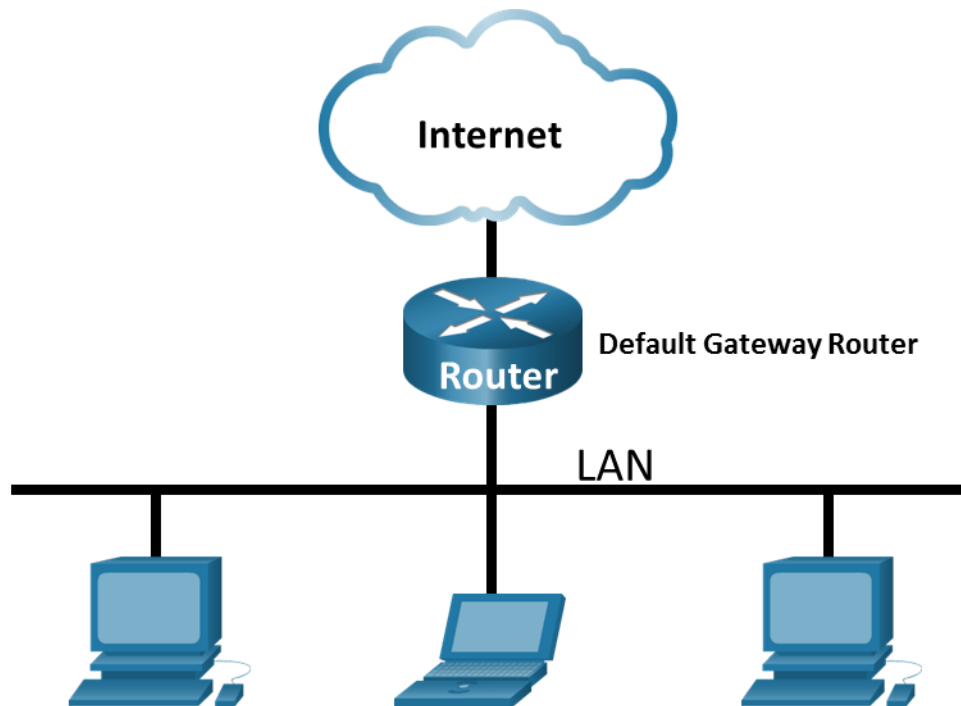


## Lab - Use Wireshark to View Network Traffic Topology



### Objectives

Part 1: Capture and Analyze Local ICMP Data in Wireshark

Part 2: Capture and Analyze Remote ICMP Data in Wireshark

### Background / Scenario

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 RFC or other specifications.

Wireshark is a useful tool for anyone working with networks and can be used with most labs for data analysis and troubleshooting. In this lab, you will use Wireshark to capture ICMP data packet IP addresses and MAC addresses.

### Required Resources

- 1 PC (Windows with internet access)
- Additional PCs on a local-area network (LAN) will be used to reply to ping requests.

### Instructions

---

## Part 1: Capture and Analyze Local ICMP Data in Wireshark

In Part 1 of this lab, 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. In a command prompt window, enter **ipconfig /all**, to the IP address of your PC interface, its description, and its MAC (physical) address.

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

```
Windows IP Configuration
```

```
Host Name . . . . . : DESKTOP-NB48BTC
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. . . . . : No
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
```

```
<output omitted>
```

- b. 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. Navigate to Wireshark. Double-click the desired interface to start the packet capture. Make sure the desired interface has traffic.
- b. Information will start scrolling down the top section in Wireshark. The data lines will appear in different colors based on protocol.

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 the **Apply** button (arrow sign) to view only ICMP (ping) PDUs.

- c. This filter causes all data in the top window to disappear, but you are still capturing the traffic on the interface. Navigate to a command prompt window and ping the IP address that you received from your team member.

```
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=128

Reply from 192.168.1.114: bytes=32 time<1ms TTL=128

Reply from 192.168.1.114: bytes=32 time<1ms TTL=128

Reply from 192.168.1.114: bytes=32 time<1ms TTL=128

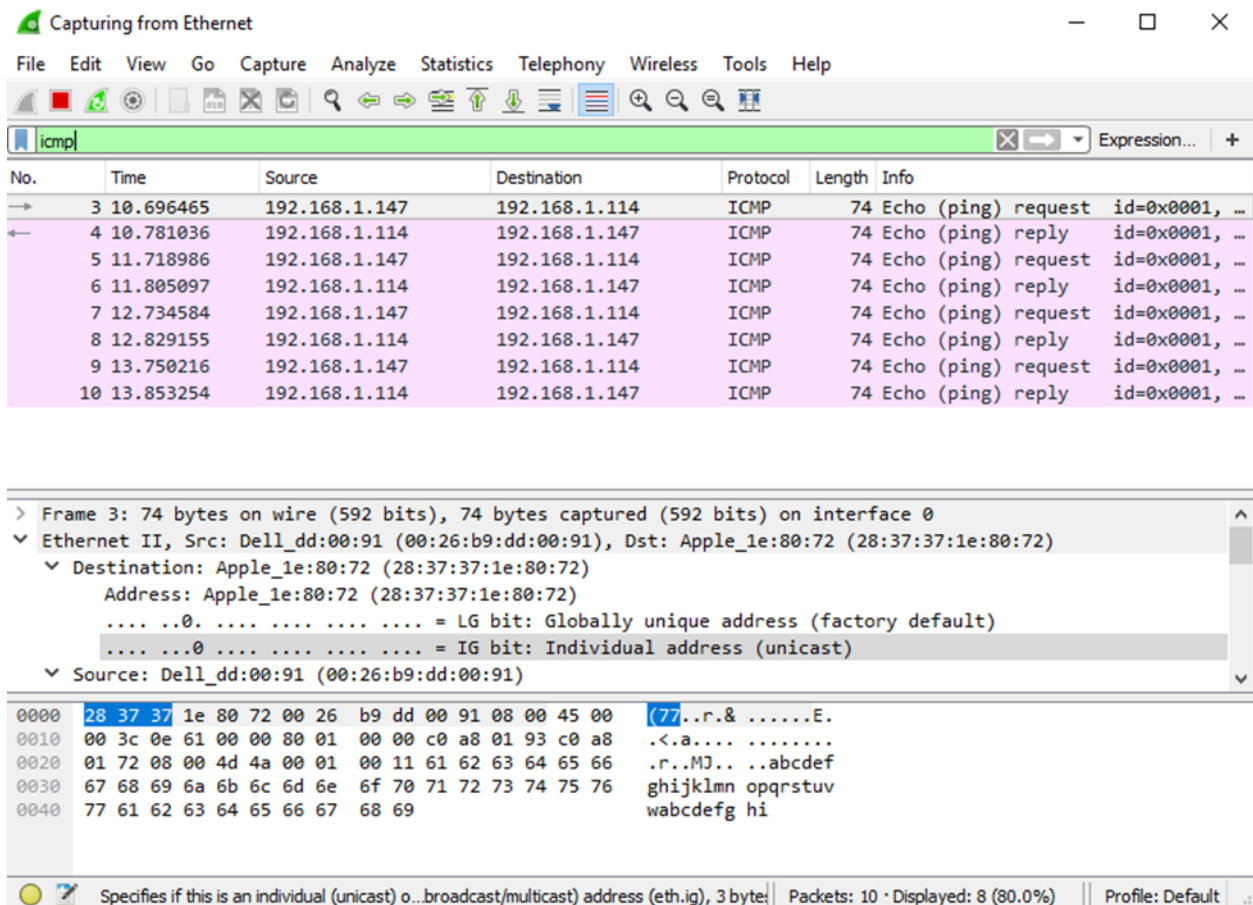
Ping statistics for 192.168.1.114:

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.



The screenshot shows the Wireshark interface with the filter 'icmp' applied. The packet list shows 10 ICMP Echo (ping) requests and replies between 192.168.1.147 and 192.168.1.114. The packet details pane for the selected packet (No. 3) shows the Ethernet II header and the ICMP Echo (ping) request details. The packet bytes pane shows the raw data in hexadecimal and ASCII.

| 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)

Destination: Apple\_1e:80:72 (28:37:37:1e:80:72)

Address: Apple\_1e:80:72 (28:37:37:1e:80:72)

.... ..0. .... = LG bit: Globally unique address (factory default)

.... ..0. .... = IG bit: Individual address (unicast)

Source: Dell\_dd:00:91 (00:26:b9:dd:00:91)

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 wabcedfg hi

Specifies if this is an individual (unicast) o...broadcast/multicast address (eth.ig), 3 bytes | Packets: 10 · Displayed: 8 (80.0%) | Profile: Default

- d. Stop capturing data by clicking the **Stop Capture** icon.

### 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.

- 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.
- 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.

Does the source MAC address match your PC interface?

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

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

## Part 2: Capture and Analyze Remote ICMP Data in Wireshark

In Part 2, 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 Part 1.

### Step 1: Start capturing data on the interface.

- a. Start the data capture again.
- b. 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**.
- c. With the capture active, ping the following three website URLs from a Windows command prompt:

1) www.yahoo.com

2) www.cisco.com

3) www.google.com

**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.

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

### Step 2: Examining and analyzing the data from the remote hosts.

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.

IP address for **www.yahoo.com**:

*Type your answers here.*

MAC address for **www.yahoo.com**:

*Type your answers here.*

IP address for **www.cisco.com**:

*Type your answers here.*

---

MAC address for **www.cisco.com**:

***Type your answers here.***

IP address for **www.google.com**:

***Type your answers here.***

MAC address for **www.google.com**:

***Type your answers here.***

What is significant about this information?

***Type your answers here.***

How does this information differ from the local ping information you received in Part 1?

***Type your answers here.***

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

***Type your answers here.***