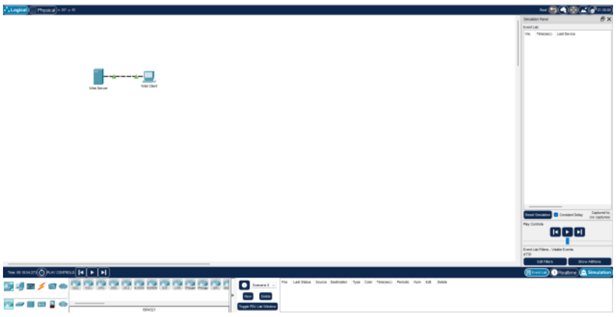
Packet Tracer - Investigate the TCP/IP and OSI Models in Action

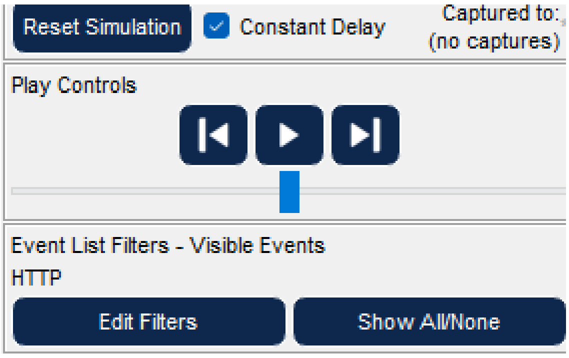
Part 1: Examine HTTP Web Traffic

Step 1: Switch from Realtime to Simulation mode.

a)



b)

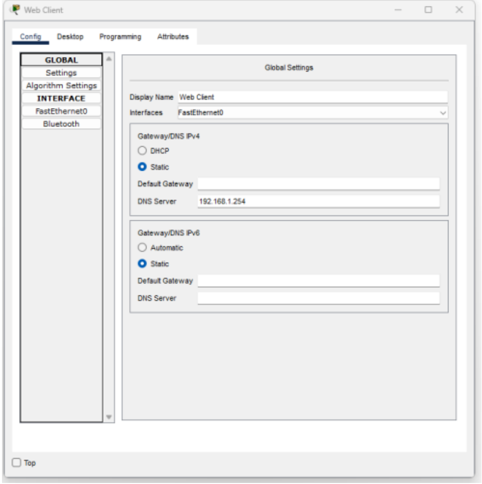


Captured to:
(no captures)

Event List Filters - Visible Events
HTTP

Step 2: Generate web (HTTP) traffic.

a)



Display Name: Web Client

Interfaces: FastEthernet0

Gateway/DNS IPv4

○ DHCP

● Static

Default Gateway:

DNS Server: 192.168.1.254

Gateway/DNS IPv6

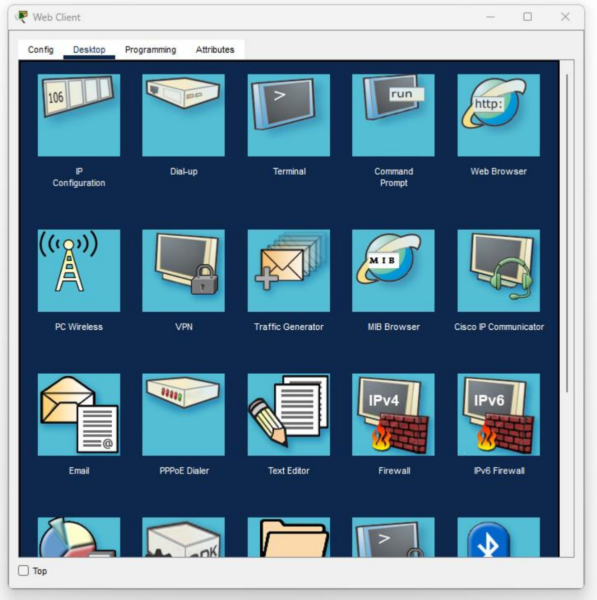
○ Automatic

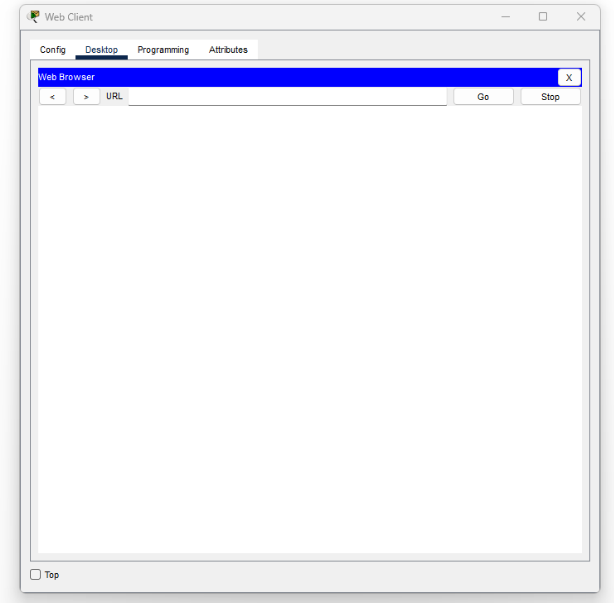
● Static

Default Gateway:

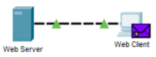
DNS Server:

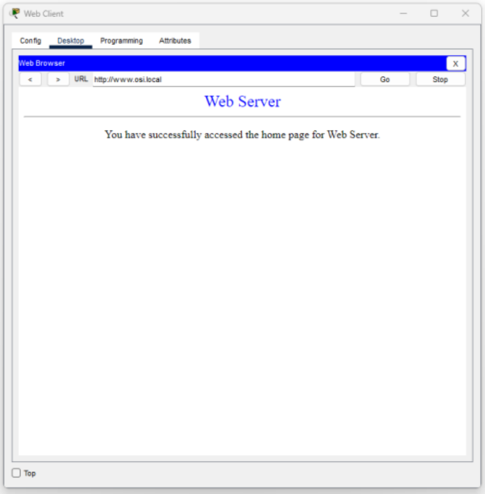
b)





c)/d)

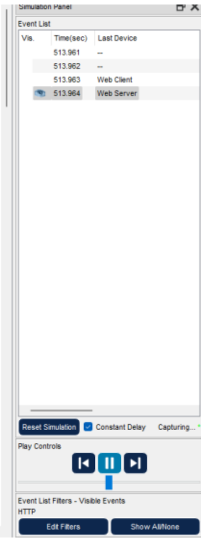




URL: http://www.osi.local

Web Server

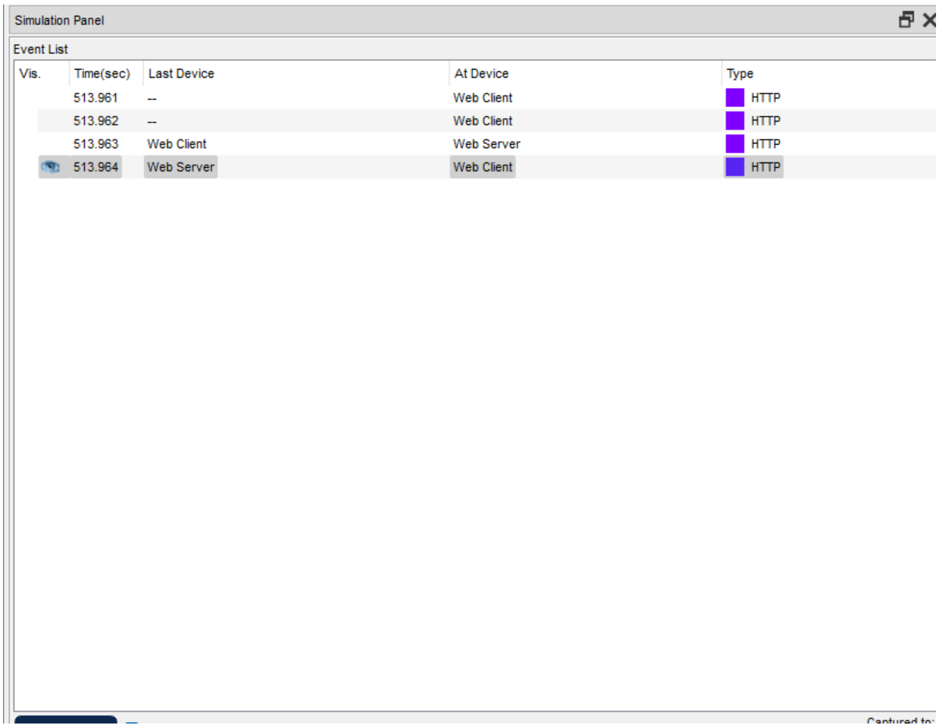
You have successfully accessed the home page for Web Server.



Vis.	Time(sec)	Last Device
	513.961	--
	513.962	--
	513.963	Web Client
👁	513.964	Web Server

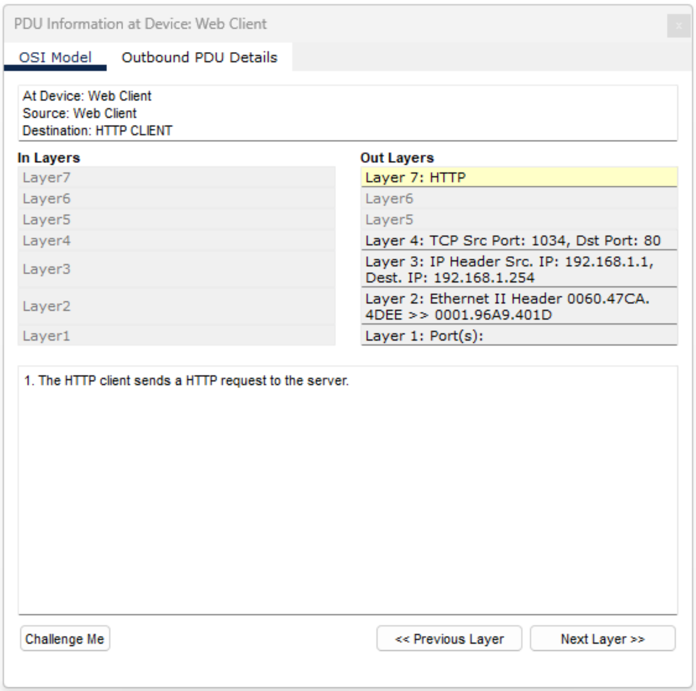
HTTP

e)



Vis.	Time(sec)	Last Device	At Device	Type
	513.961	--	Web Client	🟪 HTTP
	513.962	--	Web Client	🟪 HTTP
	513.963	Web Client	Web Server	🟪 HTTP
👁	513.964	Web Server	Web Client	🟪 HTTP

f)



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.

layer 7: 1. The HTTP client sends a HTTP request to the server.

Nothing in the in Layers

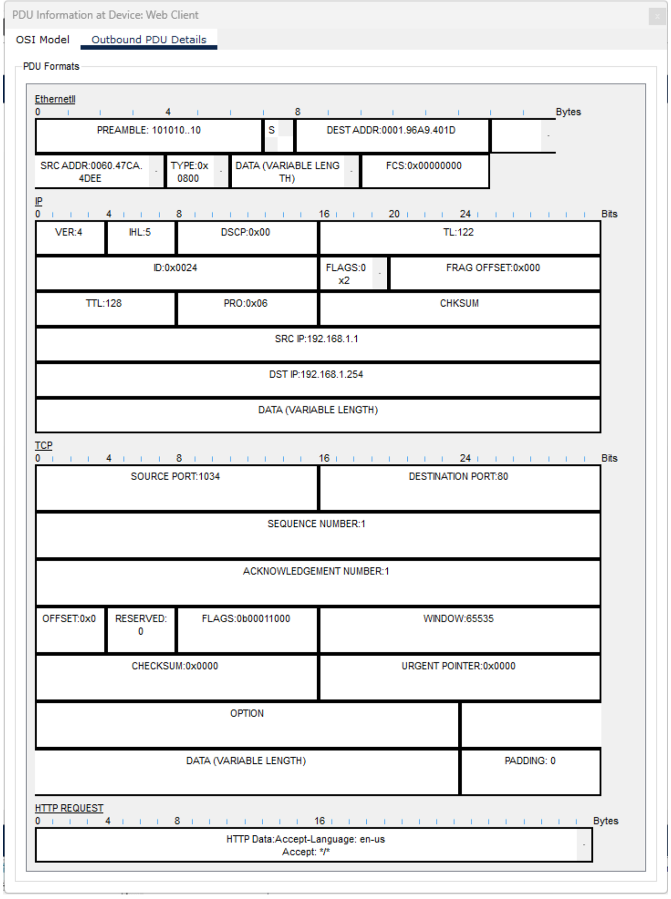
Layer 4 : Dst Port :80

Layer 3: Dest IP 192.168.1.254

Layer 2:

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.

g)



EthernetII (Bytes)

PREAMBLE: 101010..10 | S | DEST ADDR:0001.96A9.401D

SRC ADDR:0060.47CA.4DEE | TYPE:0x0800 | DATA (VARIABLE LENGTH) | FCS:0x00000000

IP (Bits)

VER:4 | IHL:5 | DSCP:0x00 | TL:122

ID:0x0024 | FLAGS:0x2 | FRAG OFFSET:0x000

TTL:128 | PRO:0x06 | CHKSUM

SRC IP:192.168.1.1

DST IP:192.168.1.254

DATA (VARIABLE LENGTH)

TCP (Bits)

SOURCE PORT:1034 | DESTINATION PORT:80

SEQUENCE NUMBER:1

ACKNOWLEDGEMENT NUMBER:1

OFFSET:0x0 | RESERVED: 0 | FLAGS:0b00011000 | WINDOW:65535

CHECKSUM:0x0000 | URGENT POINTER:0x0000

OPTION

DATA (VARIABLE LENGTH) | PADDING: 0

HTTP REQUEST (Bytes)

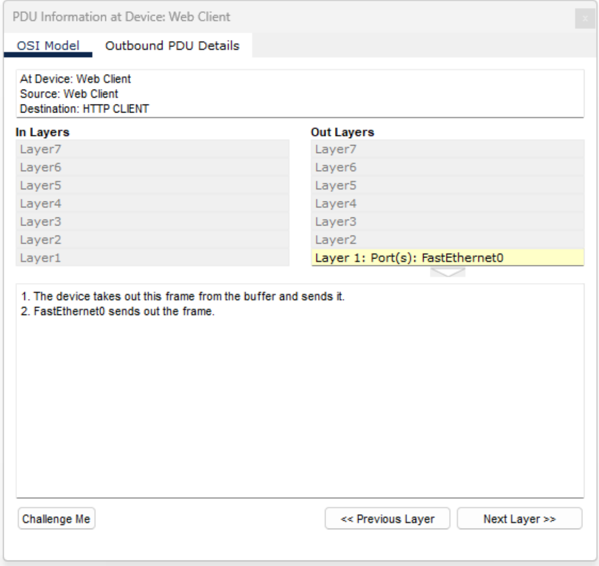
HTTP Data:Accept-Language: en-us
Accept: */*

Under the IP section we have in common the IP Source and Destination IP. Maybe associated with the Layer 3 of OSI Model

Under the TCP Model we have in common with the OSI model the Source Port and Destination Port which associated with the Layer 4

The Host is www.osi.local. The associated layer is the Layer 7

h)

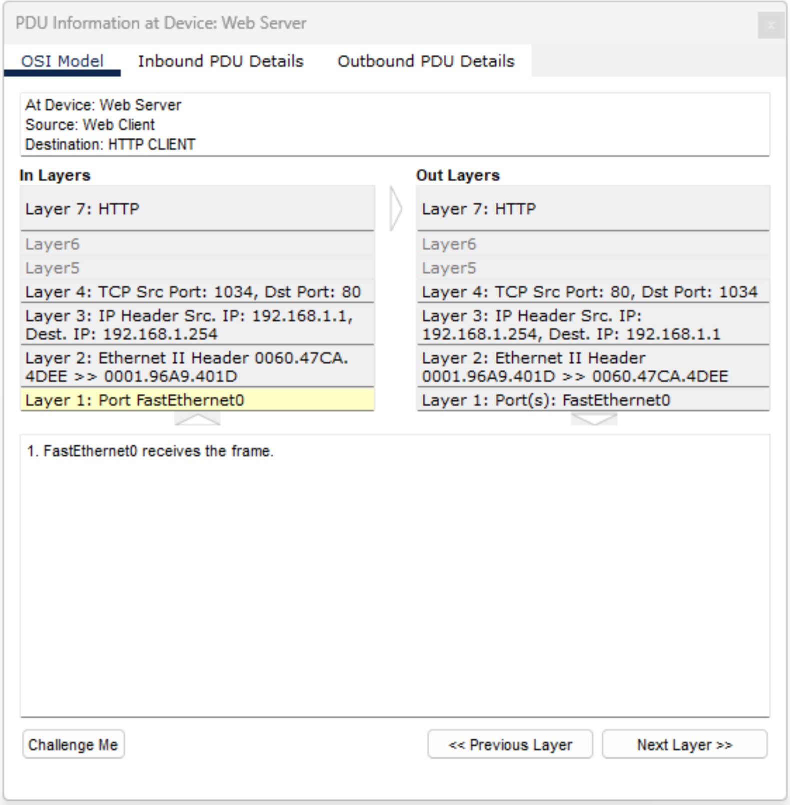


At Device: Web Client
Source: Web Client
Destination: HTTP CLIENT

Layer 1: Port(s): FastEthernet0

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

i)



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

In Layers

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

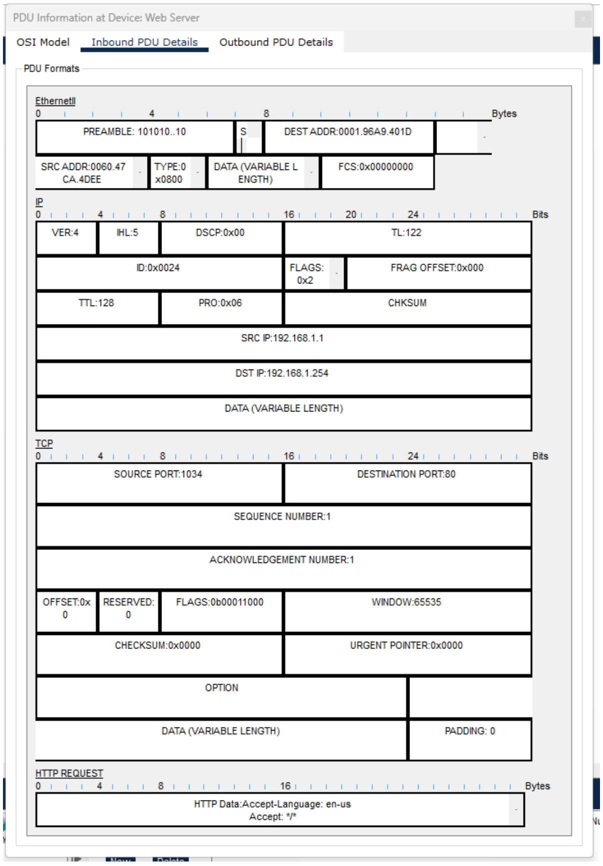
Out Layers

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

1. FastEthernet0 receives the frame.

The Major Difference is that the source and destination are reversed. We can see with the layer 4 or 3

j)

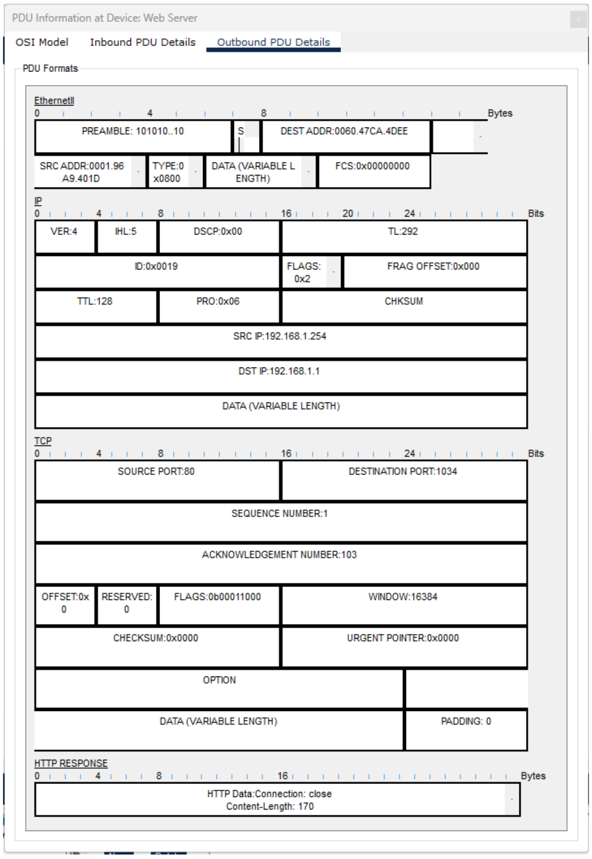


EthernetII
PREAMBLE: 101010..10
S
DEST ADDR:0001.96A9.401D
SRC ADDR:0060.47CA.4DEE
TYPE:0x0800
DATA (VARIABLE LENGTH)
FCS:0x00000000

IP
VER:4
IHL:5
DSCP:0x00
TL:122
ID:0x0024
FLAGS: 0x2
FRAG OFFSET:0x000
TTL:128
PRO:0x06
CHKSUM
SRC IP:192.168.1.1
DST IP:192.168.1.254
DATA (VARIABLE LENGTH)

TCP
SOURCE PORT:1034
DESTINATION PORT:80
SEQUENCE NUMBER:1
ACKNOWLEDGEMENT NUMBER:1
OFFSET:0x0
RESERVED: 0
FLAGS:0b00011000
WINDOW:65535
CHECKSUM:0x0000
URGENT POINTER:0x0000
OPTION
DATA (VARIABLE LENGTH)
PADDING: 0

HTTP REQUEST
HTTP Data:Accept-Language: en-us
Accept: */*



EthernetII
PREAMBLE: 101010..10
S
DEST ADDR:0060.47CA.4DEE
SRC ADDR:0001.96A9.401D
TYPE:0x0800
DATA (VARIABLE LENGTH)
FCS:0x00000000

IP
VER:4
IHL:5
DSCP:0x00
TL:292
ID:0x0019
FLAGS: 0x2
FRAG OFFSET:0x000
TTL:128
PRO:0x06
CHKSUM
SRC IP:192.168.1.254
DST IP:192.168.1.1
DATA (VARIABLE LENGTH)

TCP
SOURCE PORT:80
DESTINATION PORT:1034
SEQUENCE NUMBER:1
ACKNOWLEDGEMENT NUMBER:103
OFFSET:0x0
RESERVED: 0
FLAGS:0b00011000
WINDOW:16384
CHECKSUM:0x0000
URGENT POINTER:0x0000
OPTION
DATA (VARIABLE LENGTH)
PADDING: 0

HTTP RESPONSE
HTTP Data:Connection: close
Content-Length: 170

As said in question i) we have the reversed IP and Port. But we have a different http request

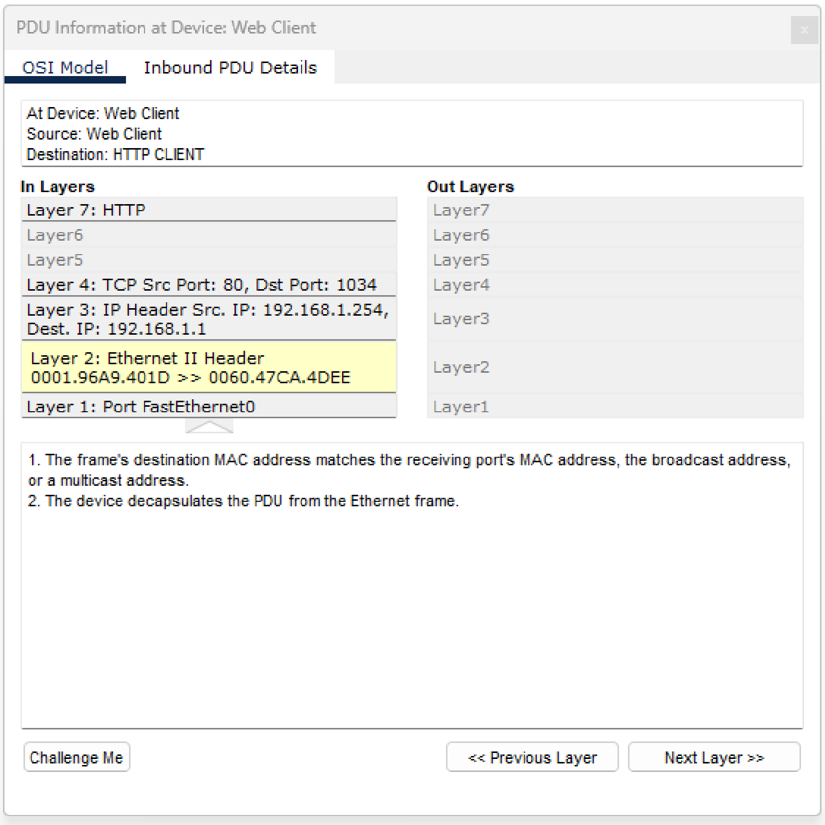
For the Inbound:

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

For the Outbound:

HTTP Data:Connection: close
Content-Length: 170
Content-Type: text/html
Server: PT-Server/5.2

k)



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

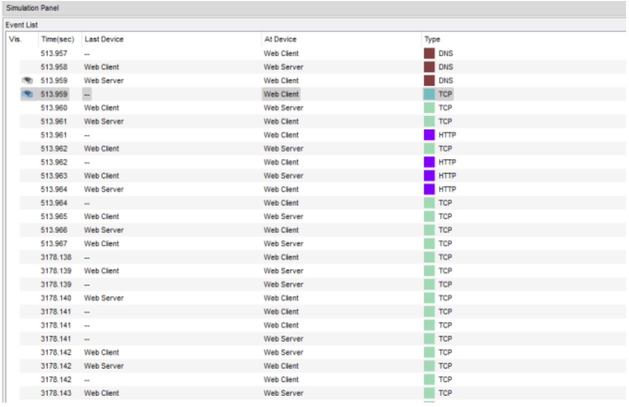
1. The frame's destination MAC address matches the receiving port's MAC address, the broadcast address, or a multicast address.
2. The device decapsulates the PDU from the Ethernet frame.

Here we have two tabs indeed we don't send to the Web Server anymore so we don't have Out Layers and Outbound.

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

Step 1: View Additional Events

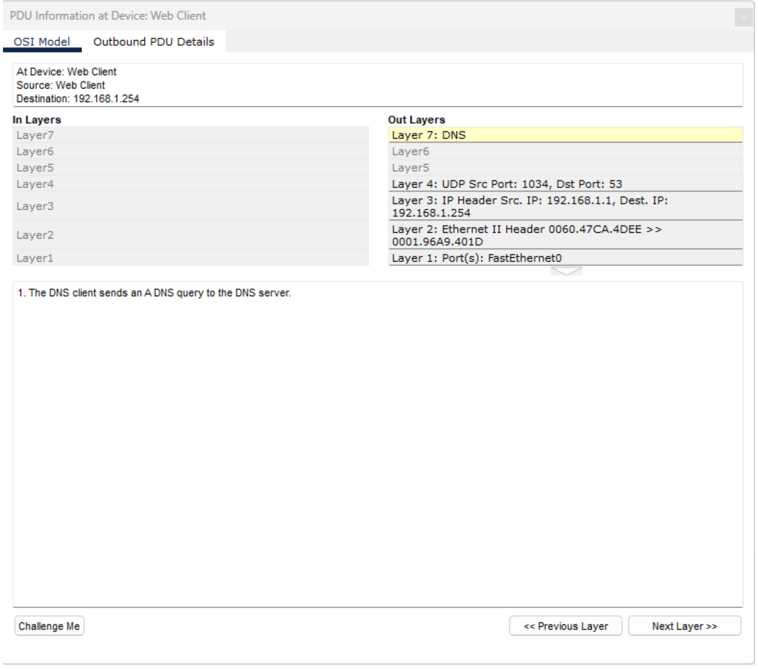
a)b)



Vis.	Time(sec)	Last Device	At Device	Type
	513.957	--	Web Client	🟥 DNS
	513.958	Web Client	Web Server	🟥 DNS
	513.959	Web Server	Web Client	🟥 DNS
	513.959	--	Web Client	🟦 TCP
	513.960	Web Client	Web Server	🟩 TCP
	513.961	Web Server	Web Client	🟩 TCP
	513.961	--	Web Client	🟪 HTTP
	513.962	Web Client	Web Server	🟩 TCP
	513.962	--	Web Client	🟪 HTTP
	513.963	Web Client	Web Server	🟪 HTTP
	513.964	Web Server	Web Client	🟪 HTTP
	513.964	--	Web Client	🟩 TCP
	513.965	Web Client	Web Server	🟩 TCP
	513.966	Web Server	Web Client	🟩 TCP
	513.967	Web Client	Web Server	🟩 TCP
	3178.138	--	Web Client	🟩 TCP
	3178.139	Web Client	Web Server	🟩 TCP
	3178.139	--	Web Server	🟩 TCP
	3178.140	Web Server	Web Client	🟩 TCP
	3178.141	--	Web Client	🟩 TCP
	3178.141	--	Web Client	🟩 TCP
	3178.141	--	Web Server	🟩 TCP
	3178.142	Web Client	Web Server	🟩 TCP
	3178.142	Web Server	Web Client	🟩 TCP
	3178.142	--	Web Client	🟩 TCP
	3178.143	Web Client	Web Server	🟩 TCP

We have new event as DNS and TCP.

c)

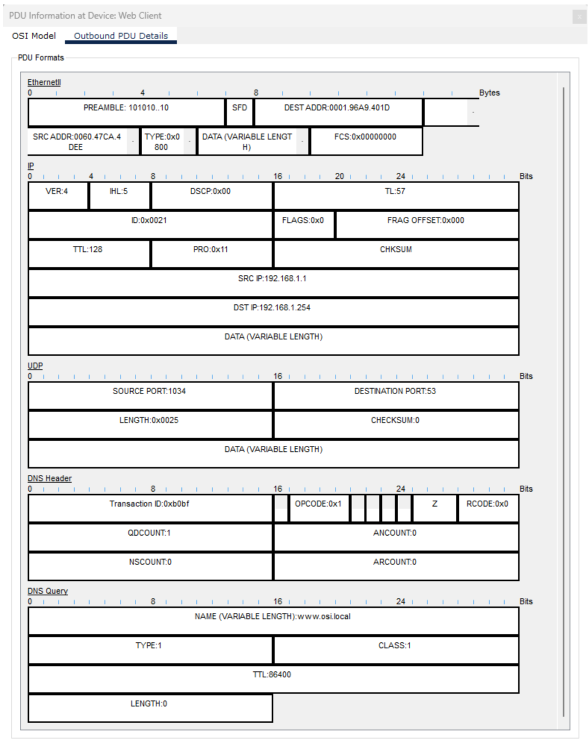


At Device: Web Client
Source: Web Client
Destination: 192.168.1.254

In Layers	Out Layers
Layer7	Layer 7: DNS
Layer6	Layer6
Layer5	Layer5
Layer4	Layer 4: UDP Src Port: 1034, Dst Port: 53
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): FastEthernet0

1. The DNS client sends an A DNS query to the DNS server.

d)



PDU Information at Device: Web Client

OSI Model | Outbound PDU Details

PDU Formats

EthernetII

PREAMBLE: 101010..10 | SFD | DEST ADDR:0001.96A9.401D

SRC ADDR:0060.47CA.4DEE | TYPE:0x0800 | DATA (VARIABLE LENGTH) | FCS:0x00000000

IP

VER:4 | IHL:5 | DSCP:0x00 | TL:57

ID:0x0021 | FLAGS:0x0 | FRAG OFFSET:0x000

TTL:128 | PRO:0x11 | CHKSUM

SRC IP:192.168.1.1

DST IP:192.168.1.254

DATA (VARIABLE LENGTH)

UDP

SOURCE PORT:1034 | DESTINATION PORT:53

LENGTH:0x0025 | CHECKSUM:0

DATA (VARIABLE LENGTH)

DNS Header

Transaction ID:0xb0bf | OPCODE:0x1 | Z | RCODE:0x0

QDCOUNT:1 | ANCOUNT:0

NSCOUNT:0 | ARCOUNT:0

DNS Query

NAME (VARIABLE LENGTH):www.osi.local

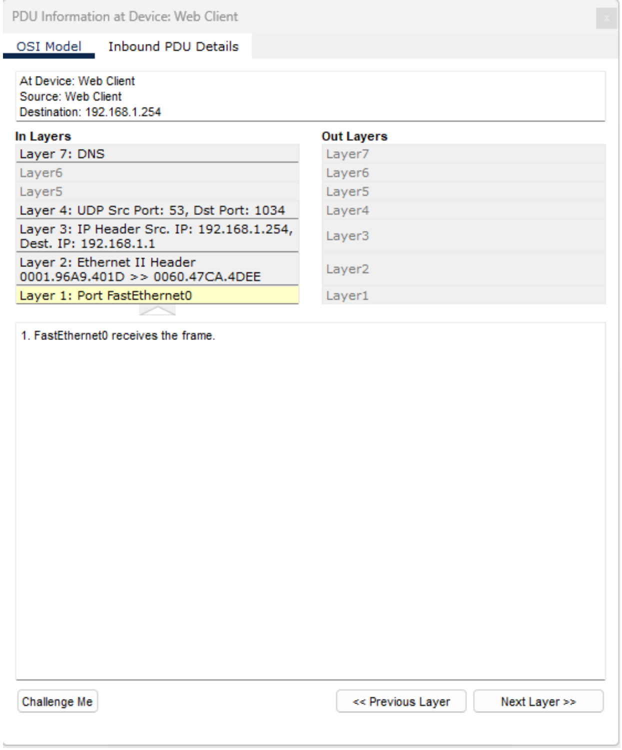
TYPE:1 | CLASS:1

TTL:86400

LENGTH:0

In the name field we have www.osi.local

e)



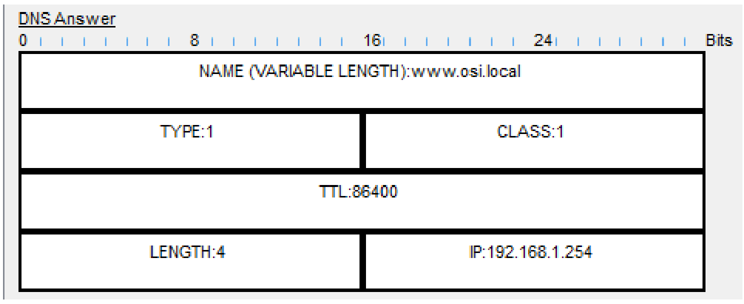
PDU Information at Device: Web Client

OSI Model | Inbound PDU Details

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

In Layers	Out Layers
Layer 7: DNS	Layer7
Layer6	Layer6
Layer5	Layer5
Layer 4: UDP Src Port: 53, 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.



DNS Answer

NAME (VARIABLE LENGTH):www.osi.local

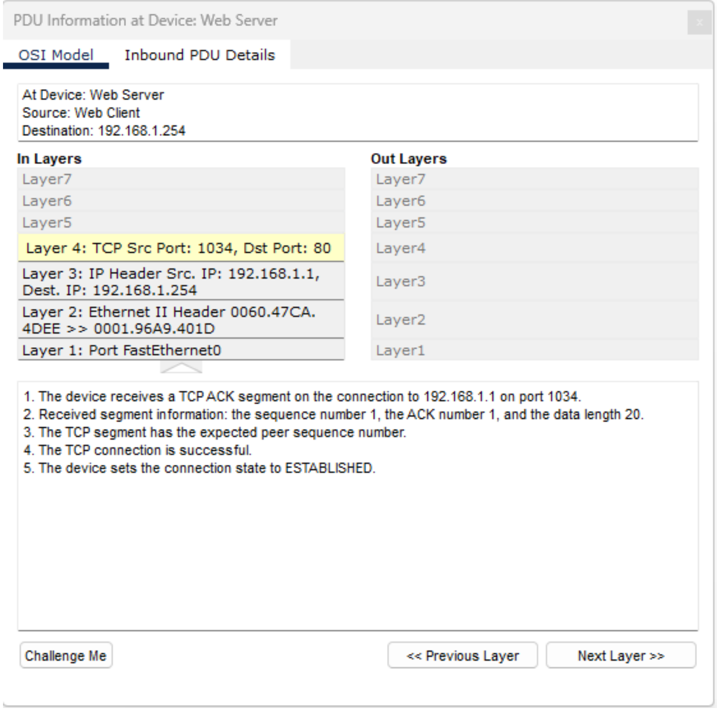
TYPE:1 | CLASS:1

TTL:86400

LENGTH:4 | IP:192.168.1.254

It was capture at the Web Client device. The Address is maybe the IP :192.168.1.254.

f)



PDU Information at Device: Web Server

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

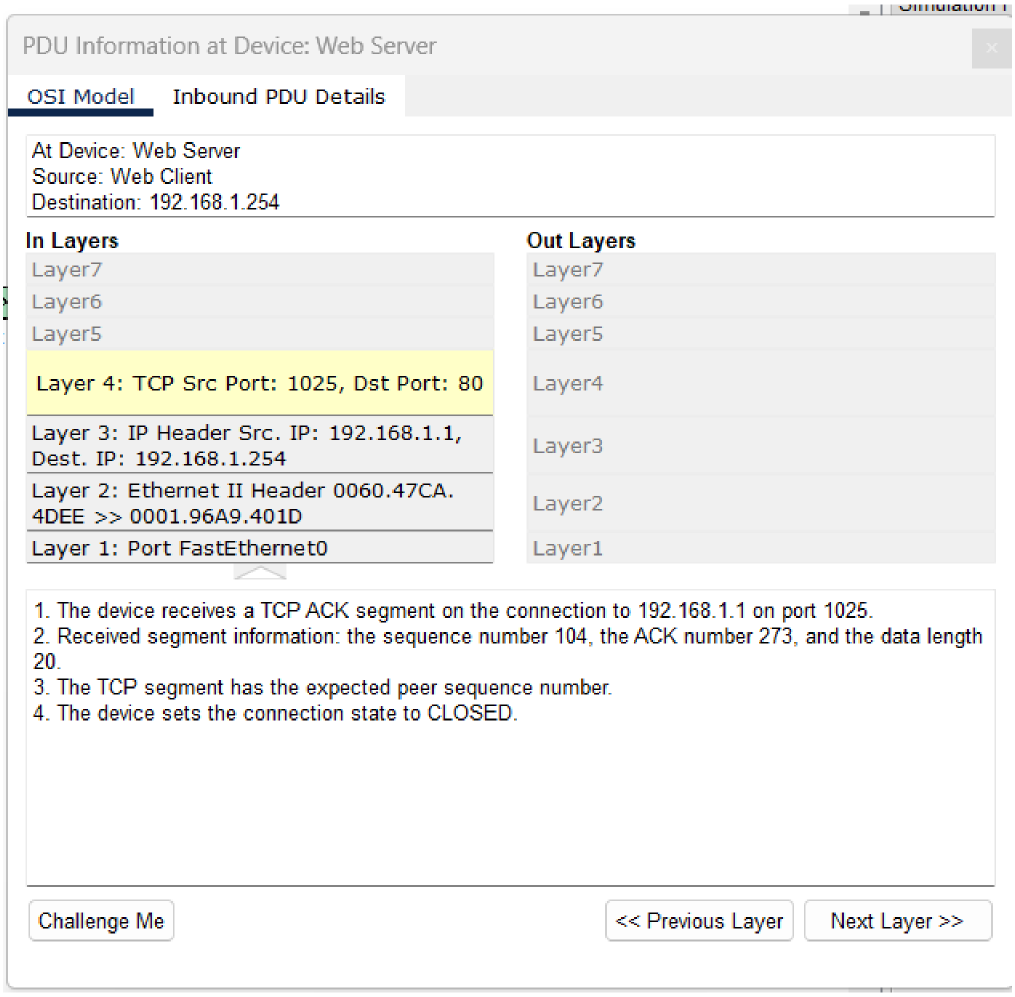
In Layers	Out Layers
Layer7	Layer7
Layer6	Layer6
Layer5	Layer5
Layer 4: TCP Src Port: 1034, Dst Port: 80	Layer4
Layer 3: IP Header Src. IP: 192.168.1.1, Dest. IP: 192.168.1.254	Layer3
Layer 2: Ethernet II Header 0060.47CA.4DEE >> 0001.96A9.401D	Layer2
Layer 1: Port FastEthernet0	Layer1

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 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.

We have :

4. The TCP connection is successful.
5. The device sets the connection state to ESTABLISHED.

g)



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: 1025, 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 1025.
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.

We see at the item 4 :

4. The device sets the connection state to CLOSED.

This event purpose is to closed connection between the client and the server.