
125 288.341526  192.168.1.147  192.168.1.1    ICMP      74 Echo (ping) request  id=0x…
126 288.341792  192.168.1.1    192.168.1.147  ICMP      74 Echo (ping) reply    id=0x…
```

Top section

```
> Frame 118: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
> Ethernet II, Src: Dell_dd:00:91 (00:26:b9:dd:00:91), Dst: BelkinIn_9f:6b:8c (14:91:82:9f:6b:8c)
> Internet Protocol Version 4, Src: 192.168.1.147, Dst: 192.168.1.1
> Internet Control Message Protocol
```

Middle section

```
0000  14 91 82 9f 6b 8c 00 26  b9 dd 00 91 08 00 45 00   ....k..& ......E.
0010  00 3c 19 c3 00 00 80 01  00 00 c0 a8 01 93 c0 a8   .<...... ........
0020  01 01 08 00 4d 26 00 01  00 35 61 62 63 64 65 66   ....M&.. .5abcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67  68 69                     wabcdefg hi
```

Bottom section

wireshark_D4A31D07-7C67-4EA5-A616-5176A4480E45_20171209222445_a0774 | Packets: 179 · Displayed: 8 (4.5%) | Profile: Default

a. 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.

b. Examine the first line in the packet details pane (middle section). This line displays the length of the frame; 74 bytes in this example.

c. 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 NIC?

- **e0 : 9d : 31 : f4 : bf : 32**

What is the default gateway's MAC address?

- **cc : 40 : d0 : 6f : 3d : 69**

d. 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?

- **IPv4 (0x0800)**

e. 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.

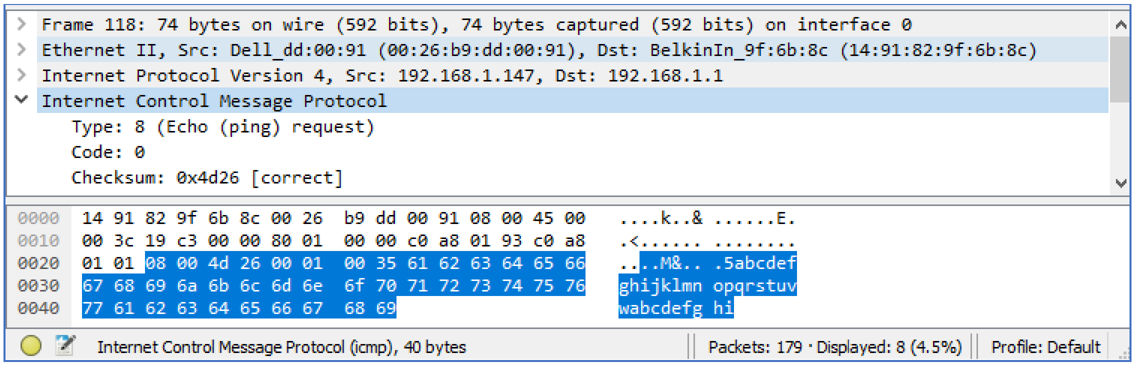
   What is the source IP address?

   - **192.168.1.12**

   What is the destination IP address?

   - **192.168.1.1**

f. You can click any line in the middle section to highlight that part of the frame (hex and ASCII) in the **Packet Bytes** pane (bottom section). Click the **Internet Control Message Protocol** line in the middle section and examine what is highlighted in the **Packet Bytes** pane.



```
> Frame 118: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
> Ethernet II, Src: Dell_dd:00:91 (00:26:b9:dd:00:91), Dst: BelkinIn_9f:6b:8c (14:91:82:9f:6b:8c)
> Internet Protocol Version 4, Src: 192.168.1.147, Dst: 192.168.1.1
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x4d26 [correct]

0000  14 91 82 9f 6b 8c 00 26  b9 dd 00 91 08 00 45 00   ....k..& ......E.
0010  00 3c 19 c3 00 00 80 01  00 00 c0 a8 01 93 c0 a8   .<...... ........
0020  01 01 08 00 4d 26 00 01  00 35 61 62 63 64 65 66   ....M&.. .5abcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67  68 69                     wabcdefg hi

Internet Control Message Protocol (icmp), 40 bytes    Packets: 179 · Displayed: 8 (4.5%)    Profile: Default
```

   What do the last two highlighted octets spell?

   - **“hi”**

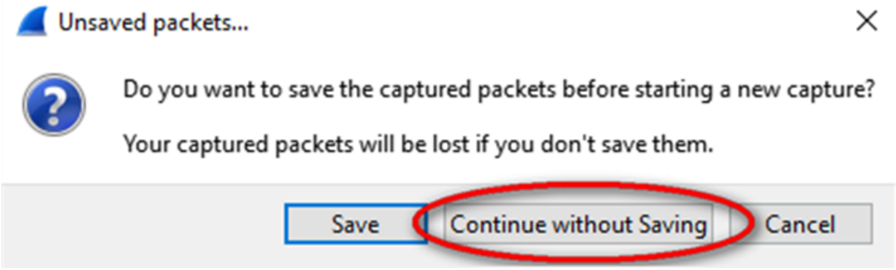
g. Click the next frame in the top section and examine an Echo reply frame. Notice that the source and destination MAC addresses have reversed, because this frame was sent from the default gateway router as a reply to the first ping.

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

   - **Device: IntelCor   MAC: e0 : 9d : 31 : f4 : bf : 32**

Step 7: 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**.



Unsaved packets...

Do you want to save the captured packets before starting a new capture?

Your captured packets will be lost if you don't save them.

Step 8: In the command prompt window, ping <u>www.cisco.com</u>.

Step 9: Stop capturing packets.

Step 10: 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: e0 : 9d : 31 : f4 : bf : 32**
- **Destination: cc : 40 : d0 : 6f : 3d : 69**

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

- **Source: 192.168.1.12**
- **Destination: 96.17.51.173**

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?

- **Destination IP doesn't change because the frame doesn't leave the LAN so the source uses the default gateway MAC address for the frame destination.**

Reflection

Wireshark does not display the preamble field of a frame header. What does the preamble contain?

- **The preamble contains seven octets of alternating 1010 sequences and one octet that signals the frame beginning**

<u>Exercise 3: Using Wireshark to Examine a UDP DNS Capture (9.2.3.5)</u>

If you have ever used the internet, you have used the Domain Name System (DNS). DNS is a distributed network of servers that translates user-friendly domain names like www.google.com to an IP address. When you type a website URL into your browser, your PC performs a DNS query to the DNS server IP address. Your PC DNS server query and the DNS server response make use of the User Datagram

Protocol (UDP) as the transport layer protocol. UDP is connectionless and does not require a session setup as does TCP. DNS queries and responses are very small and do not require the overhead of TCP.

In this exercise, you will communicate with a DNS server by sending a DNS query using the UDP transport protocol. You will use Wireshark to examine the DNS query and response exchanges with the same server.

A. Record a PC's IP Configuration Information

In Part A, you will use the **ipconfig /all** command on your local PC to find and record the MAC and IP addresses of your PC network interface card (NIC), the IP address of the specified default gateway, and the DNS server IP address specified for the PC. Record this information in the table provided. The information will be used in parts of this lab with packet analysis.

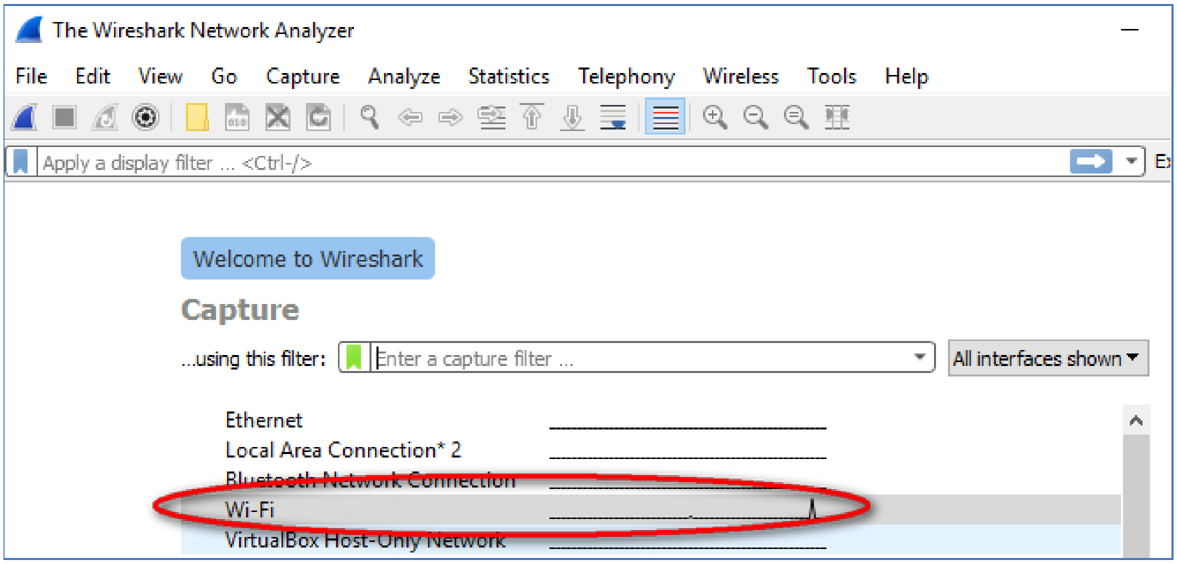
IP address	192.168.1.12
MAC address	e0 : 9d : 31 : f4 : bf : 32
Default gateway IP address	192.168.1.1
DNS server IP address	192.168.1.1

B. Use Wireshark to Capture DNS Queries and Responses

In Part B, you will set up Wireshark to capture DNS query and response packets to demonstrate the use of the UDP transport protocol while communicating with a DNS server.

i. Click the Windows **Start** button and navigate to the Wireshark program.

ii. Select an interface for Wireshark to capture packets. Select (highlight) the active capturing interface.



iii. After selecting the desired interface, click **Start** to capture the packets.

iv. Open a web browser and type **www.google.com**. Press **Enter** to continue.

v. Click **Stop** to stop the Wireshark capture when you see the Google home page.

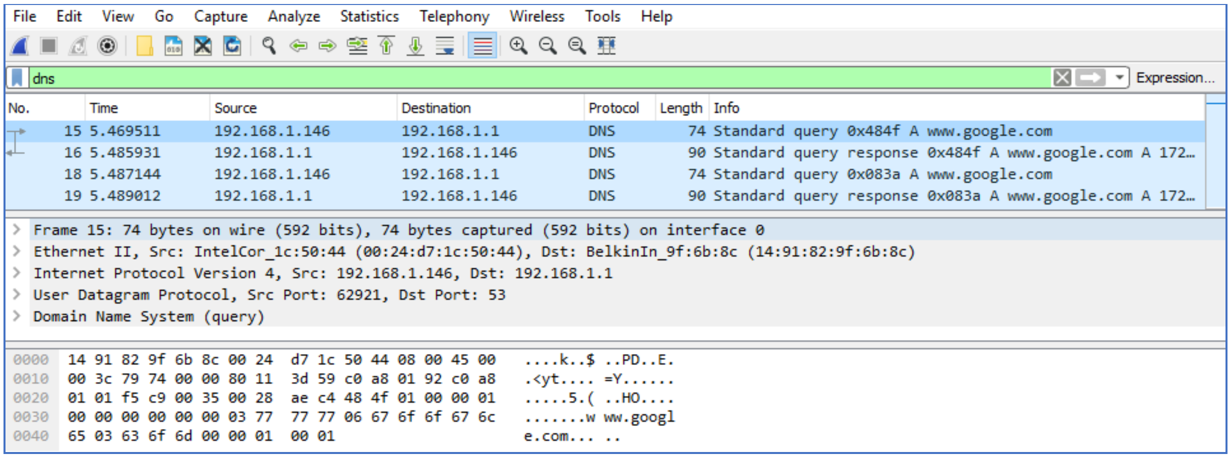
C. Analyze Captured DNS or UDP Packets

In Part C, you will examine the UDP packets that were generated when communicating with a DNS server for the IP addresses for www.google.com.

a. Filter DNS packets.

i. In the Wireshark main window, type **dns** in the entry area of the **Filter** toolbar and press **Enter**.

Note: If you do not see any results after the DNS filter was applied, close the web browser. In the command prompt window, type **ipconfig /flushdns** to remove all previous DNS results. Restart the Wireshark capture and repeat the instructions in Part 2b –2e. If this does not resolve the issue, type **nslookup www.google.com** in the command prompt window as an alternative to the web browser.



dns

```
No.      Time        Source          Destination     Protocol Length Info
      15 5.469511    192.168.1.146   192.168.1.1     DNS          74 Standard query 0x484f A www.google.com
      16 5.485931    192.168.1.1     192.168.1.146   DNS          90 Standard query response 0x484f A www.google.com A 172…
      18 5.487144    192.168.1.146   192.168.1.1     DNS          74 Standard query 0x083a A www.google.com
      19 5.489012    192.168.1.1     192.168.1.146   DNS          90 Standard query response 0x083a A www.google.com A 172…
```

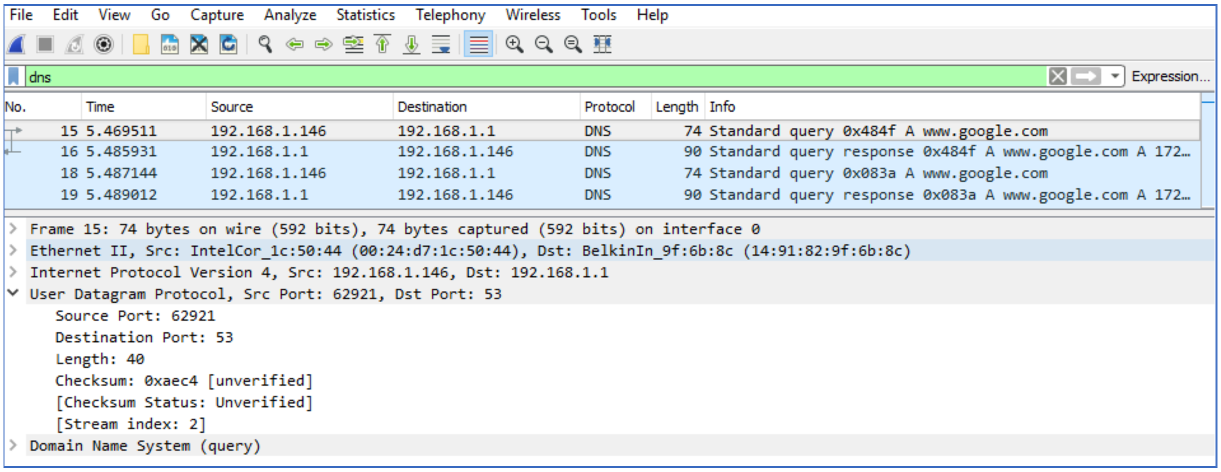
```
> Frame 15: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
> Ethernet II, Src: IntelCor_1c:50:44 (00:24:d7:1c:50:44), Dst: BelkinIn_9f:6b:8c (14:91:82:9f:6b:8c)
> Internet Protocol Version 4, Src: 192.168.1.146, Dst: 192.168.1.1
> User Datagram Protocol, Src Port: 62921, Dst Port: 53
> Domain Name System (query)
```

```
0000  14 91 82 9f 6b 8c 00 24  d7 1c 50 44 08 00 45 00   ....k..$ ..PD..E.
0010  00 3c 79 74 00 00 80 11  3d 59 c0 a8 01 92 c0 a8   .<yt.... =Y......
0020  01 01 f5 c9 00 35 00 28  ae c4 48 4f 01 00 00 01   .....5.( ..HO....
0030  00 00 00 00 00 00 03 77  77 77 06 67 6f 6f 67 6c   .......w ww.googl
0040  65 03 63 6f 6d 00 00 01  00 01                     e.com... ..
```

ii. In the packet list pane (top section) of the main window, locate the packet that includes **Standard query** and **A www.google.com**. See frame 15 as an example.

b. Examine a UDP segment using DNS query.

Examine the UDP by using a DNS query for www.google.com as captured by Wireshark. In this example, Wireshark capture frame 15 in the packet list pane is selected for analysis. The protocols in this query are displayed in the packet details pane (middle section) of the main window. The protocol entries are highlighted in gray.



```
dns
```

```
No.     Time        Source          Destination     Protocol  Length  Info
     15 5.469511    192.168.1.146   192.168.1.1     DNS           74  Standard query 0x484f A www.google.com
     16 5.485931    192.168.1.1     192.168.1.146   DNS           90  Standard query response 0x484f A www.google.com A 172…
     18 5.487144    192.168.1.146   192.168.1.1     DNS           74  Standard query 0x083a A www.google.com
     19 5.489012    192.168.1.1     192.168.1.146   DNS           90  Standard query response 0x083a A www.google.com A 172…
```

```
> Frame 15: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
> Ethernet II, Src: IntelCor_1c:50:44 (00:24:d7:1c:50:44), Dst: BelkinIn_9f:6b:8c (14:91:82:9f:6b:8c)
> Internet Protocol Version 4, Src: 192.168.1.146, Dst: 192.168.1.1
v User Datagram Protocol, Src Port: 62921, Dst Port: 53
    Source Port: 62921
    Destination Port: 53
    Length: 40
    Checksum: 0xaec4 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 2]
> Domain Name System (query)
```

i. In the first line in the packet details pane, frame 15 had 74 bytes of data on the wire. This is the number of bytes to send a DNS query to a name server requesting the IP addresses of www.google.com.

ii. The Ethernet II line displays the source and destination MAC addresses. The source MAC address is from your local PC because your local PC originated the DNS query. The destination MAC address is from the default gateway because this is the last stop before this query exits the local network.

Is the source MAC address the same as the one recorded from Part A for the local PC?

- **Yes**

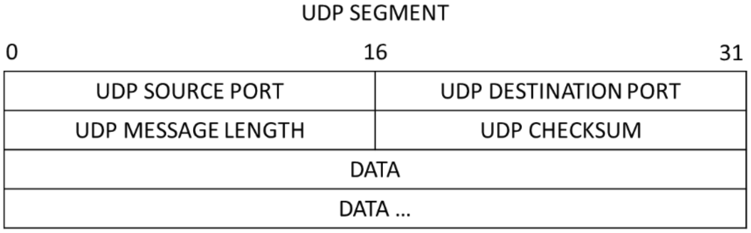
iii. In the Internet Protocol Version 4 line, the IP packet Wireshark capture indicates that the source IP address of this DNS query is 192.168.1.146 and the destination IP address is 192.168.1.1. In this example, the destination address is the default gateway. The router is the default gateway in this network.

Can you identify the IP and MAC addresses for the source and destination devices?

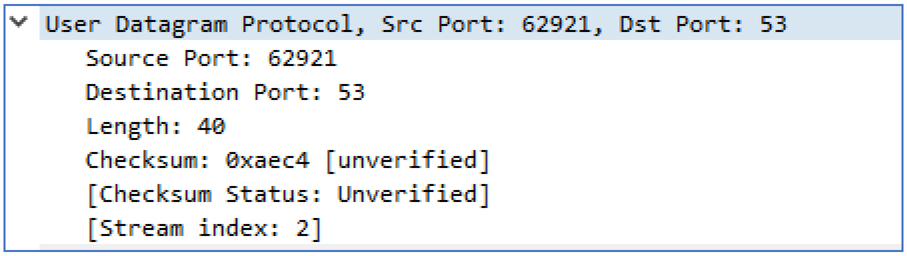
Device	IP Address	MAC Address
Local PC	192.168.1.12	e0 : 9d : 31 : f4 : bf : 32
Default Gateway	192.168.1.1	e0 : 9d : 31 : f4 : bf : 32

The IP packet and header encapsulates the UDP segment. The UDP segment contains the DNS query as the data.

iv. A UDP header only has four fields: source port, destination port, length, and checksum. Each field in a UDP header is only 16 bits as depicted below.

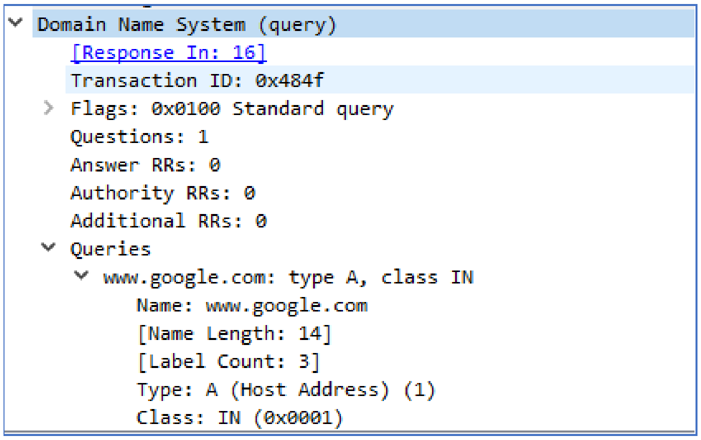


Expand the User Datagram Protocol in the packet details pane by clicking the plus (+) sign. Notice that there are only four fields. The source port number in this example is 60868. The source port was randomly generated by the local PC using port numbers that are not reserved. The destination port is 53. Port 53 is a well-known port reserved for use with DNS. DNS servers listen on port 53 for DNS queries from clients.



```
User Datagram Protocol, Src Port: 62921, Dst Port: 53
    Source Port: 62921
    Destination Port: 53
    Length: 40
    Checksum: 0xaec4 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 2]
```

In this example, the length of the UDP segment is 40 bytes. Out of 40 bytes, 8 bytes are used as the header. The other 32 bytes are used by DNS query data. The 32 bytes of DNS query data is highlighted in the following illustration in the packet bytes pane (lower section) of the Wireshark main window.



```
Domain Name System (query)
    [Response In: 16]
    Transaction ID: 0x484f
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
      v www.google.com: type A, class IN
            Name: www.google.com
            [Name Length: 14]
            [Label Count: 3]
            Type: A (Host Address) (1)
            Class: IN (0x0001)
```

The checksum is used to determine the integrity of the packet after it has traversed the internet.

The UDP header has low overhead because UDP does not have fields that are associated with the three-way handshake in TCP. Any data transfer reliability issues that occur must be handled by the application layer.

Record your Wireshark results in the table below:

Frame size	74 bytes
Source MAC address	e0 : 9d : 31 : f4 : bf : 32
Destination MAC address	cc : 40 : d0 : 6f : 3d : 69
Source IP address	192.168.1.12
Destination IP address	192.168.1.1
Source port	60071
Destination port	53

Is the source IP address the same as the local PC IP address you recorded in Part 1?

- **Yes**

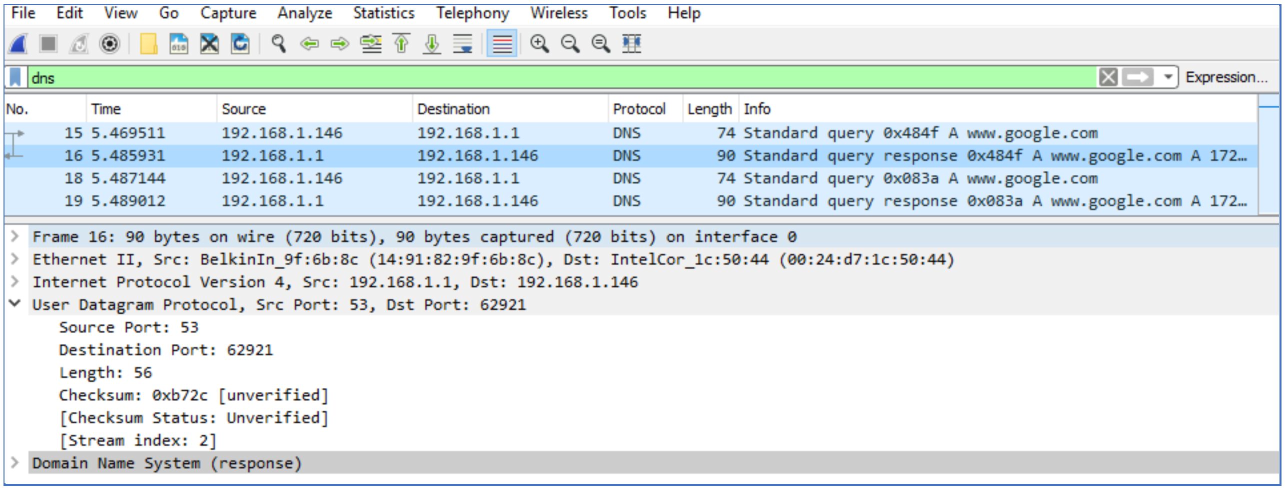
Is the destination IP address the same as the default gateway noted in Part 1?

- **Yes**

c. Examine a UDP using DNS response.

In this step, you will examine the DNS response packet and verify that the DNS response packet also uses the UDP.

i. In this example, frame 16 is the corresponding DNS response packet. Notice the number of bytes on the wire is 90. It is a larger packet compared to the DNS query packet.


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns
Expression...

```
No.   Time        Source          Destination     Protocol Length Info
   15 5.469511    192.168.1.146   192.168.1.1     DNS         74 Standard query 0x484f A www.google.com
   16 5.485931    192.168.1.1     192.168.1.146   DNS         90 Standard query response 0x484f A www.google.com A 172…
   18 5.487144    192.168.1.146   192.168.1.1     DNS         74 Standard query 0x083a A www.google.com
   19 5.489012    192.168.1.1     192.168.1.146   DNS         90 Standard query response 0x083a A www.google.com A 172…
```

```
> Frame 16: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface 0
> Ethernet II, Src: BelkinIn_9f:6b:8c (14:91:82:9f:6b:8c), Dst: IntelCor_1c:50:44 (00:24:d7:1c:50:44)
> Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.146
v User Datagram Protocol, Src Port: 53, Dst Port: 62921
    Source Port: 53
    Destination Port: 62921
    Length: 56
    Checksum: 0xb72c [unverified]
    [Checksum Status: Unverified]
    [Stream index: 2]
> Domain Name System (response)
```

ii. In the Ethernet II frame for the DNS response, what device is the source MAC address and what device is the destination MAC address?

- **Source: Netgear**
- **Destination: IntelCor**

iii. Notice the source and destination IP addresses in the IP packet. What is the destination IP address? What is the source IP address?

- **Destination IP address: 192.168.1.12**
- **Source IP address: 192.168.1.1**

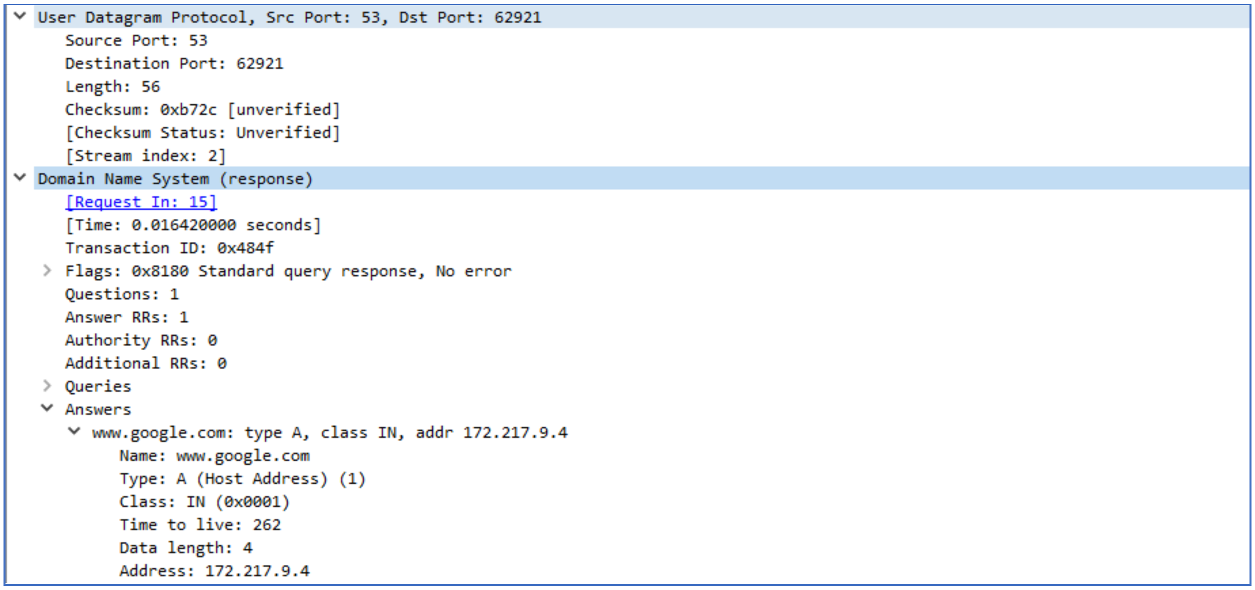
What happened to the roles of source and destination for the local host and default gateway?

- **They reversed roles**

iv. In the UDP segment, the role of the port numbers has also reversed. The destination port number is 62921. Port number 62921 is the same port that was generated by the local PC when the DNS query was sent to the DNS server. Your local PC listens for a DNS response on this port.

The source port number is 53. The DNS server listens for a DNS query on port 53 and then sends a DNS response with a source port number of 53 back to the originator of the DNS query.

When the DNS response is expanded, notice the resolved IP addresses for www.google.com in the **Answers** section.



```
v User Datagram Protocol, Src Port: 53, Dst Port: 62921
    Source Port: 53
    Destination Port: 62921
    Length: 56
    Checksum: 0xb72c [unverified]
    [Checksum Status: Unverified]
    [Stream index: 2]
v Domain Name System (response)
    [Request In: 15]
    [Time: 0.016420000 seconds]
    Transaction ID: 0x484f
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
  > Queries
  v Answers
    v www.google.com: type A, class IN, addr 172.217.9.4
        Name: www.google.com
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 262
        Data length: 4
        Address: 172.217.9.4
```

Reflection

What are the benefits of using UDP instead of TCP as a transport protocol for DNS?

- **UDP is faster and has low overhead**

Part 2: Cisco Packet Tracer

Exercises in this experiment are based on Cisco NetAcad Labs

Background

Packet Tracer is a protocol simulator developed by Cisco Systems. Packet Tracer (PT) is a powerful and dynamic tool that displays the various protocols used in networking, in either Real Time or Simulation mode. This includes layer 2 protocols such as Ethernet and PPP, layer 3 protocols such as IP, ICMP, and ARP, and layer 4 protocols such as TCP and UDP. Routing protocols can also be traced.

Exercise 4: Packet Tracer - Help and Navigation Tips (1.2.4.4)

In this exercise, you will explore a relatively complex network that highlights a few of Packet Tracer's features. While doing so, you will learn how to access Help and the tutorials. You will learn how to switch between various modes and workspaces. You may need to adjust the window size of Packet Tracer to see the full network. If necessary, you can use the zoom in and out tools to adjust the size of the Packet Tracer window.

> **Note**: It is not important that you understand everything you see and do in this activity. Feel free to explore the network on your own. If you wish to proceed more systematically, follow the steps below. Answer the questions to the best of your ability.

a. Access the Packet Tracer Help pages, tutorial videos, and online resources

i. Access the Packet Tracer Help pages in two ways:

- o Click the question mark icon in the top, right-hand corner of the menu toolbar.
- o Click the Help menu, and then choose Contents.

ii. Access the Packet Tracer tutorial videos by clicking **Help** > **Tutorials**. These videos are a visual demonstration of the information found in the **Help** pages and various aspects of the Packet Tracer software program. Before proceeding with this activity, you should gain some familiarity with the Packet Tracer interface and Simulation mode.

1. View the **Interface Overview** video in the **Getting Started** section of Tutorials.
2. View the **Simulation Environment** video in the **Realtime** and **Simulation Modes** section of **Tutorials**.

iii. Find the "Configuring Devices Using the Desktop Tab" tutorial. Watch the first part of the tutorial and answer the following question: What information can you configure in the IP Configuration window?

- ● You can configure the IP address, Subnet Mask, Default Gateway, and DNS Server.

b. Toggle between Realtime and Simulation modes.

i. Find the word **Realtime** in the bottom right corner of the Packet Tracer interface. In Realtime mode, your network is always running like a real network, whether or not you are working on the network. Your configurations are performed in real time, and the network responds in near real time.

ii. Click the tab directly behind the **Realtime** tab to switch to **Simulation** mode. In Simulation mode, you can watch your network run at a slower pace, observing the paths that data takes, and inspecting the data packets in detail.

iii. In the Simulation Panel, click **Auto Capture / Play**. You should now see data packets, represented as envelopes of various colors, traveling between the devices.

iv. Click **Auto Capture / Play** again to pause the simulation.

v. Click **Capture / Forward** to step through the simulation. Click the button a few more times to see the effect.

vi. In the network topology on the left, click one of the envelopes on an intermediary device and investigate what is inside. Throughout this lab, you will learn the meaning of most everything inside these envelopes. For now, see if you can answer the following questions:

- o Under the **OSI Model tab**, how many **In Layers** and **Out Layers** have information?
    - ▪ Layer 1 for both In and Out Layers
- o Under the **Inbound PDU Details** and **Outbound PDU Details** tabs, what are the headings of the main sections?
    - ▪ Inbound: Ethernet II, IP, ICMP, Variable Size
    - ▪ Outbound: Ethernet II, IP, ICMP, Variable Size
- o Click back and forth between the **Inbound PDU Details** and **Outbound PDU Details** tabs. Do you see information changing? If so, what?
    - ▪ The source and destination addresses are changing

vii. Click the toggle button above **Simulation** in the bottom right corner to return to **Realtime** mode.

c. Toggle between Logical and Physical views.

i. Find the word **Logical** in the top left corner of the Packet Tracer interface. You are currently in the Logical workspace where you will spend the majority of your time building, configuring, investigating, and troubleshooting networks.

Note: Although you can add a geographical map as the background image for the Logical workspace, it does not usually have any relationship to the actual physical location of devices.

ii. Click the tab below **Logical** to switch to the **Physical** workspace. The purpose of the Physical workspace is to give a physical dimension to your Logical network topology. It gives you a sense of scale and placement (how your network might look in a real environment).

iii. During this lab, you will use this workspace on occasion. For now, just know that it is available for you to use. To learn more about the Physical workspace, refer to the Help files and tutorial videos.

iv. Click the toggle button below **Physical** in the top right corner to return to the **Logical** workspace.

- Open a new instance of Packet Tracer. Create a new network with at least two LANs connected by a WAN. Connect all the devices. Investigate the original Packet Tracer activity to see what else you might need to do to make your new network functional. Record your thoughts and save your Packet Tracer file. You may want to revisit your network later after you have mastered a few more skills.

Exercise 5: Packet Tracer – Network Representation (1.2.4.5)

a. **Identify common components of a network as represented in Packet Tracer.**

i. The icon toolbar at the bottom left hand corner has various categories of networking components. You should see categories that correspond to intermediary devices, end devices, and media. The **Connections** category (with the lightning bolt icon) represents the networking media supported by Packet Tracer. There is also an **End Devices** category and two categories specific to Packet Tracer: **Custom Made Devices** and **Multiuser Connection**.

ii. List the intermediary device categories.

- **Routers, Switches, Hubs, Wireless Devices, and WAN Emulation**

iii. Without entering into the Internet cloud or Intranet cloud, how many icons in the topology represent endpoint devices (only one connection leading to them)? 15

iv. Without counting the two clouds, how many icons in the topology represent intermediary devices (multiple connections leading to them)? 11

v. How many end devices are **not** desktop computers? 8

vi. How many different types of media connections are used in this network topology? 4

b. **Explain the purpose of the devices.**

1. In Packet Tracer, only the Server-PT device can act as a server. Desktop or Laptop PCs cannot act as a server. Based on your studies so far, explain the client-server model.
   - **Servers enable hosts to provide information and services to other hosts on the network. Clients are hosts that enable them to request and display the information obtained from the server. Each has specialized software to allow for these services.**
2. List at least two functions of intermediary devices.
   - **They can allow or deny the flow of information, or they can maintain pathways within a network.**
3. List at least two criteria for choosing a network media type.
   - **Speed and size of transmission and the cost of installation and maintenance.**

c. **Compare and contrast LANs and WANs.**

i. Explain the difference between a LAN and a WAN. Give examples of each.

- **Local Area Network is a private network that consists of shorter range areas such as within a particular room or a building. Wide Area Network is a large range network to connect devices from different geographical areas over thousands of kilometers.**

ii. In the Packet Tracer network, how many WANs do you see?

- **Two**

iii. How many LANs do you see?

- **Three**

iv. The Internet in this Packet Tracer network is overly simplified and does not represent the structure and form of the real Internet. Briefly describe the Internet.

- **The internet is a global network of interconnected devices continuously communicating with one another in smaller intranet networks.**

v. What are some of the common ways a home user connects to the Internet?

- **One can use a variety of devices, such as the mobile phone, laptop, or desktop computer via cable, dial-up, satellite, or DSL**

vi. What are some common methods that businesses use to connect to the Internet in your area?

- **Businesses can usually use the same methods such as DSL, cable, satellite, or more specialized methods such as dedicated leased line**