



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

Applied Computing

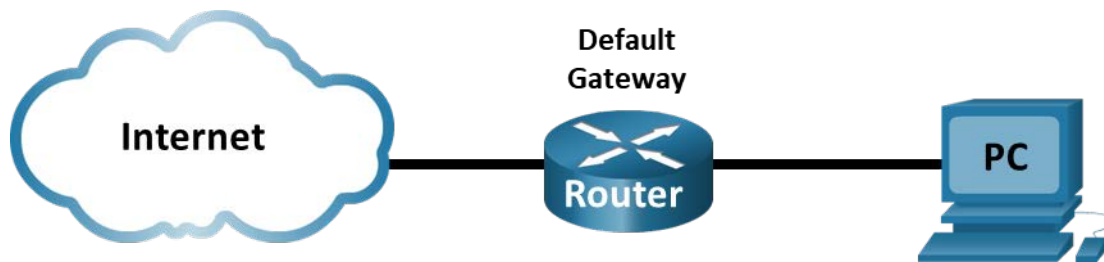
Wales Institute of Science and Art (WISA)

Advanced Networking (ACCA5024)

Lab 2: Analyse Network Packets

Cisco | **Networking Academy**[®]
| **Mind Wide Open**[™]

Topology



Objectives

Part 1: Capture and Analyze Local ICMP Data in Wireshark

Part 2: Capture and Analyze Remote ICMP Data in Wireshark

Part 3: Examine the Header Fields in an Ethernet II Frame

Part 4: Use Wireshark to Capture and Analyze Ethernet Frames

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 for data analysis and troubleshooting. 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 use Wireshark to capture ICMP data packet IP addresses and Ethernet frame MAC addresses. You will review the fields contained in an Ethernet II frame and use Wireshark to capture and analyze Ethernet II frame header fields for local and remote traffic.

Required Resources

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

Warning

Using a packet sniffer such as Wireshark may be considered a breach of the security policy of organizations. It is recommended that permission be obtained before running Wireshark for this lab. If using a packet sniffer such as Wireshark is an issue, Please contact the Lecturer.

Instructions

Prerequisite: Download and install Wireshark <https://www.wireshark.org/#download>

PART 1

Capture and Analyze Local ICMP Data in Wireshark

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.

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.

- 1) 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>
```

- 2) 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. Alternatively, you could use other Laptops or End devices which are connected to your home network. (If practicing this lab from home)

Start Wireshark and begin capturing data.

- 3) Navigate to Wireshark. Double-click the desired interface to start the packet capture. Make sure the desired interface has traffic.
- 4) 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.

- 5) 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

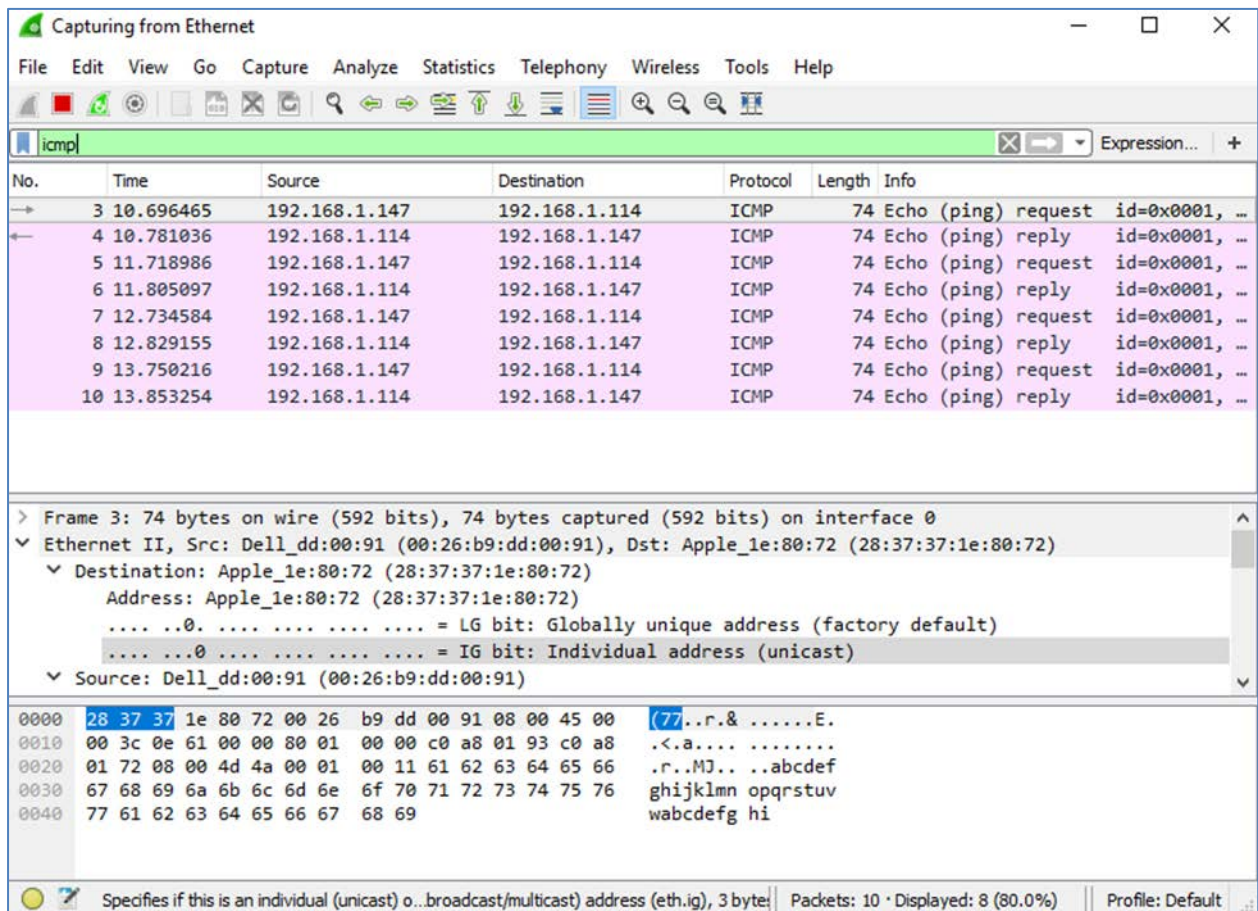
Ping statistics for 192.168.1.114:

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.



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.

6) Stop capturing data by clicking the **Stop Capture** icon.

Examine the captured data.

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;
 - 3) The bottom section displays the raw data of each layer. The raw data is displayed in both hexadecimal and decimal form.
- 7) 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.

- 8) 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.

Record your reflection:

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?

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.

Start capturing data on the interface.

- 9) Start the data capture again.
- 10) 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**.
- 11) 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.
- 12) You can stop capturing data by clicking the **Stop Capture** icon.

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.

Record your reflection:

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

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

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

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

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

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

What is significant about this information?

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

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

PART 3

Examine the Header Fields in an Ethernet II Frame

Examine the header fields and content in an Ethernet II frame. A Wireshark capture will be used to examine the contents in those fields.

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

Examine the network configuration of the PC.

In this example, this PC host IP address is 192.168.1.147 and the default gateway has an IP address of 192.168.1.1.

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

```
Ethernet adapter Ethernet:
```

```
Connection-specific DNS Suffix . :
```

```
Description . . . . . : Intel(R) 82579LM Gigabit Network Connection
```

```
Physical Address. . . . . : F0-1F-AF-50-FD-C8
```

```
DHCP Enabled. . . . . : Yes
```

```
Autoconfiguration Enabled . . . . : Yes
```

```
Link-local IPv6 Address . . . . . : fe80::58c5:45f2:7e5e:29c2%11(Preferred)
```

```
IPv4 Address. . . . . : 192.168.1.147(Preferred)
```

```
Subnet Mask . . . . . : 255.255.255.0
```

```
Lease Obtained. . . . . : Friday, September 6, 2019 11:08:36 AM
```

```
Lease Expires . . . . . : Saturday, September 7, 2019 11:08:36 AM
```

```
Default Gateway . . . . . : 192.168.1.1
```

```
DHCP Server . . . . . : 192.168.1.1
```

```
<output omitted>
```

Examine Ethernet frames in a Wireshark capture.

The screenshots of 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. ARP stands for address resolution protocol. ARP is a communication protocol that is used for determining the MAC address that is associated with the IP address. The session begins with an ARP query and reply for the MAC address of the gateway router, followed by four ping requests and replies.

This screenshot highlights the frame details for an ARP request.

Wireshark interface showing an ARP request frame (Frame 65). The packet list shows frame 65 as an ARP request from Dell_50:fd:c8 to Broadcast. The packet details pane shows Ethernet II, ARP, and Address Resolution Protocol (request) fields. The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
65	12.995821	Dell_50:fd:c8	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.147
66	12.996247	Netgear_99:c5:72	Dell_50:fd:c8	ARP	60	192.168.1.1 is at 30:46:9a:99:c5:72
72	19.346624	192.168.1.147	192.168.1.1	ICMP	74	Echo (ping) request id=0x0001, seq=81/2
73	19.346931	192.168.1.1	192.168.1.147	ICMP	74	Echo (ping) reply id=0x0001, seq=81/2
74	20.356540	192.168.1.147	192.168.1.1	ICMP	74	Echo (ping) request id=0x0001, seq=82/2
75	20.356880	192.168.1.1	192.168.1.147	ICMP	74	Echo (ping) reply id=0x0001, seq=82/2
76	21.367689	192.168.1.147	192.168.1.1	ICMP	74	Echo (ping) request id=0x0001, seq=83/2
77	21.368063	192.168.1.1	192.168.1.147	ICMP	74	Echo (ping) reply id=0x0001, seq=83/2

Frame 65: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0

Ethernet II, Src: Dell_50:fd:c8 (f0:1f:af:50:fd:c8), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

Destination: Broadcast (ff:ff:ff:ff:ff:ff)

Source: Dell_50:fd:c8 (f0:1f:af:50:fd:c8)

Type: ARP (0x0806)

Address Resolution Protocol (request)

Hardware type: Ethernet (1)

Protocol type: IPv4 (0x0800)

Hardware size: 6

Protocol size: 4

0000 ff ff ff ff ff ff f0 1f af 50 fd c8 08 06 00 01 P.....

0010 08 00 06 04 00 01 f0 1f af 50 fd c8 c0 a8 01 93 P.....

0020 00 00 00 00 00 00 c0 a8 01 01 P.....

Frame (frame), 42 bytes

Packets: 85 · Displayed: 13 (15.3%) · Dropped: 0 (0.0%) · Profile: Default

This screenshot highlights the frame details for an ARP reply.

Wireshark interface showing an ARP reply frame (Frame 66). The packet list shows frame 66 as an ARP reply from Netgear_99:c5:72 to Dell_50:fd:c8. The packet details pane shows Ethernet II, ARP, and Address Resolution Protocol (reply) fields. The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
65	12.995821	Dell_50:fd:c8	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.147
66	12.996247	Netgear_99:c5:72	Dell_50:fd:c8	ARP	60	192.168.1.1 is at 30:46:9a:99:c5:72
72	19.346624	192.168.1.147	192.168.1.1	ICMP	74	Echo (ping) request id=0x0001, seq=81/2
73	19.346931	192.168.1.1	192.168.1.147	ICMP	74	Echo (ping) reply id=0x0001, seq=81/2
74	20.356540	192.168.1.147	192.168.1.1	ICMP	74	Echo (ping) request id=0x0001, seq=82/2
75	20.356880	192.168.1.1	192.168.1.147	ICMP	74	Echo (ping) reply id=0x0001, seq=82/2
76	21.367689	192.168.1.147	192.168.1.1	ICMP	74	Echo (ping) request id=0x0001, seq=83/2
77	21.368063	192.168.1.1	192.168.1.147	ICMP	74	Echo (ping) reply id=0x0001, seq=83/2

Frame 66: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0

Ethernet II, Src: Netgear_99:c5:72 (30:46:9a:99:c5:72), Dst: Dell_50:fd:c8 (f0:1f:af:50:fd:c8)

Destination: Dell_50:fd:c8 (f0:1f:af:50:fd:c8)

Source: Netgear_99:c5:72 (30:46:9a:99:c5:72)

Type: ARP (0x0806)

Padding: 00000000000000000000000000000000c4a798ec

Address Resolution Protocol (reply)

Hardware type: Ethernet (1)

Protocol type: IPv4 (0x0800)

Hardware size: 6

0000 f0 1f af 50 fd c8 30 46 9a 99 c5 72 08 06 00 01 P...0F.....

0010 08 00 06 04 00 02 30 46 9a 99 c5 72 c0 a8 01 01 0F.....

0020 f0 1f af 50 fd c8 c0 a8 01 93 00 00 00 00 00 00 P.....

0030 00 00 00 00 00 00 00 00 c4 a7 98 ec

Frame (frame), 60 bytes

Packets: 85 · Displayed: 13 (15.3%) · Dropped: 0 (0.0%) · Profile: Default

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.						
Source Address	Netgear_99:c5:72 (30:46:9a:99:c5:72)	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.						
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 these: <table><tr><th>Value</th><th>Description</th></tr><tr><td>0x0800</td><td>IPv4 Protocol</td></tr><tr><td>0x0806</td><td>Address Resolution Protocol (ARP)</td></tr></table>	Value	Description	0x0800	IPv4 Protocol	0x0806	Address Resolution Protocol (ARP)
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 device, encompassing frame addresses, type, and data field. It is verified by the receiver.						

Record your reflection:

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 NIC in the ARP reply?

What portion of the MAC address is the OUI?

What is the NIC serial number of the source?

PART 4

Use Wireshark to Capture and Analyze Ethernet Frames

Use Wireshark to capture local and remote Ethernet frames. You will then examine the information that is contained in the frame header fields.

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?

Start capturing traffic on your PC NIC.

Open Wireshark to start data capture. Observe the traffic that appears in the packet list window.

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 you want 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.*

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 have already recorded.

Stop capturing traffic on the NIC.

Click the **Stop Capturing Packets** icon to stop capturing traffic.

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 previously, Wireshark should display the ICMP information in the packet list pane of Wireshark.

In the packet list pane (top section), click the first frame listed. You should see **Echo (ping) request** under the **Info** heading. The line should now be highlighted.

Examine the first line in the packet details pane (middle section). This line displays the length of the frame.

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

Record your reflection:

What is the MAC address of the PC NIC?

What is the default gateway's MAC address?

You can click the greater than (>) sign at the beginning of the second line to obtain more information about the Ethernet II frame.

What type of frame is displayed?

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?

*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*

What do the last two highlighted octets spell?

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?

Capture packets for a remote host.

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**.

In a command prompt window, ping www.cisco.com.

Stop capturing packets. Examine the new data in the packet list pane of Wireshark.

Record your reflection:

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 already. 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?

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

APPENDIX

A: Allowing ICMP Traffic through a Firewall

If the members of your team are unable to ping your PC/ or if you can't successfully ping a device in your home network, 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.

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

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

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

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

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

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

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

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

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

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

Name the rule with **Allow ICMP Requests**. Click **Finish** to continue. This new rule should allow your team members to receive ping replies from your PC.

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 previously. 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.

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

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.