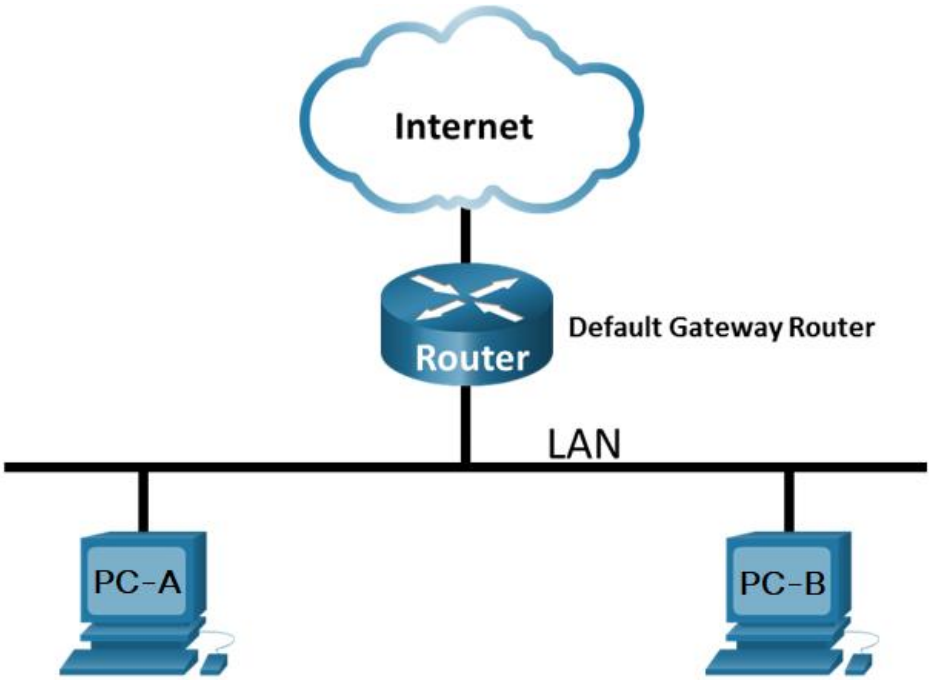
Lab 3.7.10 - Use Wireshark to View Network Traffic

This lab has been updated for use on NETLAB+.
www.netdevgroup.com

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 in the CCNA courses for data analysis and troubleshooting. In this lab, you will use Wireshark to capture ICMP data packet IP addresses and Ethernet frame MAC addresses. The Internet connection is simulated in the Netlab environment.

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.

Before moving on to *Step 1*, please wait 7-8 minutes so that the *Default Gateway Router* has enough time to fully initialize after bootup. If you are not receiving a DHCP address in *Step 1*, that means more time is needed for the router to finish booting up.

Step 1: Retrieve your PC interface addresses.

For this lab, you can utilize both PC-A and PC-B for use. Click on PC-A and then you will need to retrieve your PC IP address and its network interface card (NIC) physical address, also called the MAC address. The IP address on either PC-A or PC-B will be provided via DHCP.

In a command prompt window, enter **ipconfig /all**, to the IP address of your PC interface, its description, and its MAC (physical) address. If a 169.254.x.x address exists, use **ipconfig /renew "network_adapter_name"** on the PC (since the PC may have more than one network adapter attached, issue the *ipconfig* command by specifying the network adapter, for example, "**ipconfig /renew Ethernet**".

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

Windows IP Configuration

   Host Name . . . . . . . . . . . . : MDP-PC-A
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) PRO/1000 MT Network Connection
   Physical Address. . . . . . . . . :00-50-56-A4-2C-94
   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
<output omitted>
```

b. Click on PC-B and use the ipconfig command to record the IP address provided to the 2nd PC.

Step 2: Start Wireshark and begin capturing data.

a. On PC-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.

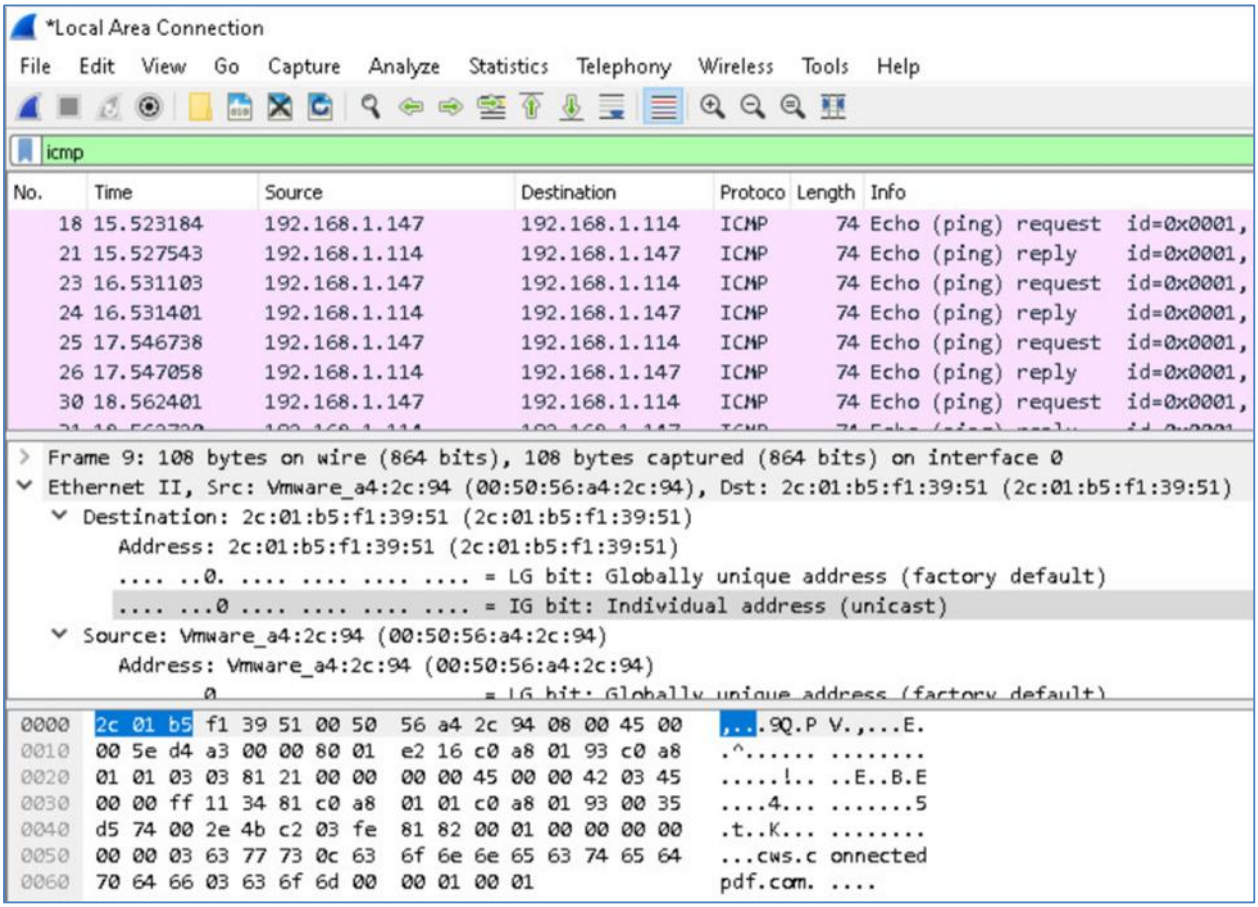
c. This filter causes all data in the top window to disappear, but you are still capturing the traffic on the interface. Navigate to a command prompt window and ping the IP address of PC-B.

```
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.



Note: If PC-B does not reply to your pings, this may be because the PC firewall 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.

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 to PC-B. 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 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?

Type your answers here.

Yes

Does the destination MAC address in Wireshark match PC-B's MAC address?

Type your answers here.

Yes

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

Type your answers here.

MAC addresses are 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.

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.

98.137.246.7

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

Type your answers here.

4C-71-0D-42-CB-61

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

Type your answers here.

96.7.79.147

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

Type your answers here.

4C-71-0D-42-CB-61

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

Type your answers here.

172.217.14.100

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

Type your answers here.

4C-71-0D-42-CB-61

What is significant about this information?

Type your answers here.

All 3 MAC addresses are the same.

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

Type your answers here.

The local pings in part one used the MAC address of the PC's NIC, while pinging a host outside of the network used the MAC address of the default gateway's NIC.

Reflection Question

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

The MAC addresses of remote hosts are not known to the local devices. The MAC addresses of the default gateway are used instead, then the Layer 2 information is stripped and the MAC address of the next router is added. This process repeats for each hop until it reaches the destination IP.

Appendix A: Allowing ICMP Traffic Through a Firewall

If PC-B is unable to ping your PC, the firewall may be blocking those requests. This appendix describes how to create a rule in the firewall to allow ping requests. It also describes how to disable the new ICMP rule after you have completed the lab.

Part 1: Create a new inbound rule allowing ICMP traffic through the firewall.

a. Navigate to the **Control Panel** and click the **System and Security** option in the Category view.

b. In the **System and Security** window, click **Windows Defender Firewall** or **Windows Firewall**.

c. In the left pane of the **Windows Defender Firewall** or **Windows Firewall** window, click **Advanced settings**.

d. On the **Advanced Security** window, click the **Inbound Rules** option on the left sidebar and then click **New Rule…** on the right sidebar.

e. This launches the **New Inbound Rule** wizard. On the **Rule Type** screen, click the **Custom** radio button and click **Next**.

f. In the left pane, click the **Protocol and Ports** option and using the **Protocol Type** drop-down menu, select **ICMPv4**, and then click **Next**.

g. Verify that **Any IP address** for both the local and remote IP addresses are selected. Click **Next** to continue.

h. Select **Allow the connection**. Click **Next** to continue.

i. By default, this rule applies to all the profiles. Click **Next** to continue.

j. Name the rule **Allow ICMP Requests**. Click **Finish** to continue. This new rule should allow your PC-B to receive ping replies from your PC.

Part 2: Disabling or deleting the new ICMP rule.

After the lab is complete, you may want to disable or even delete the new rule you created in Step 1. Using the **Disable Rule** option allows you to enable the rule again at a later date. Deleting the rule permanently deletes it from the list of inbound rules.

a. On the **Advanced Security** window, click **Inbound Rules** in the left pane and then locate the rule you created previously.

b. Right-click the ICMP rule and select **Disable Rule** if so desired. You may also select **Delete** if you want to permanently delete it. If you choose this option, you must re-create the rule again to allow ICMP replies.

Router and Switch Interface Summary Table

Router / Switch Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2960	Fast Ethernet 0/1 (F0/1)	Fast Ethernet 0/2 (F0/2)	n/a	n/a
3560	Fast Ethernet 0/1 (F0/1)	Fast Ethernet 0/2 (F0/2)	n/a	n/a
3650	Gigabit Ethernet 1/0/1 (G1/0/1)	Gigabit Ethernet 1/0/2 (G1/0/2)	n/a	n/a
4221	Gigabit Ethernet 0/0/0 (G0/0/0)	Gigabit Ethernet 0/0/1 (G0/0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
4300	Gigabit Ethernet 0/0/0 (G0/0/0)	Gigabit Ethernet 0/0/1 (G0/0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)

Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and Serial interfaces in the device. The table does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.