LABORATORY 7: TRANSPORT LAYER PROTOCLS

Objectives

By the end of the laboratory, students will be able to

- capture IP packets and observe the Transport Layer information.
- verify the port number of various Application Layer services.

Introduction:

Internet applications use IP packets to carry data. In most cases, a computer will be having multiple internet communication sessions going on simultaneously. In order to ensure that the incoming IP packet to a computer is directed to the correct process, a method is needed to identify the intended recipient of the IP packet. This information is carried by the Transport Layer header's Destination Port field. When a host receives an IP packet (Layer 3), it strips off the IP Packet header and reveals the Transport Layer data segment. The Destination Port field in the Transport Layer header indicates the process supposed to receive this data segment.

Port numbers are 16-bit unsigned binary numbers, giving the range of 0 to 65535. Some port numbers, known as "Well-Known" port numbers, are reserved for widely used services. These numbers are generally used as the destination port number by a client sending a request to a server passively waiting for incoming request carrying that port number. For example, web servers wait for incoming TCP data segment with Destination Port number of 80, as TCP Port 80 has been reserved for HTTP service.

The Source Port number is generally ephemeral and is mainly meant for directing the reply to the process that originated the outgoing data segment. When a process at the sending host sends out a data segment, the Source Port field carries the port number of the process, with the Destination Port field carrying the port number of the intended recipient process at the remote receiving host. When the remote host replies, the Source Port number and the Destination Port number are swapped. Hence, for the returned data segment, the Destination Port now points to the originating process at the local host. This ensures that the data segment is directed to the correct process.

There are two main Transport Layer protocols: TCP and UDP. TCP is meant for connection-oriented, reliable transmission. It is feature-rich but slow compared to UDP, due to the need of acknowledgement from the communication hosts. UDP is meant for applications where speed is a main concern. UDP is fast as it does not wait for acknowledgement, which makes it unreliable as compared to TCP. The choice of using TCP or UDP depends on the application. For example, TELNET, FTP and HTPP use TCP, while DNS and VoIP use UDP.

Equipment:

Windows OS laptops with Cisco Packet Tracer installed.

Procedures:

1. Construction and Configuration of a Computer Network for observing Transport Layer protocols.

1.1 Construct the network shown in Figure 7.1.

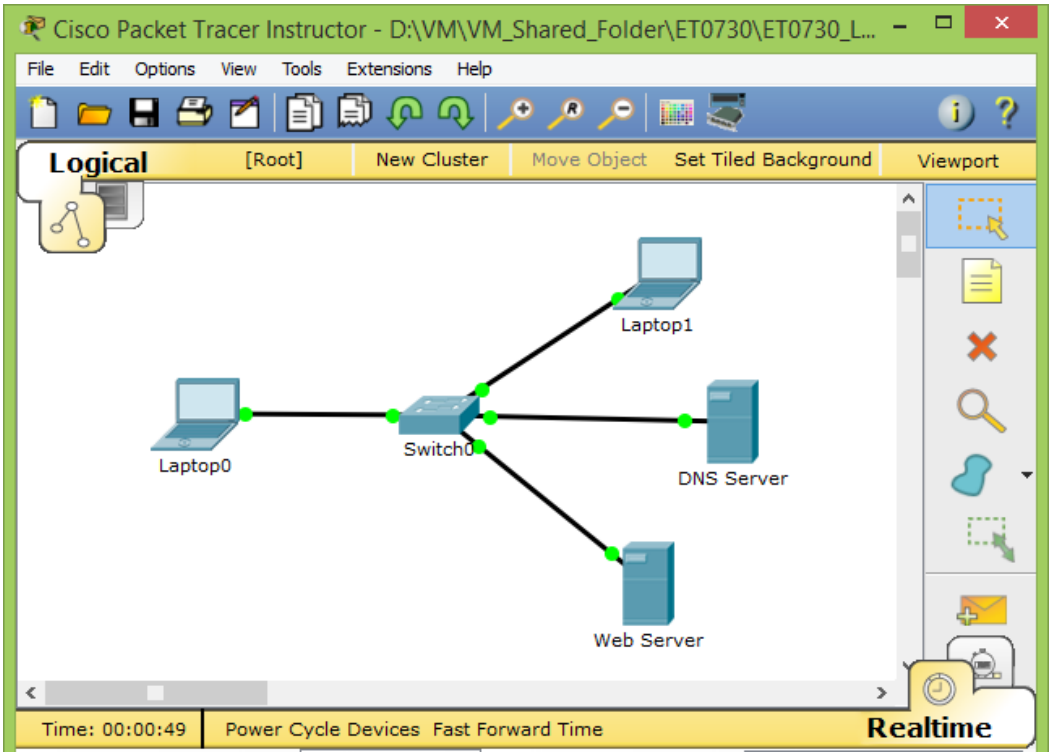

Figure 7.1 - A network for observing Transport layer protocols.

Device	IP Address	Subnet Mask
Laptop0	192.168.1.101	255.255.255.0
Laptop1	192.168.1.102	255.255.255.0
DNS Server	192.168.1.150	255.255.255.0
Web Server	192.168.1.200	255.255.255.0

Table 7.1 – Network configuration parameters for Figure 7.1.

1.2 Configure the laptops and servers interfaces with parameters as shown in Table 7.1.

1.3 Verify connectivity among all the laptops and servers.

1.4 Click on Laptop0 and select the "Config" tab. In the textbox next to "DNS Server", enter the IP address of the DNS Server (i.e. 192.168.1.150). This informs Laptop0 about the DNS server to be contacted for DNS name resolution.

2. Configuration of DNS Server.

2.1 Configure the DNS server by carrying out the following steps.

2.1.1 Click on DNS Server.

2.1.2 Click “Services” → “DNS”.

2.1.3 Click the “On” radio button next to “DNS Service”. This activates the DNS service on the DNS server.

2.1.4 In the textbox of “Name”, enter www.CompanyA.com. In the textbox of “Address”, enter 192.168.1.200 (i.e. the IP address of the Web Server). Figure 7.2 shows the entries to be made.

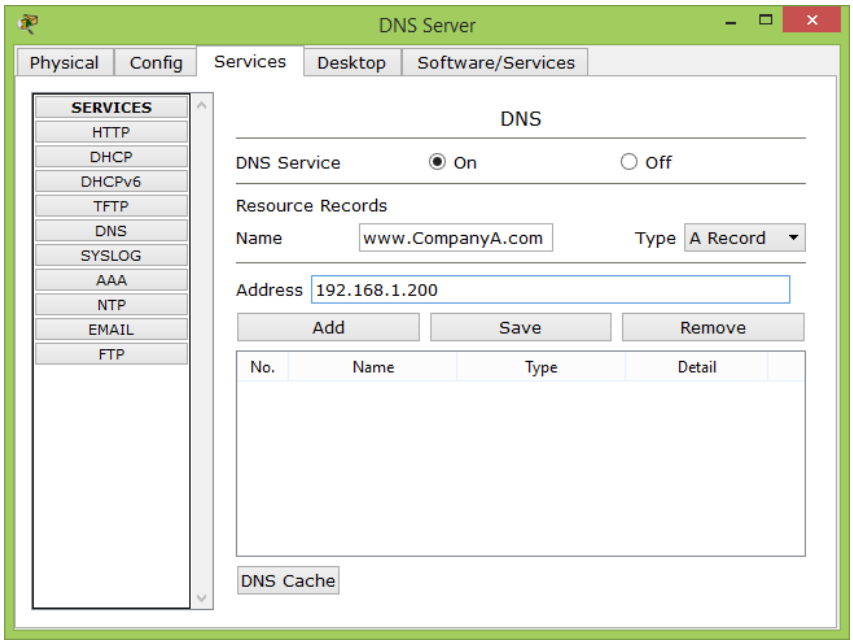

Figure 7.2 – Adding an entry to the DNS database.

2.1.5 Click the “Add” button. A new entry will be added to the table below. The domain name will be in lowercase. This is fine since DNS service is not case-sensitive.

3. Configuration of Web Server.

3.1 Configure the Web server by carrying out the following steps.

3.1.1 Click on Web Server.

3.1.2 Click “Services” → “HTTP”.

3.1.3 Make sure that the “On” radio button next to “HTTP” is selected. This activates the HTTP service on the Web server.

4. Observe Transport Layer of the DNS Service.

4.1 Switch the Packet Tracer to “Simulation Mode”.

4.2 Click the “Show All/None” button once. This de-selects all protocols.

4.3 Click the “Edit Filters” button, then select “Ipv4” tab. Put a tick in the box next to “DNS”. The rest should not be selected.

4.4 Click on the “Misc” tab, then put a tick in the box next to “HTTP”. The rest should not be selected.

4.5 Click somewhere else to close the “Edit Filters” window.

4.6 Click on Laptop0. Select the “Desktop” tab, then select “Web Browser”.

4.7 Enter ***www.CompanyA.com*** in the URL textbox. Click the “Go” button.

4.8 Minimise the Laptop0 window. You should see a DNS packet appearing at Laptop0.

4.9 At the Simulation Panel, click the “Info” box of “DNS” type. Figure 7.3 shows the “Info” box of “DNS” type to be clicked. A window showing the PDU information will pop up, as shown in Figure 7.4.

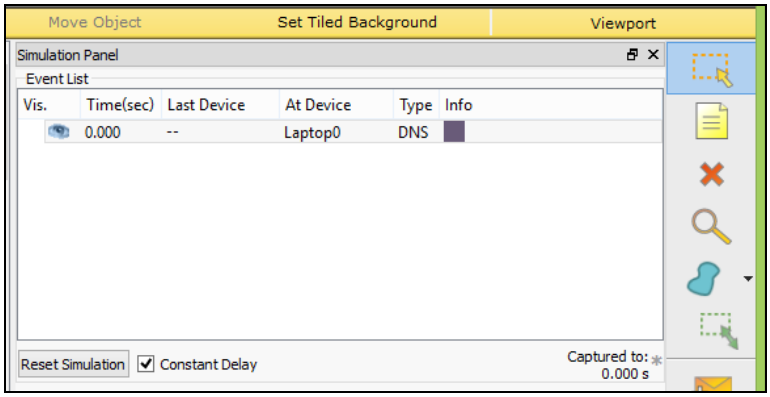

Figure 7.3 – DNS info box representing the DNS Query.

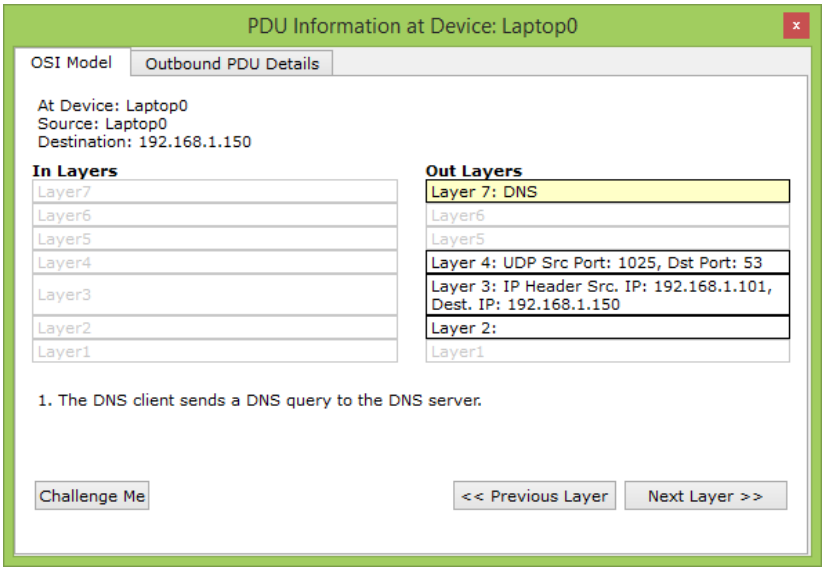

Figure 7.4 – PDU information of the DNS Query.

4.10 Click on “Layer 7: DNS” of the “Out Layers” column (right-hand-side). A message appears at lower part of the window. The message should be showing “**1. The DNS client sends a DNS query to the DNS server.**”.

Question:

By checking “Layer 4” of the “Out Layers” column, find the answer for the following:

Transport Layer Protocol for “DNS”:

Source Port:

Destination Port:

4.11 Click the “Capture/Forward” button 3 times. The DNS Query packet will arrive at the DNS server. Click on the “DNS” info box.

4.12 Click on “Layer 7: DNS” of the “Out Layers” column (right-hand-side). A message appears at lower part of the window. Record this message.

4.13 Observe “Layer 4” of both the “In Layers” and “Out Layers”. You should see what Figure 7.5 shows.

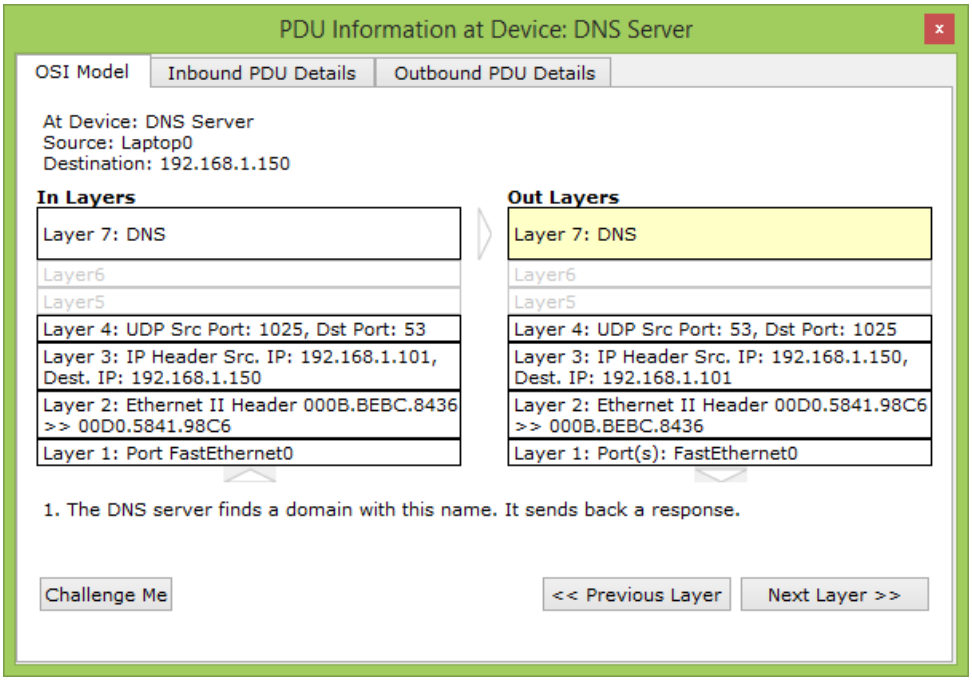

Figure 7.5 – PDU information of the DNS reply.

4.14 Compare the “Layer 4” of “In Layers” and “Out Layers”. Pay attention to the Source Port and Destination Port.

Question:

Do you notice that the Source Port and Destination Port numbers have been swapped? Can you explain this?

5. Observe Transport Layer of the Web (HTTP) Service.

5.1 Click the "Capture/Forward" button several times until a "HTTP" packet appears at Laptop0. This is the HTTP Request to be sent to the Web Server.

5.2 At the Simulation Panel, click the "Info" box of "HTTP" type. Figure 7.6 shows the "Info" box of "HTTP" type to be clicked. A window showing the PDU information will pop up, as shown in Figure 7.7.

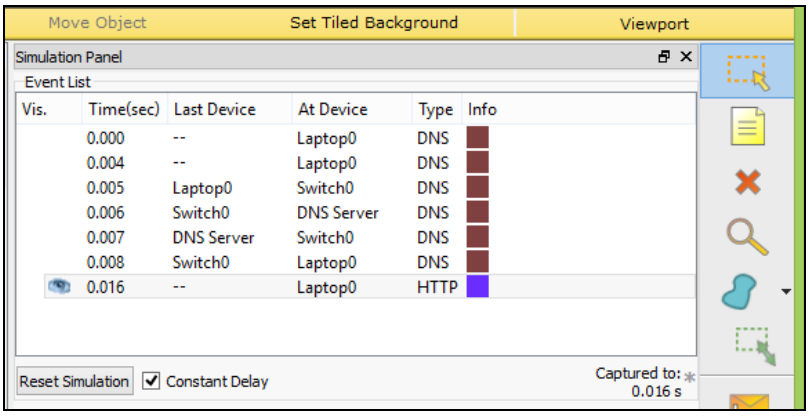

Figure 7.6 – HTTP info box representing the HTTP request.

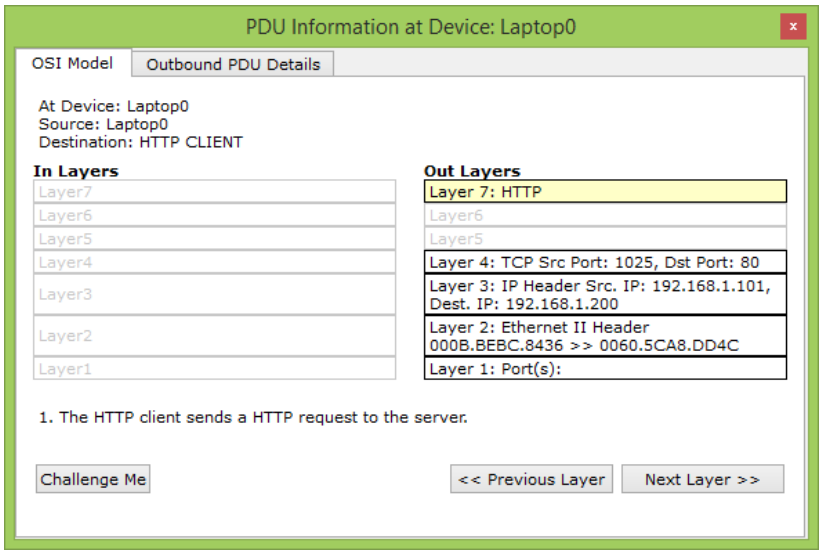

Figure 7.7 – PDU information of the DNS Query.

5.3 Click on “Layer 7: HTTP” of the “Out Layers” column (right-hand-side). A message appears at lower part of the window. Record this message.

Question:

By checking “Layer 4” of the “Out Layers” column, find the answer for the following:

Transport Layer Protocol for “HTTP”:

Source Port:

Destination Port:

5.4 Click the “Capture/Forward” button 3 times. The HTTP request packet will arrive at the Web server. Click on the “HTTP” info box.

5.5 Click on “Layer 7: HTTP” of the “Out Layers” column (right-hand-side). A message appears at lower part of the window. Record this message.

5.6 Observe “Layer 4” of both the “In Layers” and “Out Layers”. You should see what Figure 7.8 shows.

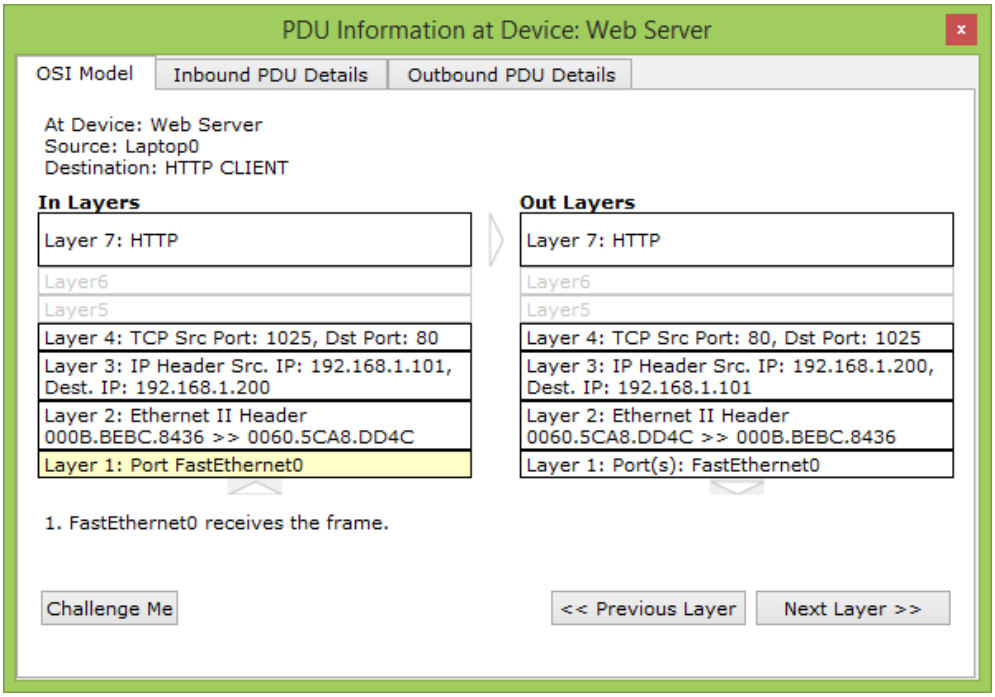

Figure 7.8 – PDU information of the HTTP reply.

5.7 Compare the “Layer 4” of “In Layers” and “Out Layers”. Pay attention to the Source Port and Destination Port.

Question:

Do you also notice that the Source Port and Destination Port numbers have been swapped? If you receive an IP packet with the Transport Layer‘s Source Port carrying value of 80, from what server does that IP packet come from?

5.8 Click the “Capture/Play” button until the HTTP reply packet returns to Laptop0.

5.9 Click on the last “HTTP” info box.

5.10 Click on “Layer 7: HTTP” of the “In Layers” column (left-hand-side). Observe “Layer 4”. What is the Source Port number? Does it agree with what you predicted in Step 5.7?

6. Observe ICMP message (ping).

6.1 Click the “Reset Simulation” button to clear the simulation panel.

6.2 Click the “Edit Filters” button, then select “Ipv4” tab. Remove the tick in the box next to “DNS”. Put a tick in the box next to “ICMP”. The rest should not be selected.

6.3 Click on the “Misc” tab, then remove the tick in the box next to “HTTP”. None should be selected in this window.

6.4 Click somewhere else to close the “Edit Filters” window.

6.5 Click on Laptop0. Select the “Desktop” tab. Close the “Web Browser” window.

6.6 Still selecting the “Desktop” tab, click “Command Prompt”.

6.7 Ping Laptop1 from Laptop0 (i.e. `ping 192.168.1.102`).

6.8 Minimise the Laptop0 window. You should see an ICMP packet appearing at Laptop0.

6.9 At the Simulation Panel, click the “Info” box of “ICMP” type. Figure 7.9 shows the “Info” box of “ICMP” type to be clicked. A window showing the PDU information will pop up, as shown in Figure 7.10.

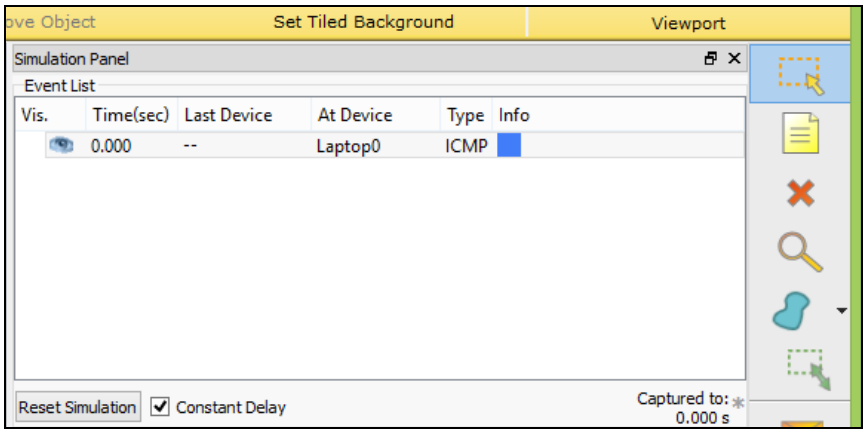

Figure 7.9 – ICMP info box representing the ICMP Echo Request message.

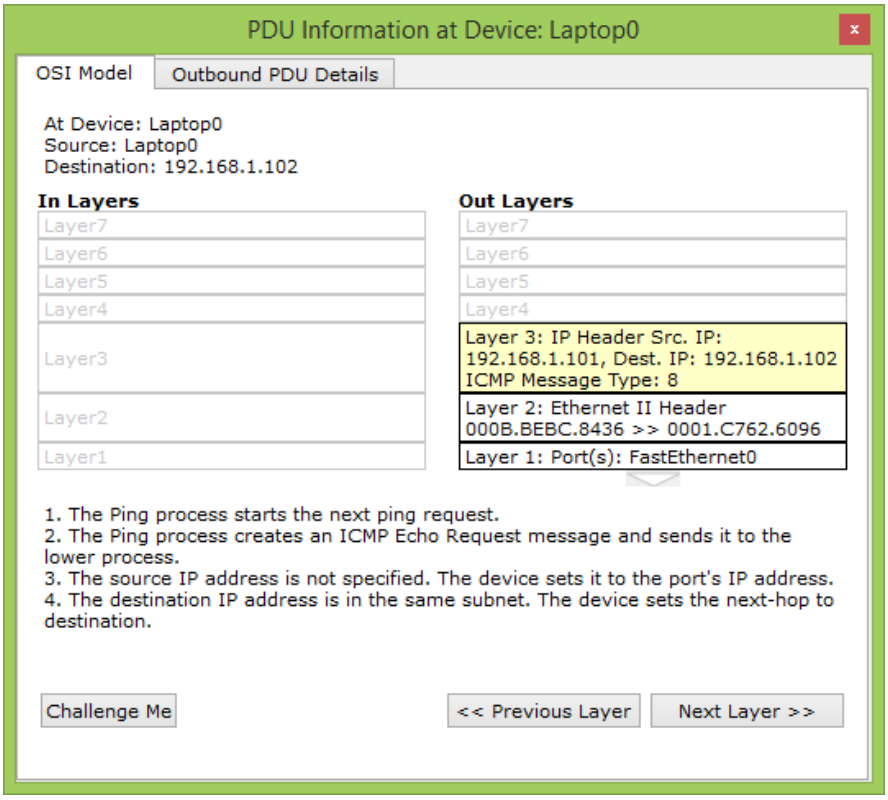

Figure 7.10 – PDU information of the ICMP Echo Request message.

6.10 Observe the “Out Layers” column (right-hand-side).

Question:

Do you see any information displayed under Layers 4 to 7? Can you explain why?