Week 1: Packet Tracer – Investigate the TCP/IP and OSI Models in Action.

Report by: Tonny Odhiambo, CS-CNS06-24028

Introduction

This simulation activity is intended to provide a foundation for understanding the TCP/IP protocol suite and the relationship to the OSI model. Simulation mode allows you to view the data contents being sent across the network at each layer.

As data moves through the network, it is broken down into smaller pieces and identified so that the pieces can be put back together when they arrive at the destination. Each piece is assigned a specific name (protocol data unit [PDU]) and associated with a specific layer of the TCP/IP and OSI models. Packet Tracer simulation mode enables you to view each of the layers and the associated PDU. The following steps lead the user through the process of requesting a web page from a web server by using the web browser application available on a client PC.

Even though much of the information displayed will be discussed in more detail later, this is an opportunity to explore the functionality of Packet Tracer and be able to visualize the encapsulation process.

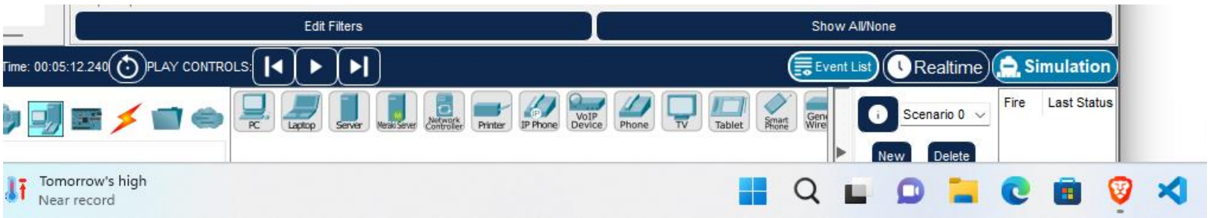
Objectives

- **Part 1: Examine HTTP Web Traffic**
- **Part 2: Display Elements of the TCP/IP Protocol Suite**

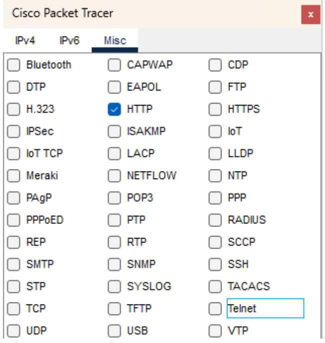
Part 1: Examine HTTP Web Traffic

Step 1: Switch from Realtime to Simulation mode.

a) Switched to simulation mode.



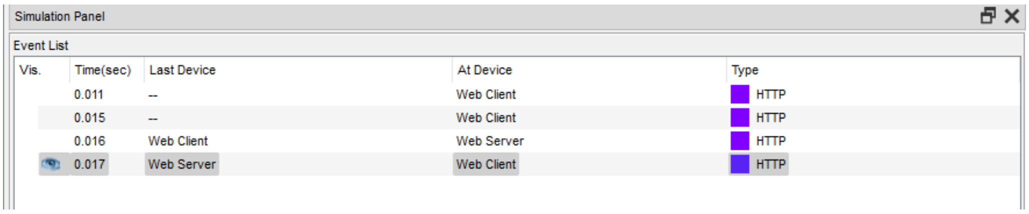
b) Selected HTTP from the Event List Filters.


Cisco Packet Tracer

IPv4 IPv6 Misc

☐ Bluetooth	☐ CAPWAP	☐ CDP
☐ DTP	☐ EAPOL	☐ FTP
☐ H.323	☑ HTTP	☐ HTTPS
☐ IPSec	☐ ISAKMP	☐ IoT
☐ IoT TCP	☐ LACP	☐ LLDP
☐ Meraki	☐ NETFLOW	☐ NTP
☐ PAgP	☐ POP3	☐ PPP
☐ PPPoED	☐ PTP	☐ RADIUS
☐ REP	☐ RTP	☐ SCCP
☐ SMTP	☐ SNMP	☐ SSH
☐ STP	☐ SYSLOG	☐ TACACS
☐ TCP	☐ TFTP	☐ Telnet
☐ UDP	☐ USB	☐ VTP

Step 2: Generate web (HTTP) traffic.

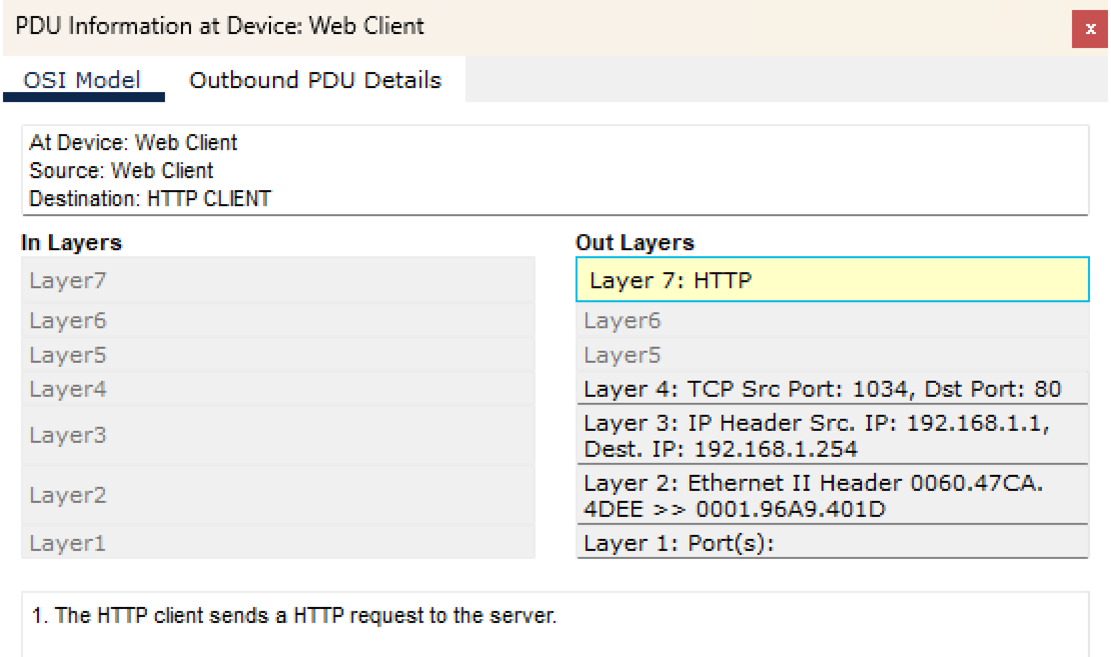


Simulation Panel

Event List

Vis.	Time(sec)	Last Device	At Device	Type
	0.011	--	Web Client	■ HTTP
	0.015	--	Web Client	■ HTTP
	0.016	Web Client	Web Server	■ HTTP
👁	0.017	Web Server	Web Client	■ HTTP

Selected the OSI Model tab and clicked layer 7 and displayed the information listed in the numbered steps i.e., The HTTP client sends a HTTP request to the server.



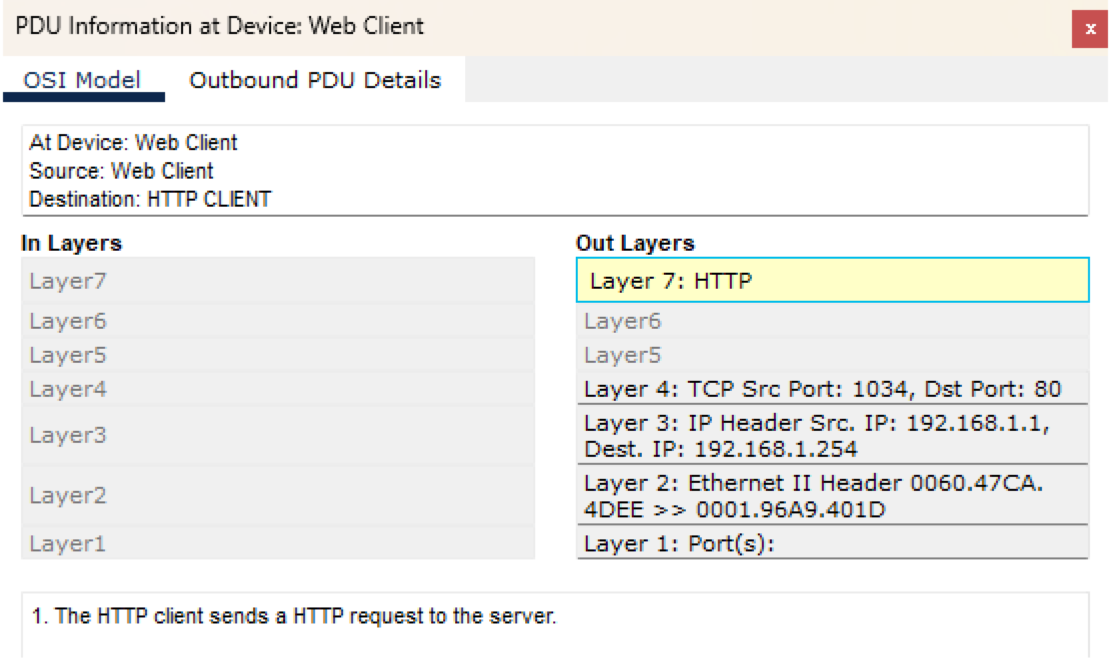
PDU Information at Device: Web Client

At Device: Web Client
Source: Web Client
Destination: HTTP CLIENT

In Layers	Out Layers
Layer7	Layer 7: HTTP
Layer6	Layer6
Layer5	Layer5
Layer4	Layer 4: TCP Src Port: 1034, Dst Port: 80
Layer3	Layer 3: IP Header Src. IP: 192.168.1.1, Dest. IP: 192.168.1.254
Layer2	Layer 2: Ethernet II Header 0060.47CA.4DEE >> 0001.96A9.401D
Layer1	Layer 1: Port(s):

1. The HTTP client sends a HTTP request to the server.

The Dst Port value for Layer 4 under the Out Layers column is 80 and the Dest. IP value for Layer 3 under the Out Layers column is 192.168.1.254



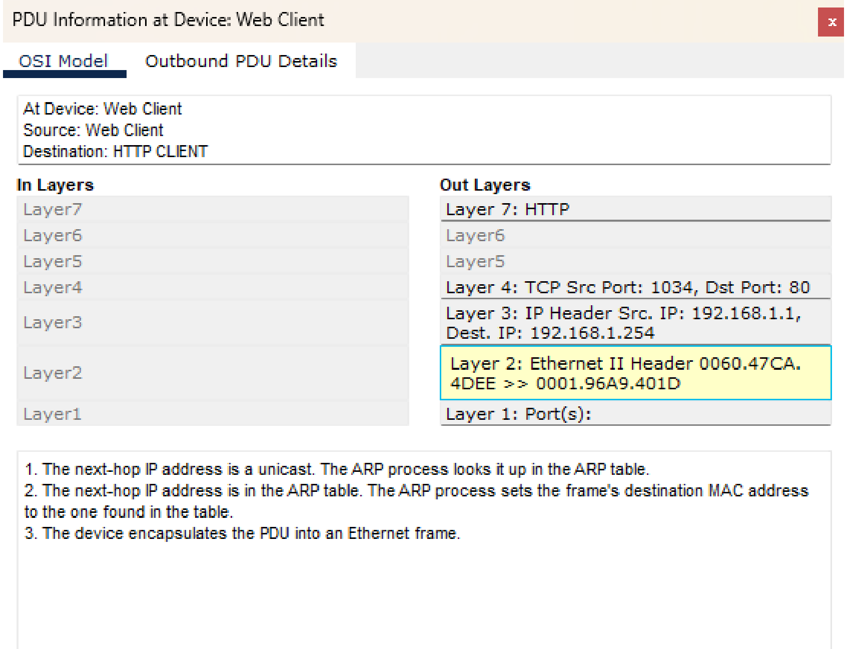
PDU Information at Device: Web Client

At Device: Web Client
Source: Web Client
Destination: HTTP CLIENT

In Layers	Out Layers
Layer7	Layer 7: HTTP
Layer6	Layer6
Layer5	Layer5
Layer4	Layer 4: TCP Src Port: 1034, Dst Port: 80
Layer3	Layer 3: IP Header Src. IP: 192.168.1.1, Dest. IP: 192.168.1.254
Layer2	Layer 2: Ethernet II Header 0060.47CA.4DEE >> 0001.96A9.401D
Layer1	Layer 1: Port(s):

1. The HTTP client sends a HTTP request to the server.

The information displayed at Layer 2 under the Out Layers column is Ethernet II Header 0060.47CA.4DEE >> 0001.96A9.401D

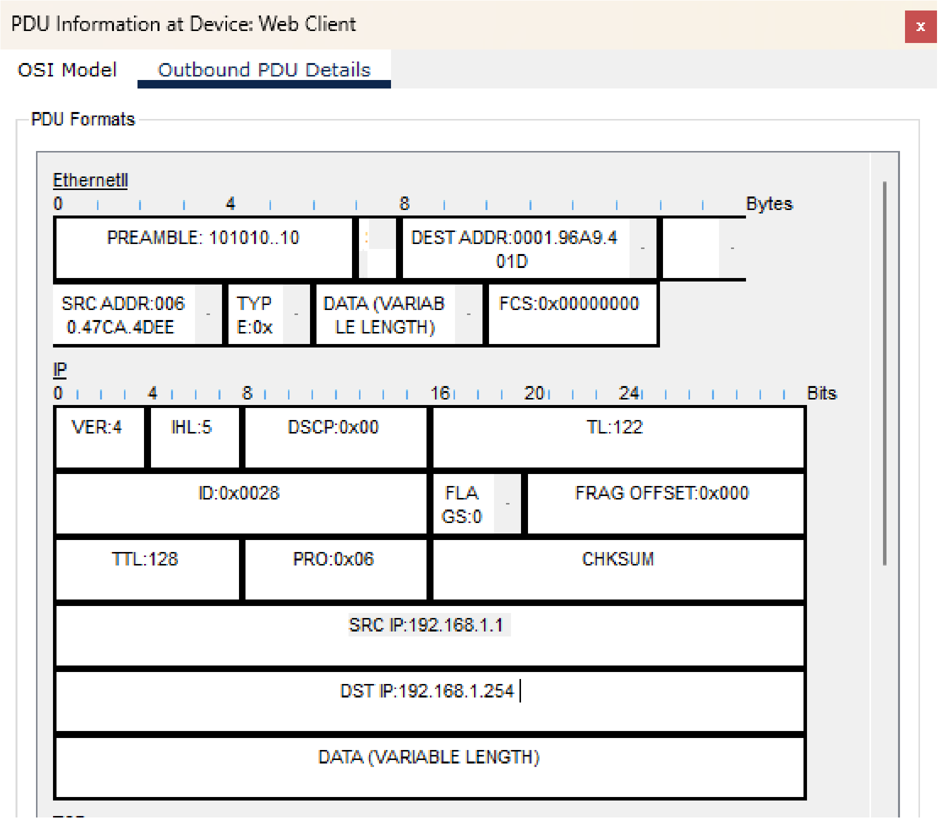

PDU Information at Device: Web Client

At Device: Web Client
Source: Web Client
Destination: HTTP CLIENT

In Layers	Out Layers
Layer7	Layer 7: HTTP
Layer6	Layer6
Layer5	Layer5
Layer4	Layer 4: TCP Src Port: 1034, Dst Port: 80
Layer3	Layer 3: IP Header Src. IP: 192.168.1.1, Dest. IP: 192.168.1.254
Layer2	Layer 2: Ethernet II Header 0060.47CA.4DEE >> 0001.96A9.401D
Layer1	Layer 1: Port(s):

1. The next-hop IP address is a unicast. The ARP process looks it up in the ARP table.
2. The next-hop IP address is in the ARP table. The ARP process sets the frame's destination MAC address to the one found in the table.
3. The device encapsulates the PDU into an Ethernet frame.

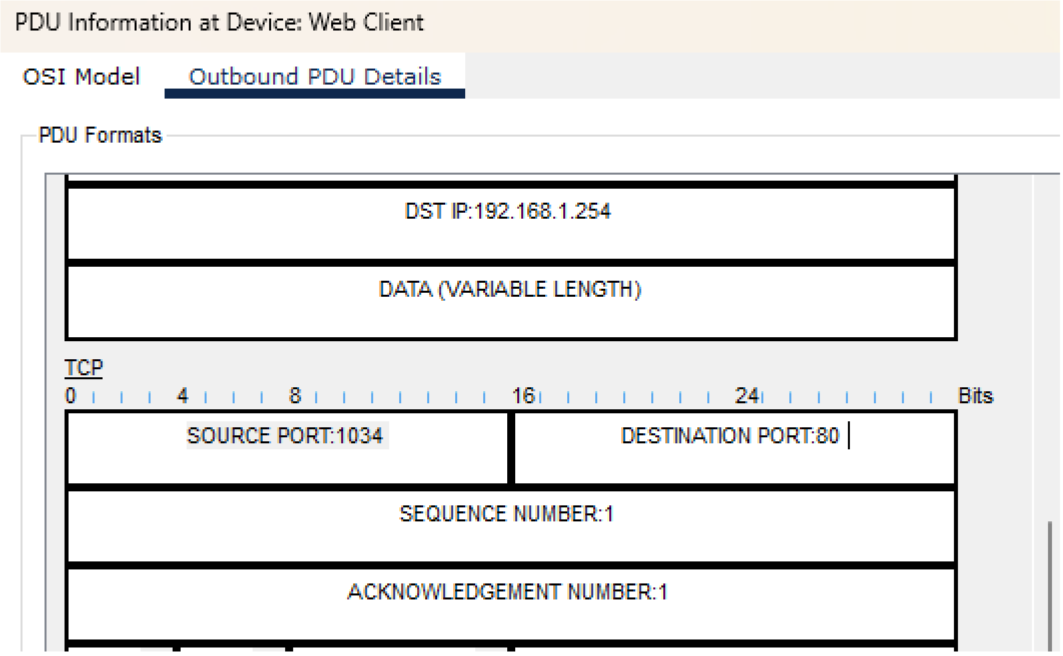
The common information listed under the **IP** section of **PDU Details** as compared to the information listed under the **OSI Model** tab is the Src. IP and Dest.IP and they are associated with Layer 3 in the OSI Model tab.


PDU Information at Device: Web Client

PREAMBLE: 101010..10
DEST ADDR:0001.96A9.401D
SRC ADDR:0060.47CA.4DEE
TYPE:0x
DATA (VARIABLE LENGTH)
FCS:0x00000000

VER:4
IHL:5
DSCP:0x00
TL:122
ID:0x0028
FLAGS:0
FRAG OFFSET:0x000
TTL:128
PRO:0x06
CHKSUM
SRC IP:192.168.1.1
DST IP:192.168.1.254
DATA (VARIABLE LENGTH)

The common information listed under the **TCP** section of **PDU Details**, as compared to the information listed under the **OSI Model** tab is the SOURCE PORT:1034 and DESTINATION PORT:80. They are associated with layer 4 of the OSI Model tab.



PDU Information at Device: Web Client

DST IP:192.168.1.254

DATA (VARIABLE LENGTH)

TCP

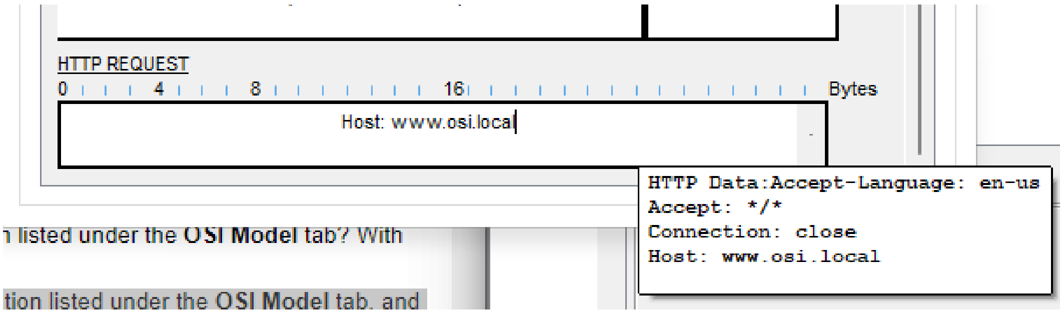
SOURCE PORT:1034

DESTINATION PORT:80

SEQUENCE NUMBER:1

ACKNOWLEDGEMENT NUMBER:1

The Host listed under the HTTP section of the PDU Details is www.osi.local. This information would be associated with Layer 7 of the OSI Model tab.



HTTP REQUEST

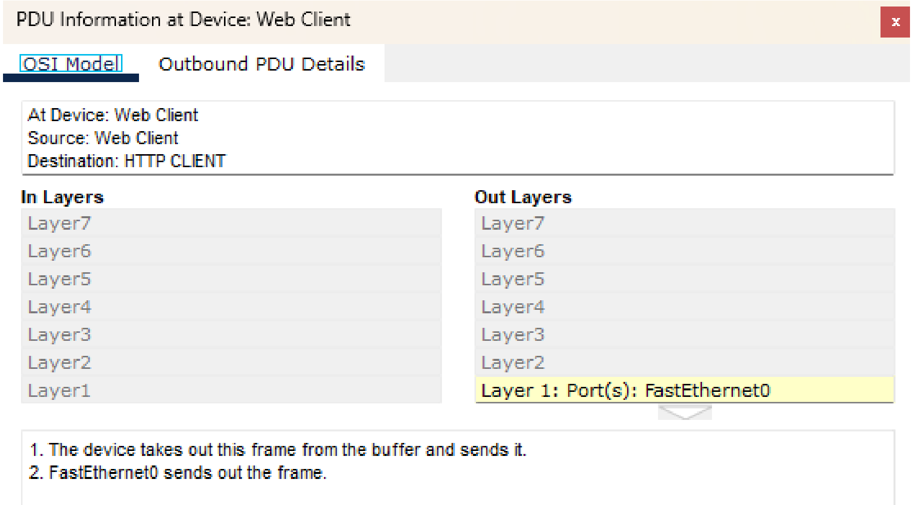
Host: www.osi.local

```
HTTP Data:Accept-Language: en-us
Accept: */*
Connection: close
Host: www.osi.local
```

ı listed under the **OSI Model** tab? With

tion listed under the **OSI Model** tab, and

Click the next coloured square box under the **Event List** > **Type** column. Only Layer 1 is active (not greyed out). The device is moving the frame from the buffer and placing it on to the network.



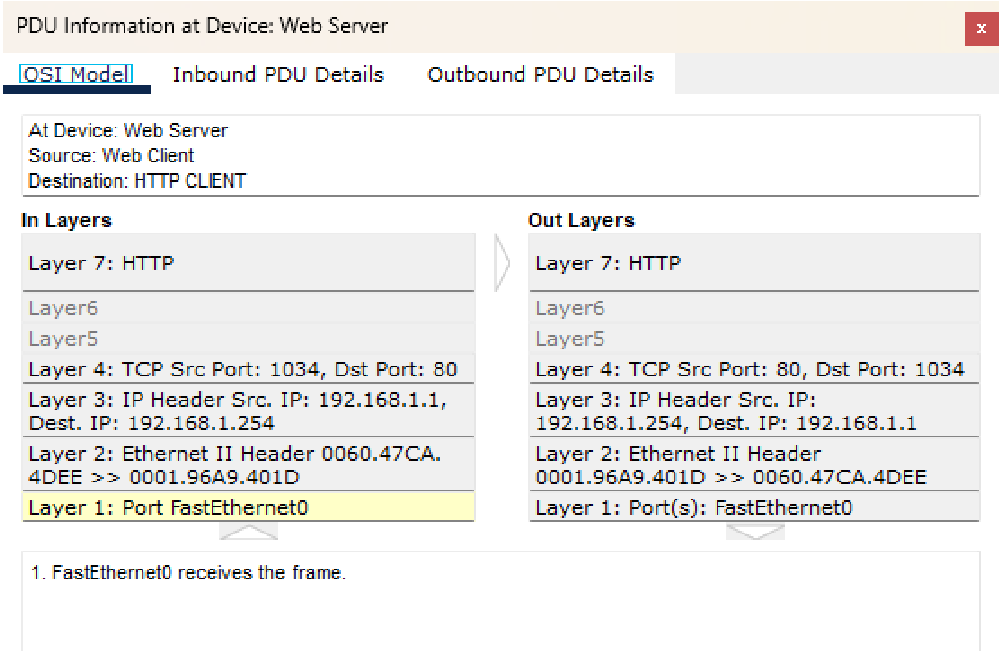
PDU Information at Device: Web Client

At Device: Web Client
Source: Web Client
Destination: HTTP CLIENT

In Layers	Out Layers
Layer7	Layer7
Layer6	Layer6
Layer5	Layer5
Layer4	Layer4
Layer3	Layer3
Layer2	Layer2
Layer1	Layer 1: Port(s): FastEthernet0

1. The device takes out this frame from the buffer and sends it.
2. FastEthernet0 sends out the frame.

Advance to the next HTTP **Type** box within the **Event List** and click the coloured square box. This window contains both **In Layers** and **Out Layers**. Notice the direction of the arrow directly under the **In Layers** column; it is pointing upward, indicating the direction the data is travelling. Scroll through these layers making note of the items previously viewed. At the top of the column the arrow points to the right. This denotes that the server is now sending the information back to the client.



At Device: Web Server
Source: Web Client
Destination: HTTP CLIENT

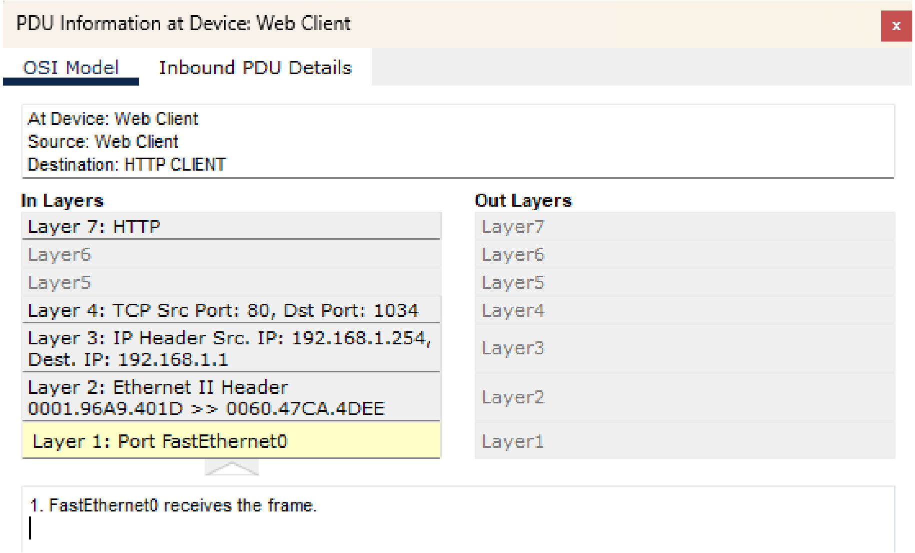
In Layers	Out Layers
Layer 7: HTTP	Layer 7: HTTP
Layer6	Layer6
Layer5	Layer5
Layer 4: TCP Src Port: 1034, Dst Port: 80	Layer 4: TCP Src Port: 80, Dst Port: 1034
Layer 3: IP Header Src. IP: 192.168.1.1, Dest. IP: 192.168.1.254	Layer 3: IP Header Src. IP: 192.168.1.254, Dest. IP: 192.168.1.1
Layer 2: Ethernet II Header 0060.47CA.4DEE >> 0001.96A9.401D	Layer 2: Ethernet II Header 0001.96A9.401D >> 0060.47CA.4DEE
Layer 1: Port FastEthernet0	Layer 1: Port(s): FastEthernet0

1. FastEthernet0 receives the frame.

The major differences ion the In Layers column with that of the Out Layers column are:

- Layer4; TCP Src port and Dst Port in the In Layers are interchanged with those in the Out Layers section.
- Layer 3, the Src and Dest IP have also been interchanged in the In Layers and Out Layers sections.
- In Layer 2, the values of the Ethernet II Header have also been interchanged.

Click the last-colored box under the info column



At Device: Web Client
Source: Web Client
Destination: HTTP CLIENT

In Layers	Out Layers
Layer 7: HTTP	Layer7
Layer6	Layer6
Layer5	Layer5
Layer 4: TCP Src Port: 80, Dst Port: 1034	Layer4
Layer 3: IP Header Src. IP: 192.168.1.254, Dest. IP: 192.168.1.1	Layer3
Layer 2: Ethernet II Header 0001.96A9.401D >> 0060.47CA.4DEE	Layer2
Layer 1: Port FastEthernet0	Layer1

1. FastEthernet0 receives the frame.

In the above displayed event, there are only two tabs, OSI Model tab and Inbound PDU Details tab. This is because at this point in the HTTP communication process, the outbound traffic details are not yet available because the response from the server has not been received.

Part 2: Display Elements of the TCP/IP Protocol Suite

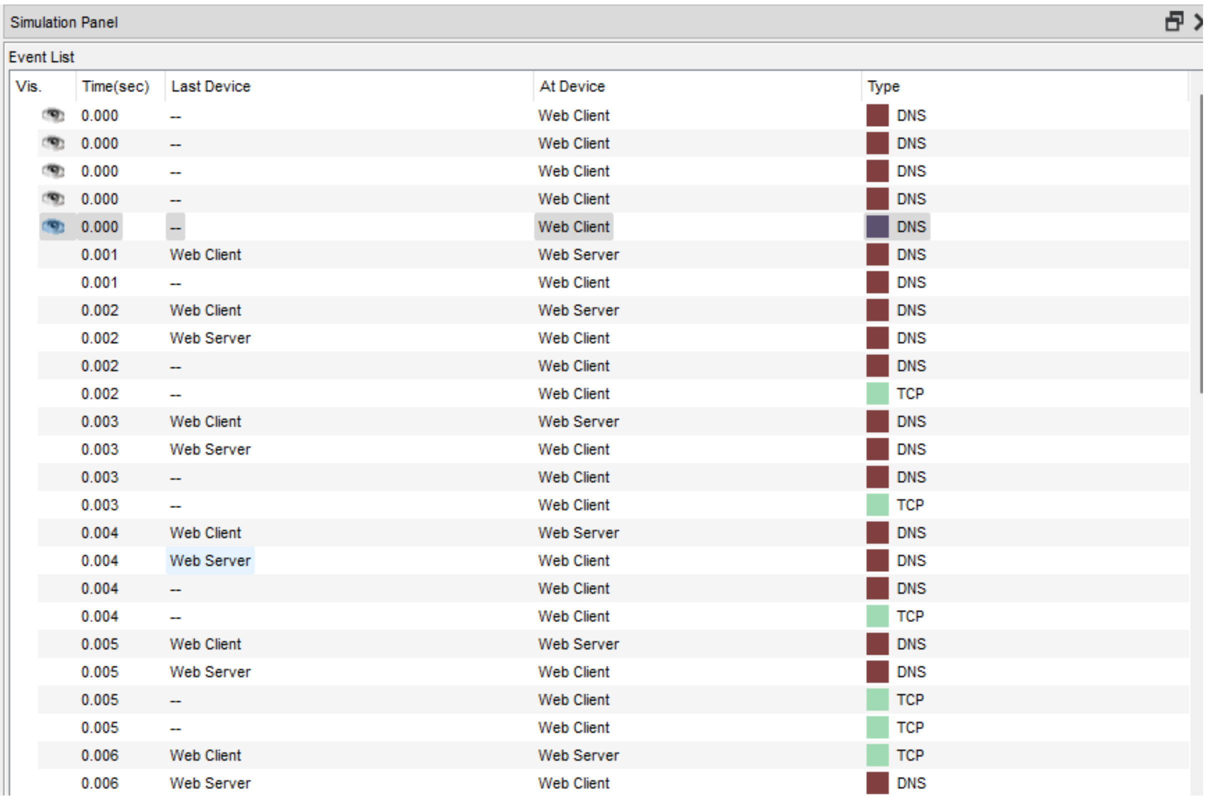
In Part 2 of this activity, I used the Packet Tracer Simulation mode to view and examine some of the other protocols comprising of TCP/IP suite.

In the **Event List Filters** > **Visible Events** section, click **Show All/None**.

Question:

What additional Event Types are displayed?

These extra entries play various roles within the TCP/IP suite. Address Resolution Protocol (ARP) requests MAC addresses for destination hosts. DNS is responsible for converting a name (for example, **www.osi.local**) to an IP address. The additional TCP events are responsible for connecting, agreeing on communication parameters, and disconnecting the communications sessions between the devices. These protocols have been mentioned previously and will be further discussed as the course progresses. Currently there are over 35 possible protocols (event types) available for capture within Packet Tracer.



Simulation Panel

Event List

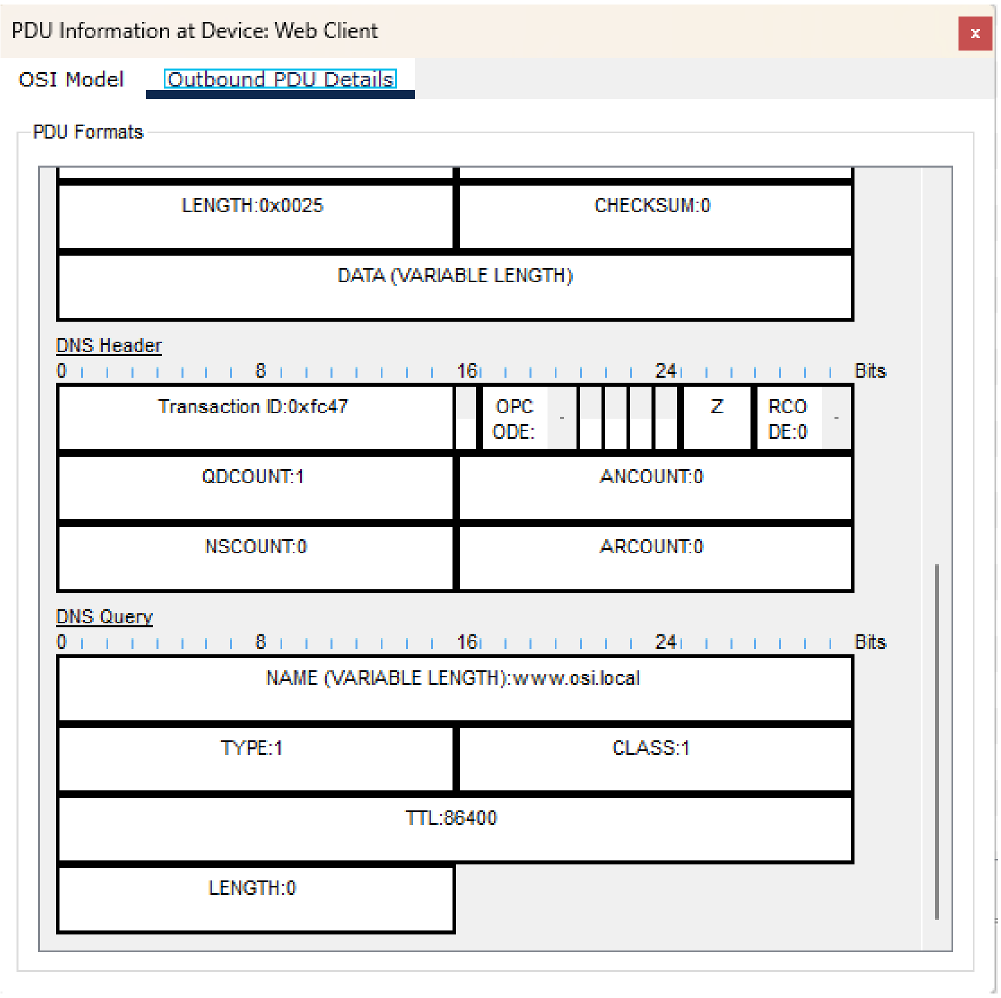
Vis.	Time(sec)	Last Device	At Device	Type
👁	0.000	--	Web Client	🟥 DNS
👁	0.000	--	Web Client	🟥 DNS
👁	0.000	--	Web Client	🟥 DNS
👁	0.000	--	Web Client	🟥 DNS
👁	0.000	--	Web Client	🟪 DNS
	0.001	Web Client	Web Server	🟥 DNS
	0.001	--	Web Client	🟥 DNS
	0.002	Web Client	Web Server	🟥 DNS
	0.002	Web Server	Web Client	🟥 DNS
	0.002	--	Web Client	🟥 DNS
	0.002	--	Web Client	🟩 TCP
	0.003	Web Client	Web Server	🟥 DNS
	0.003	Web Server	Web Client	🟥 DNS
	0.003	--	Web Client	🟥 DNS
	0.003	--	Web Client	🟩 TCP
	0.004	Web Client	Web Server	🟥 DNS
	0.004	Web Server	Web Client	🟥 DNS
	0.004	--	Web Client	🟥 DNS
	0.004	--	Web Client	🟩 TCP
	0.005	Web Client	Web Server	🟥 DNS
	0.005	Web Server	Web Client	🟥 DNS
	0.005	--	Web Client	🟩 TCP
	0.005	--	Web Client	🟩 TCP
	0.006	Web Client	Web Server	🟩 TCP
	0.006	Web Server	Web Client	🟥 DNS

Click the first DNS event in the **Type** column. Explore the **OSI Model** and **PDU Detail** tabs and note the encapsulation process. As you look at the **OSI Model** tab with **Layer 7** highlighted, a description of what is occurring is listed directly below the **In Layers** and **Out Layers** ("1. The DNS client sends a DNS query to the DNS server.”). This is very useful information to help understand what is occurring during the communication process.

Click the **Outbound PDU Details** tab.

Question:

What information is listed in the **NAME** field: in the DNS QUERY section? The information listed is www.osi.local



PDU Information at Device: Web Client

LENGTH:0x0025 | CHECKSUM:0

DATA (VARIABLE LENGTH)

DNS Header

Transaction ID:0xfc47 | OPCODE: | Z | RCODE:0

QDCOUNT:1 | ANCOUNT:0

NSCOUNT:0 | ARCOUNT:0

DNS Query

NAME (VARIABLE LENGTH):www.osi.local

TYPE:1 | CLASS:1

TTL:86400

LENGTH:0

Click the last DNS **Info** coloured square box in the event list.

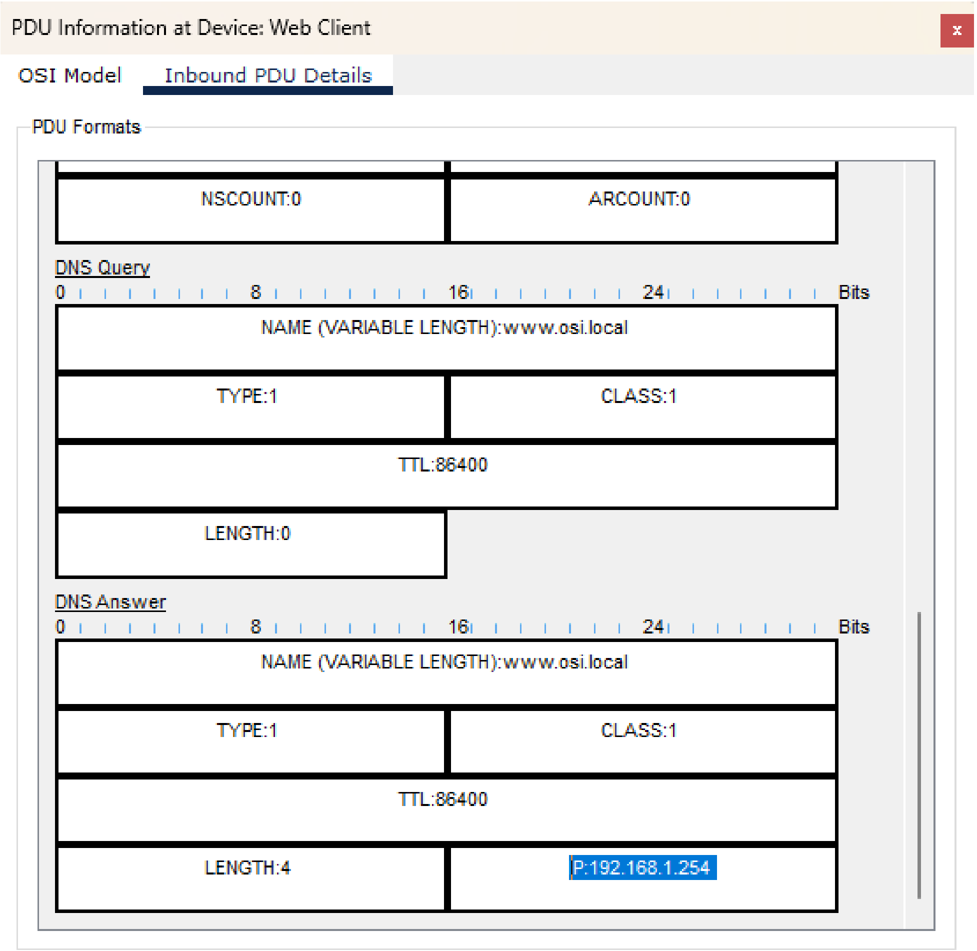
Questions:

At which device was the PDU captured?

The PDU was Captured at the Web Client device as shown in the screenshot attached below.

What is the value listed next to **ADDRESS**: in the DNS ANSWER section of the **Inbound PDU Details**?

The listed value is: IP:192.168.1.254



PDU Information at Device: Web Client

PDU Formats

NSCOUNT:0 | ARCOUNT:0

DNS Query

NAME (VARIABLE LENGTH):www.osi.local

TYPE:1 | CLASS:1

TTL:86400

LENGTH:0

DNS Answer

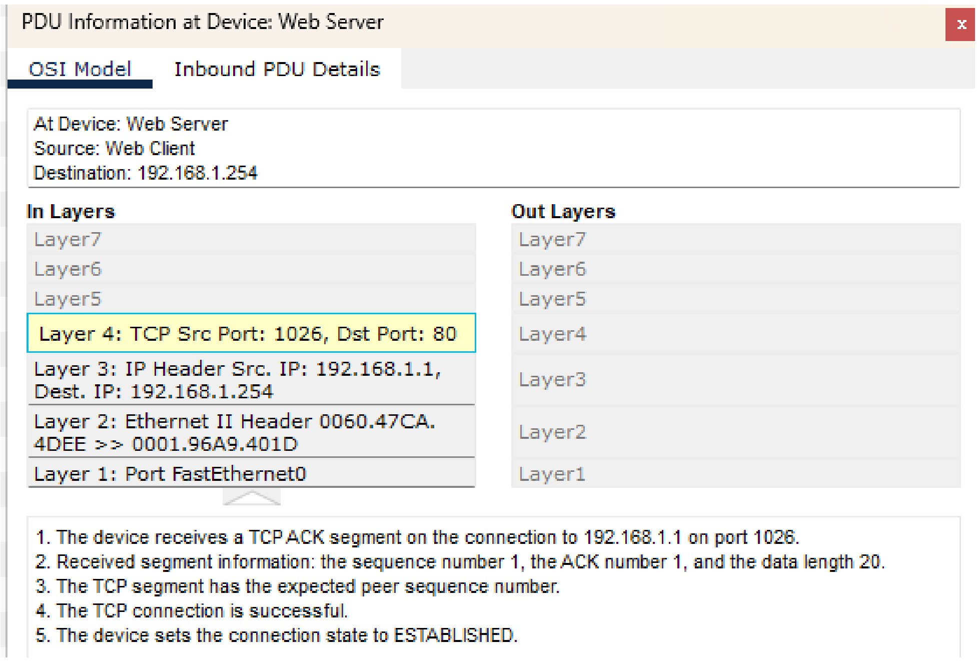
NAME (VARIABLE LENGTH):www.osi.local

TYPE:1 | CLASS:1

TTL:86400

LENGTH:4 | IP:192.168.1.254

Find the first HTTP event in the list and click the colored square box of the TCP event immediately following this event. Highlight Layer 4 in the OSI Model tab.



PDU Information at Device: Web Server

At Device: Web Server
Source: Web Client
Destination: 192.168.1.254

In Layers	Out Layers
Layer7	Layer7
Layer6	Layer6
Layer5	Layer5
Layer 4: TCP Src Port: 1026, Dst Port: 80	Layer4
Layer 3: IP Header Src. IP: 192.168.1.1, Dest. IP: 192.168.1.254	Layer3
Layer 2: Ethernet II Header 0060.47CA.4DEE >> 0001.96A9.401D	Layer2
Layer 1: Port FastEthernet0	Layer1

1. The device receives a TCP ACK segment on the connection to 192.168.1.1 on port 1026.
2. Received segment information: the sequence number 1, the ACK number 1, and the data length 20.
3. The TCP segment has the expected peer sequence number.
4. The TCP connection is successful.
5. The device sets the connection state to ESTABLISHED.

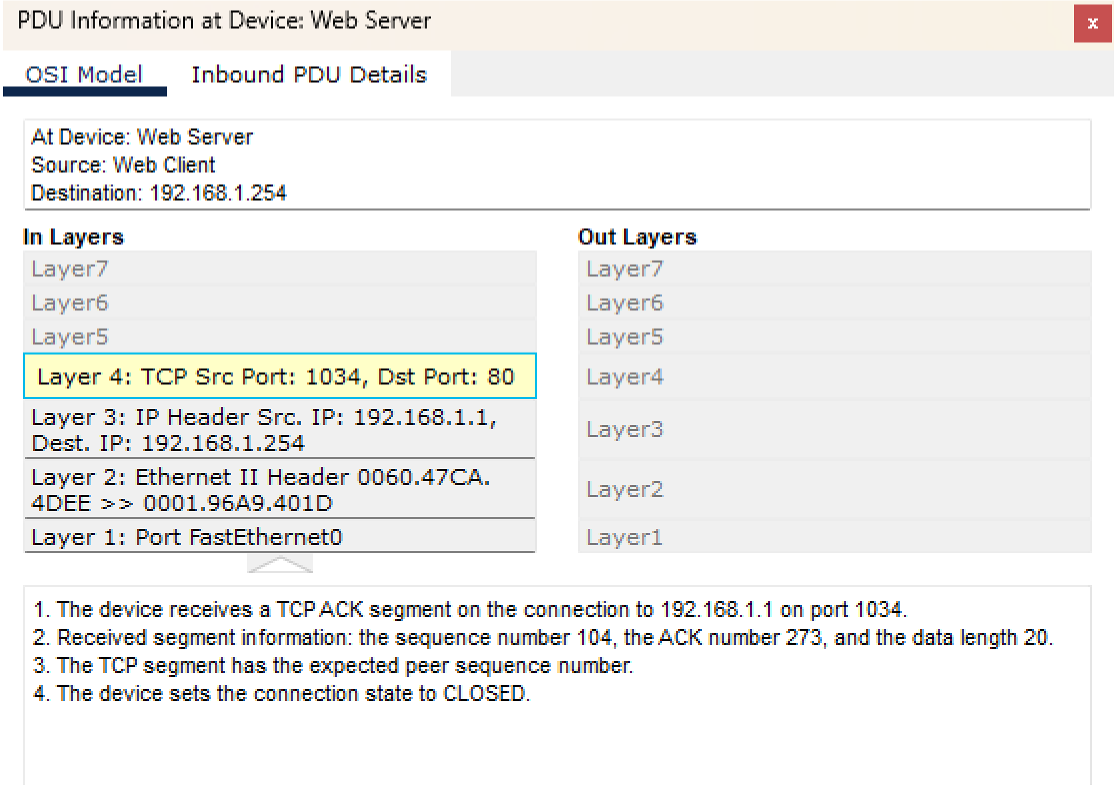
Question:

In the numbered list directly below the **In Layers** and **Out Layers**, what is the information displayed under items 4 and 5?

The information displayed is; The TCP connection is successful and the device sets the connection state to ESTABLISHED.

TCP manages the connecting and disconnecting of the communications channel along with other responsibilities. This particular event shows that the communication channel has been ESTABLISHED.

Click the last TCP event. Highlight Layer 4 in the **OSI Model** tab. Examine the steps listed directly below **In Layers** and **Out Layers**.



At Device: Web Server
Source: Web Client
Destination: 192.168.1.254

In Layers	Out Layers
Layer7	Layer7
Layer6	Layer6
Layer5	Layer5
Layer 4: TCP Src Port: 1034, Dst Port: 80	Layer4
Layer 3: IP Header Src. IP: 192.168.1.1, Dest. IP: 192.168.1.254	Layer3
Layer 2: Ethernet II Header 0060.47CA.4DEE >> 0001.96A9.401D	Layer2
Layer 1: Port FastEthernet0	Layer1

1. The device receives a TCP ACK segment on the connection to 192.168.1.1 on port 1034.
2. Received segment information: the sequence number 104, the ACK number 273, and the data length 20.
3. The TCP segment has the expected peer sequence number.
4. The device sets the connection state to CLOSED.

Question:

What is the purpose of this event, based on the information provided in the last item in the list (should be item 4)?

This event marks the successful completion of the TCP communication session, where data has been transmitted, acknowledged, and the connection is now being closed.

Challenge Questions

This simulation provided an example of a web session between a client and a server on a local area network (LAN). The client makes requests to specific services running on the server. The server must be set up to listen on specific ports for a client request. (Hint: Look at Layer 4 in the **OSI Model** tab for port information.)

Based on the information that was inspected during the Packet Tracer capture, what port number is the **Web Server** listening on for the web request?

The Web Server is listening on port **80** for the web request.

What port is the **Web Server** listening on for a DNS request?

For a DNS request, the Web Server typically listens on port **53.**

Conclusion

This exercise provides an interactive way to explore the TCP/IP and OSI models using Cisco Packet Tracer's simulation mode. By examining HTTP web traffic and other protocols, users gain a practical understanding of how data is encapsulated and transmitted across a network. Through step-by-step instructions and guided exploration, learners can visualize the communication process, including the role of each protocol layer.

By analysing network events and inspecting Protocol Data Units (PDUs) at different layers, users can grasp concepts such as encapsulation, addressing, and protocol-specific details. Additionally, the exercise offers insights into the interaction between TCP/IP protocols and their relationship to the OSI model.

Overall, this activity serves as a valuable tool for networking students to reinforce theoretical knowledge with hands-on practice, enhancing their comprehension of network communication principles.