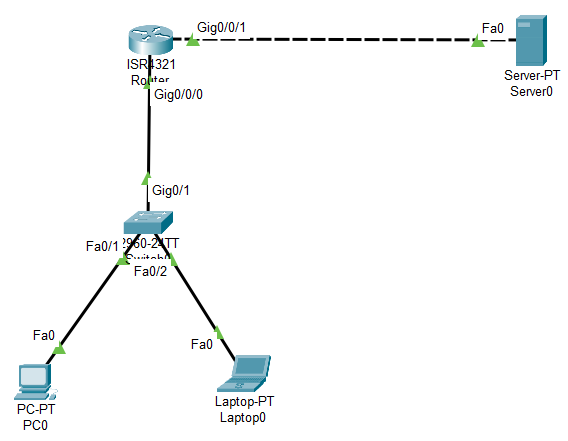
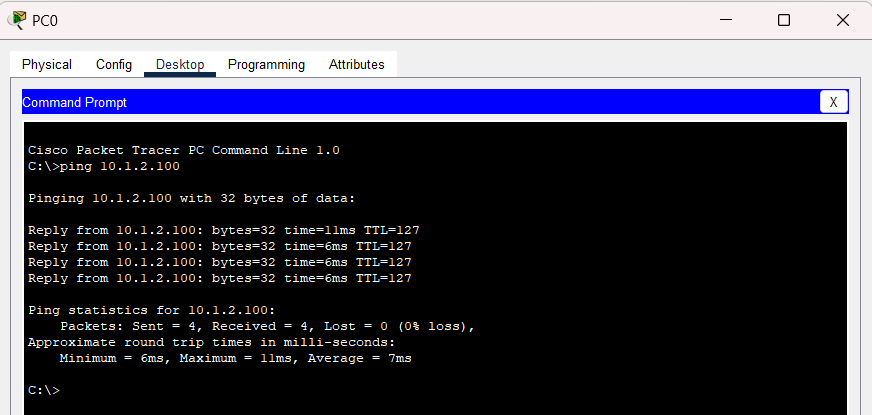
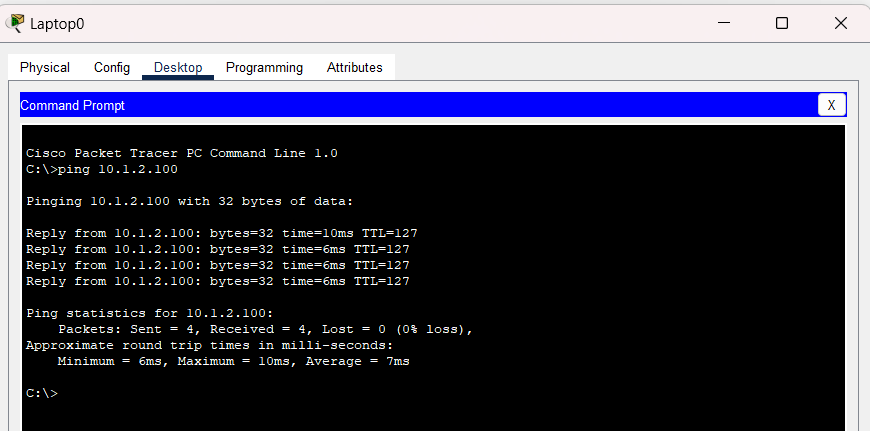
# Introduction

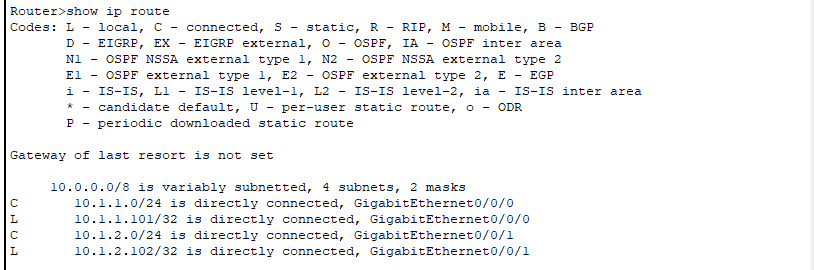


This network diagram includes:

* A server
* A Router
* A Switch
* A PC
* A Laptop

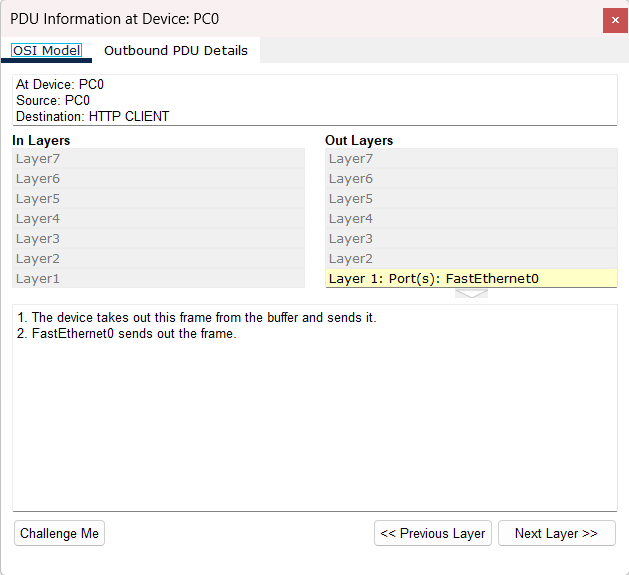
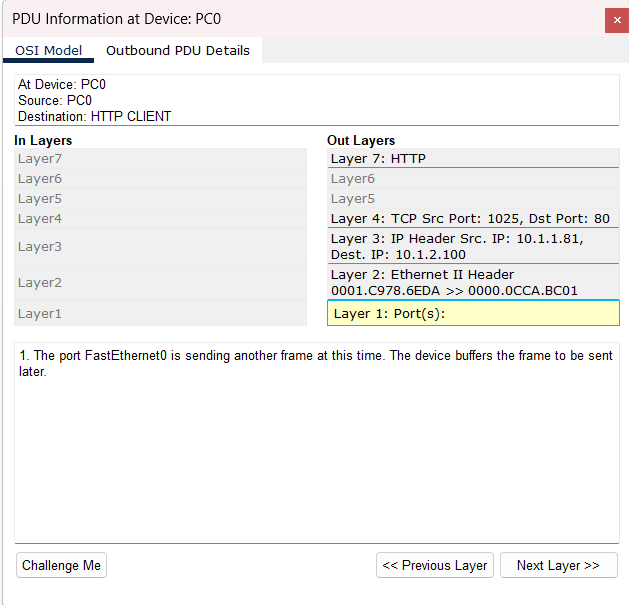
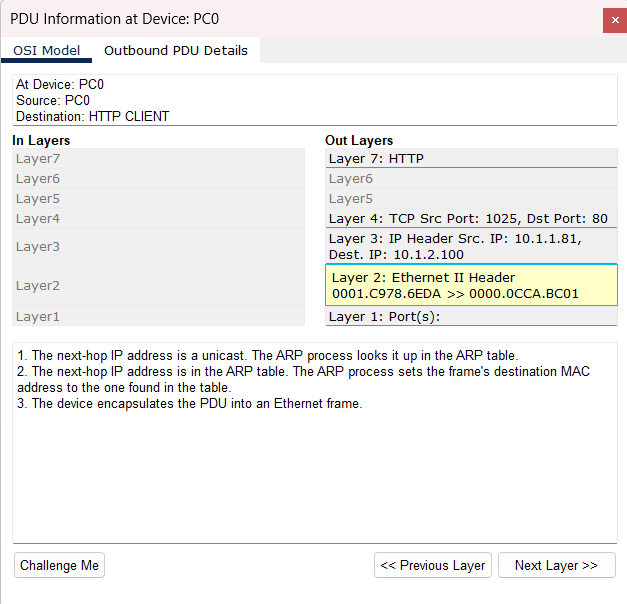
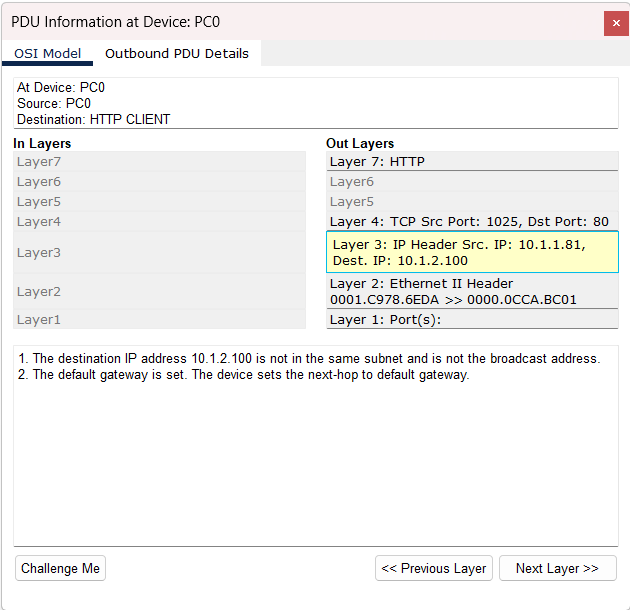
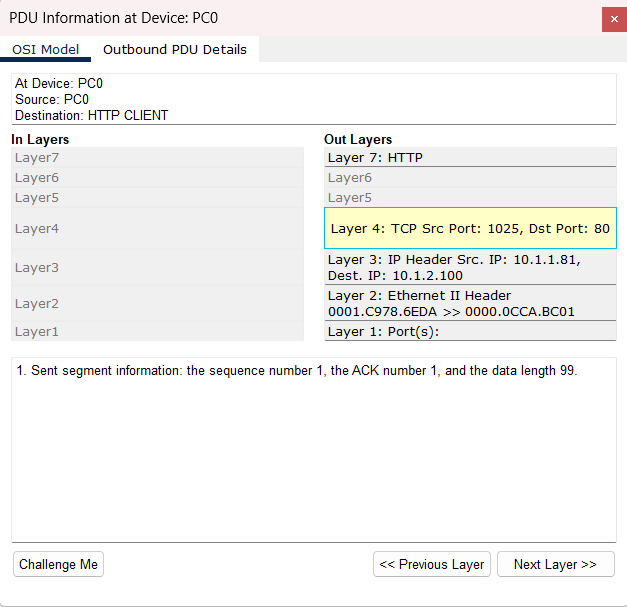
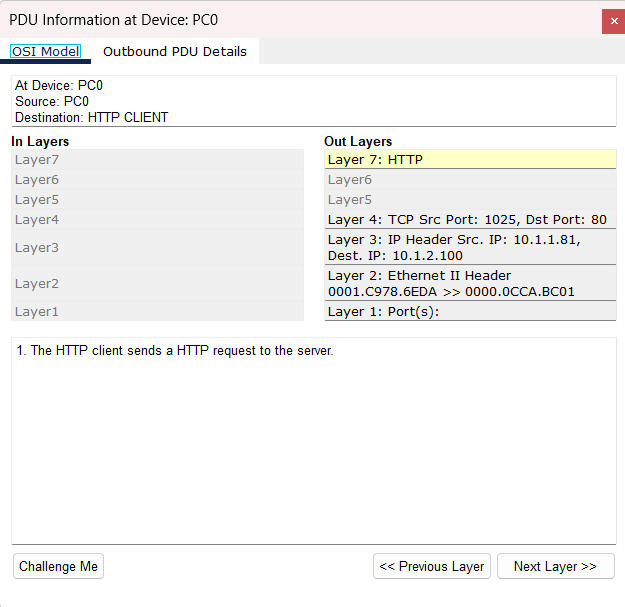
| Device | Interface | IP Address | Subnet Mask | Default Gateway |
| --- | --- | --- | --- | --- |
| Server0 | Fa0 | 10.1.2.100 | 255.255.255.0 | 10.1.2.102 |
| Router |  |  | 255.255.255.0 |  |
|  |  |  |  |
| Switch0 |  |  | 255.255.255.0 |  |
| PC0 |  |  | 255.255.255.0 |  |
| Laptop0 |  |  | 255.255.255.0 |  |





# Processes (Encapsulation and Decapsulation)

## From PC0 to Switch 0



The PC0 in the **application layer** will send out a HTTP request to the server ip address.(10.1.2.100)

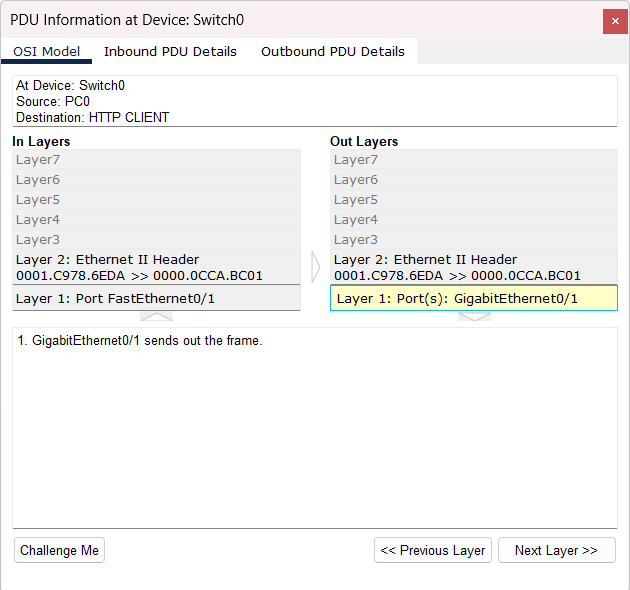
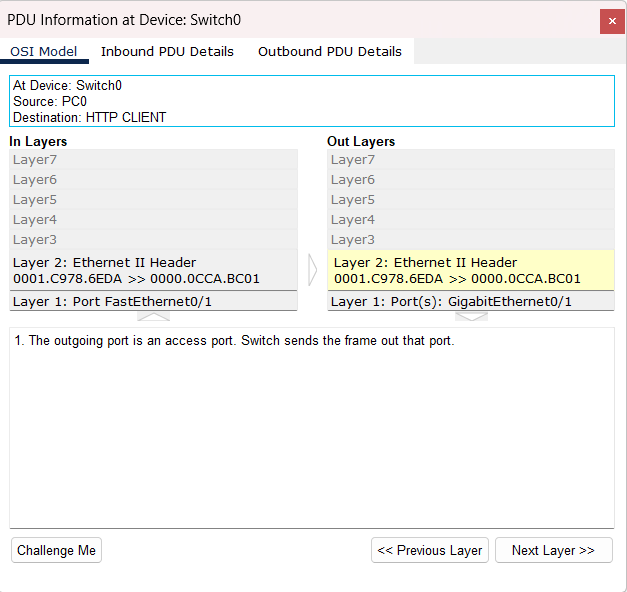
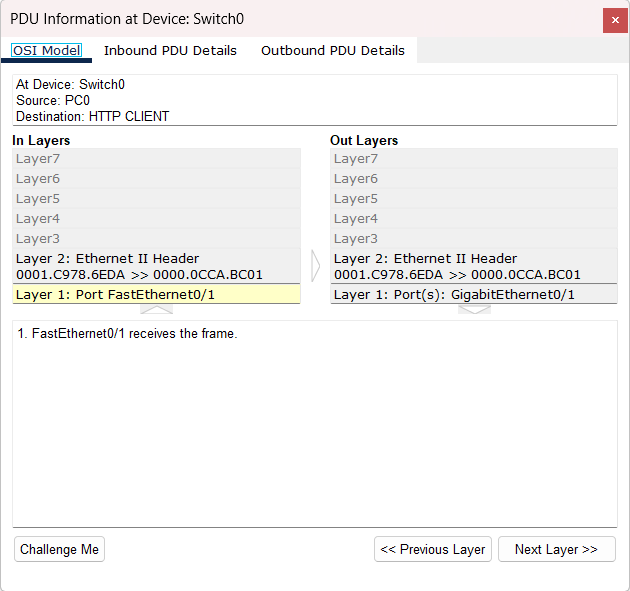
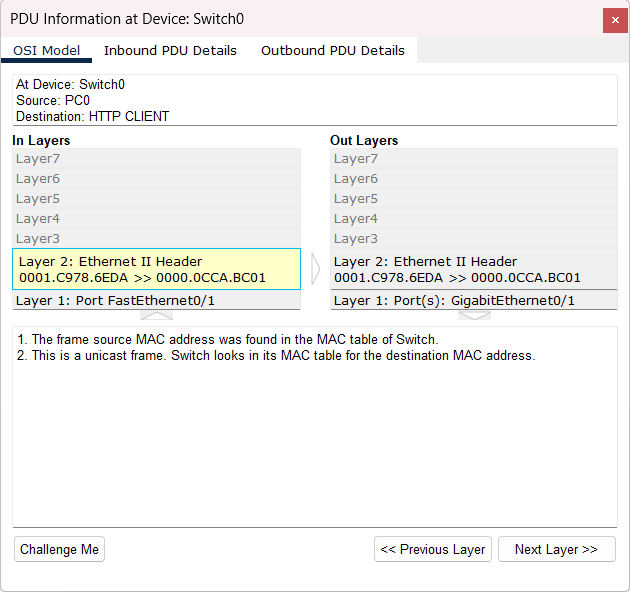
**In the transport layer:** The home port is 1026 and the HTTP port is 80. Segment information is sent through sequence number 1 which is the first segment of communication. The Acknowledgment Number 1(ACK) indicates that a segment has been received successfully.

**In the internet layer**, the destination IP address 10.1.2.100 is not in the same subnet, routing is needed for communication between the source and destination. Hence, a default gateway is then set, which helps with the routing of packets.

**In the network access layer,** the packet is sent to another destination which is the server. The ARP table will map the next-hop IP address to the corresponding MAC address. It will then set the next-hop IP address value to the frame’s destination MAC address. This will prepare the device to encapsulate the packet to be transmitted over the ethernet network.

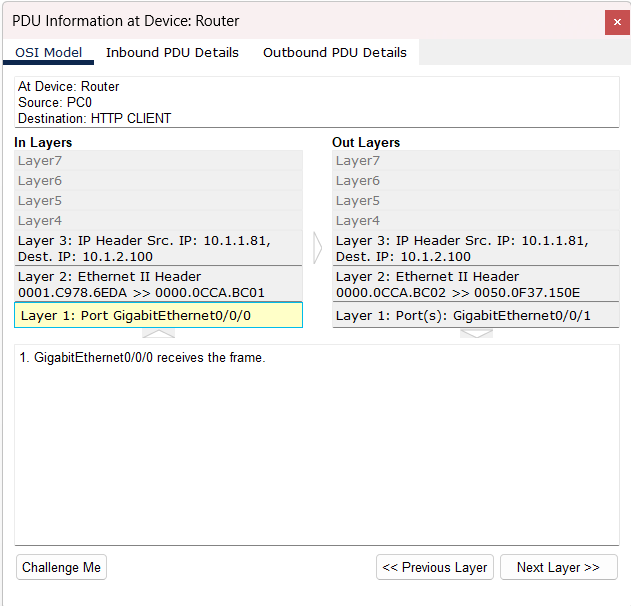
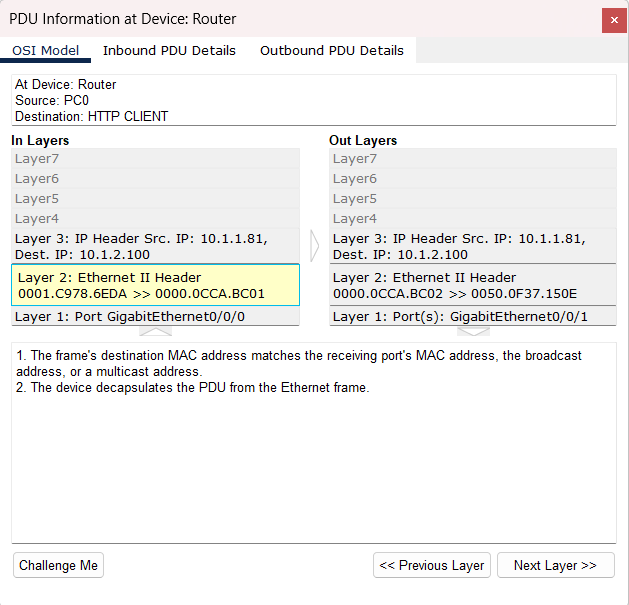
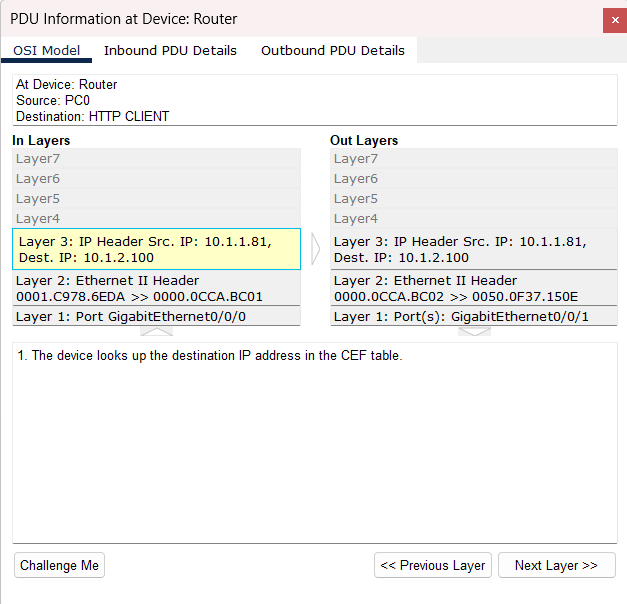
The other frame that is sent later is buffered as it helps to ensure no collision between all packets.

## From Switch0 to Router



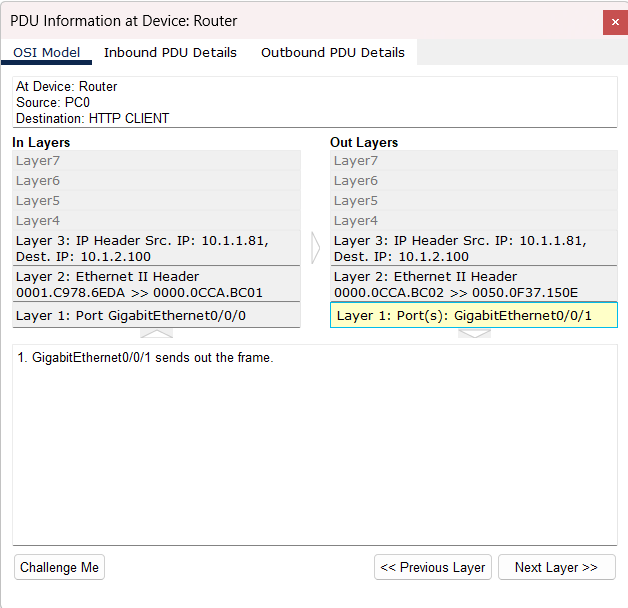
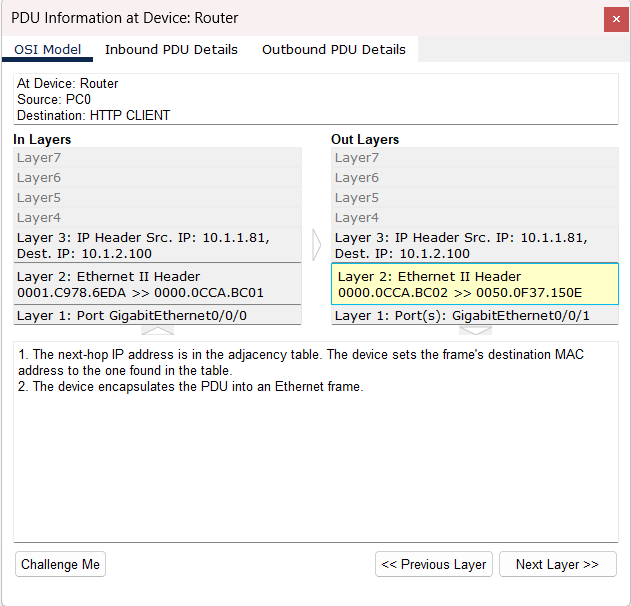
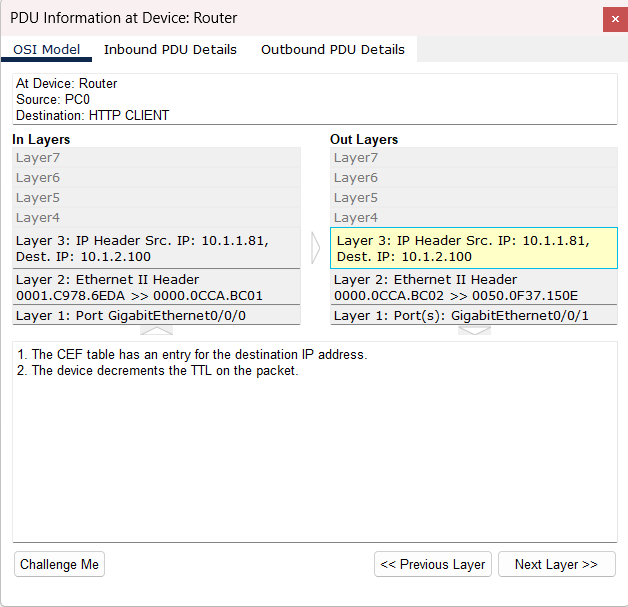
**In the network access layer,** Switch0 now has received the frame through the port FastEthernet0/1. Since the frame source MAC address was found in the MAC table of Switch0, the switch0 is able to quickly determine the associated port (GigabitEthernet0/1) to send the frame to by using the MAC address sent from PC0.

## From Router to Server



**In the network access layer,** the frame is received by GigabitEthernet0/0/0 port, the receiving port’s MAC address matches the frame’s destination MAC. Since both MAC addresses match, the router will then decapsulate the Protocol Data Unit (PDU) from the Ethernet Frame. This process will remove the Ethernet trailer ,and header which includes the source IP and destination IP.

**In the internet layer,** once the destination IP is located, the router will look up the destination IP in the CEF table. This table is a data structure that helps to map the destination IP address to the MAC address. If an entry is found in the CEP table, the router will acquire the related MAC address for further processing.

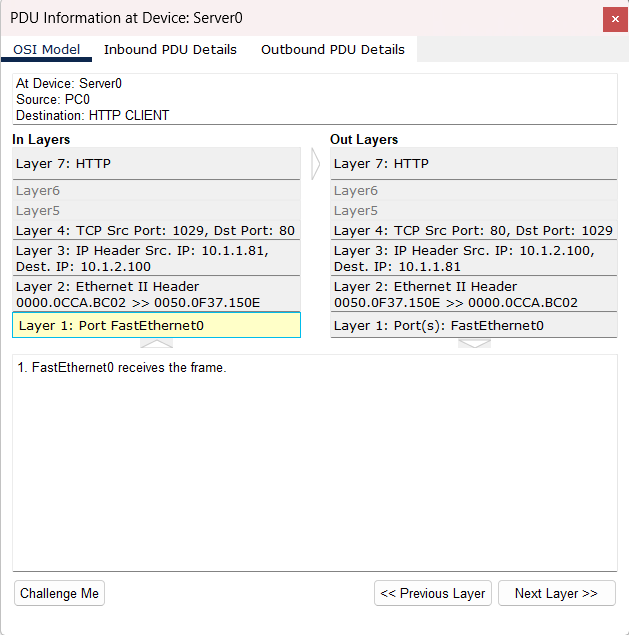
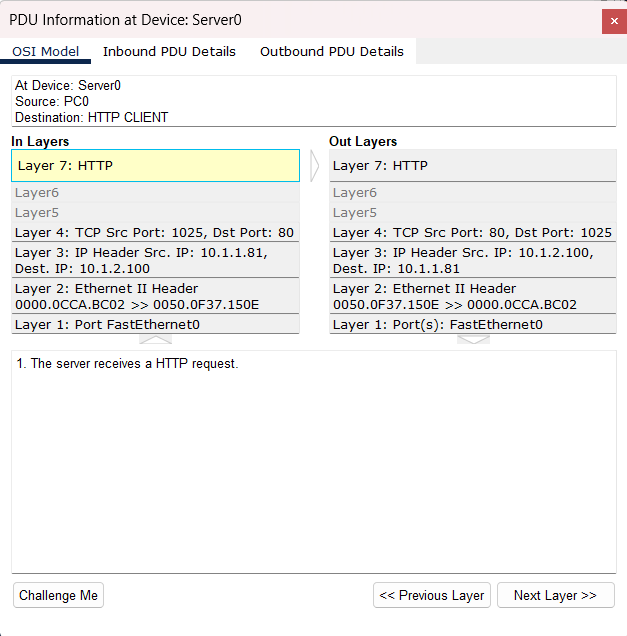
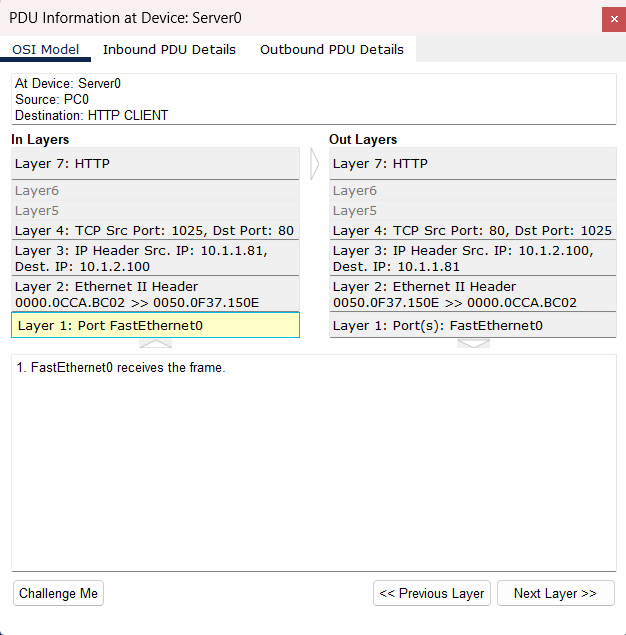


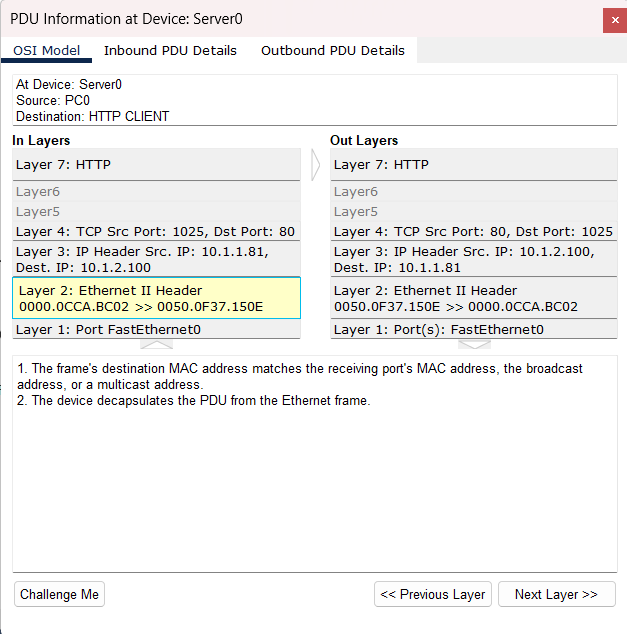
**In the internet layer,** the device will decrement the Time-to-Live (TTL) value on the packet by one. By doing this, it helps to prevent packet loops.

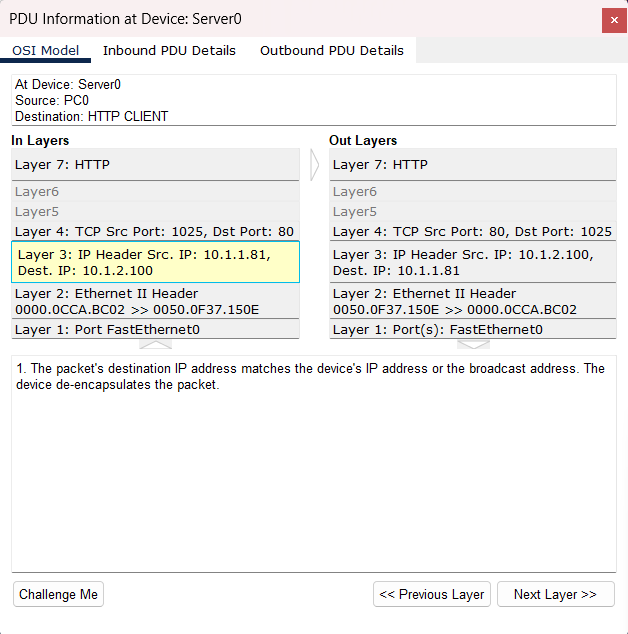
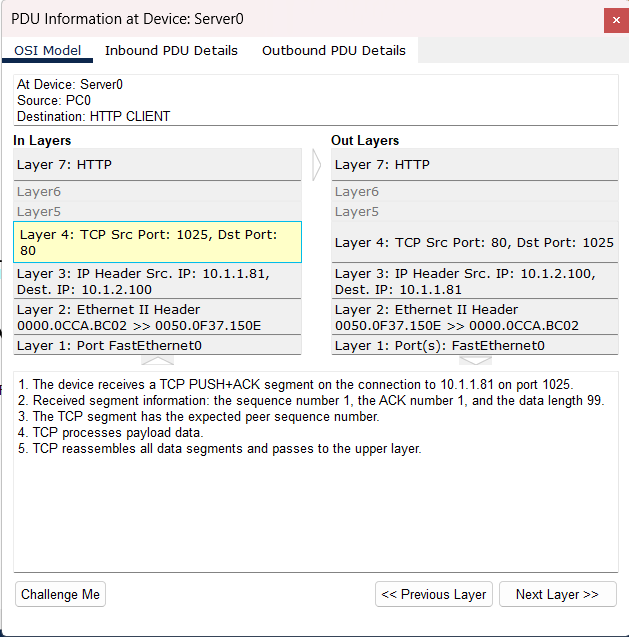
**In the network access layer,** the routing table will then map the destination IP address to the next-hop IP address. The adjacency table will also link the MAC address for the next-hop IP address. Once a connection has been determined, the router will encapsulate the PDU into a new Ethernet frame. This process will add an Ethernet header and trailer. The header contains information such as MAC address and destination MAC address.

Now that the PDU has been encapsulated into an Ethernet frame, the router will then forward the Ethernet frame through the port (GigabitEthernet0/0/1) to the next device that is related to destination IP.

## From Server to Router

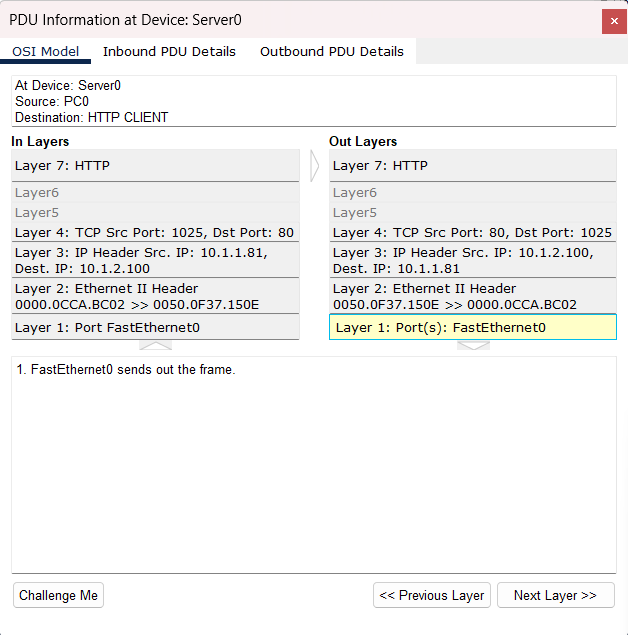
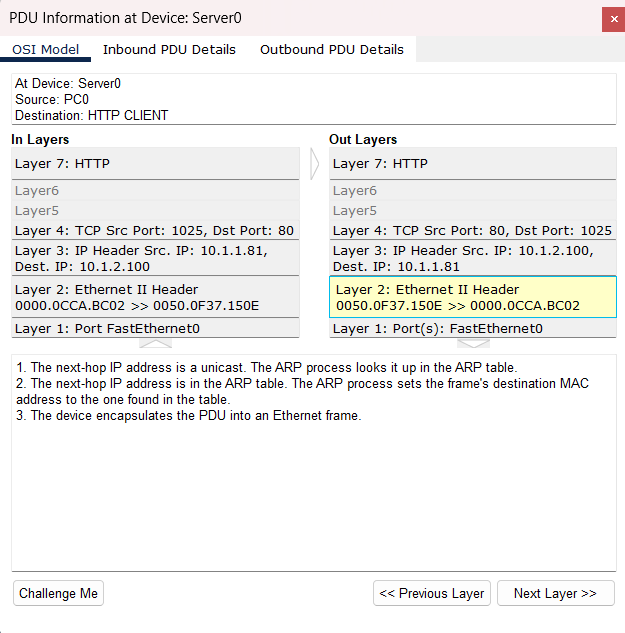
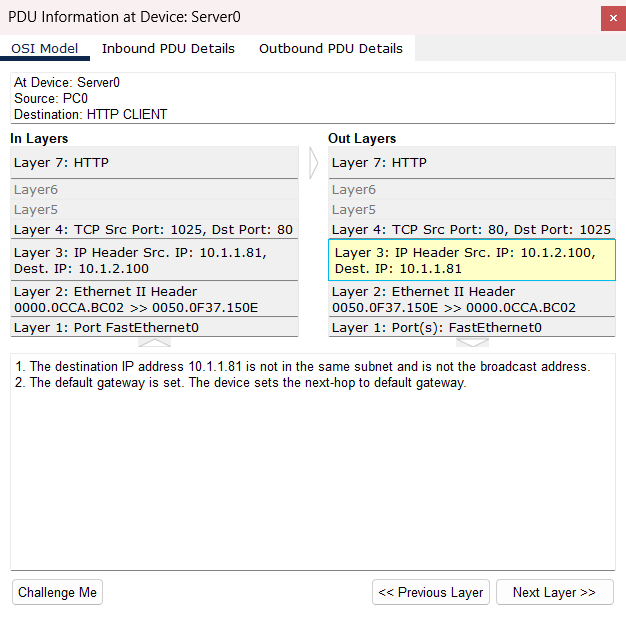
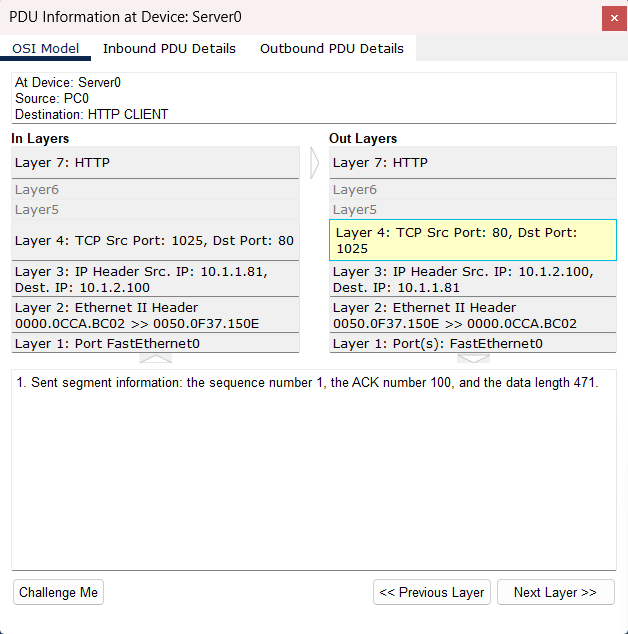
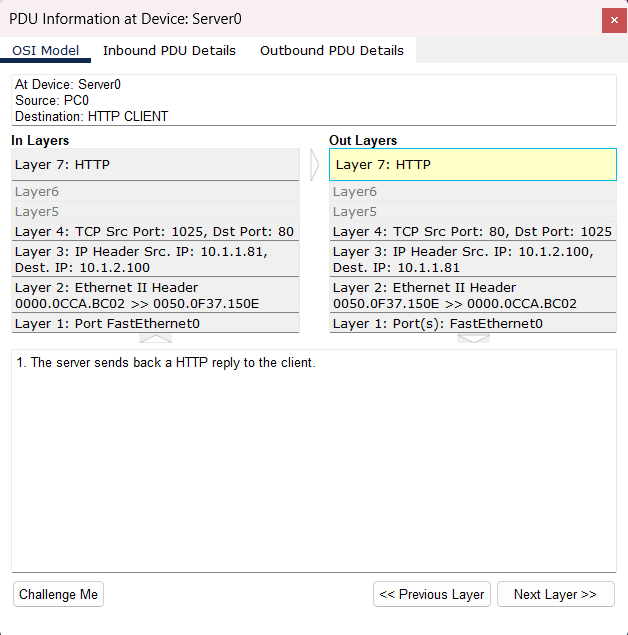
****

****

****

The **application layer** has received the HTTP request.

The device received the TCP PUSH+ACK segment in the **transport layer.** After checking all three segments if they match, the TCP will then reassemble all data segments in a complete data stream which is then passed to the upper **application layer** to be interpreted and for further processing.  
**In the network access layer:** The device (server0) will take out the destination MAC address from the frame header. It will then compare between the receiving port’s MAC address, the broadcast address, or a multicast address if it matches. After comparing, it turns out to be a unicast frame as the destination MAC address matches the MAC address that came from the FastEthernet0 port. After that, the device will decapsulate the PDU from the Ethernet frame. This process involves the removal of the Ethernet header and trailer.  
**In the network access layer:** Server0 has received the frame through FastEthernet0 port.

  
**In the application layer:** The server sends back a HTTP reply to the PC0.

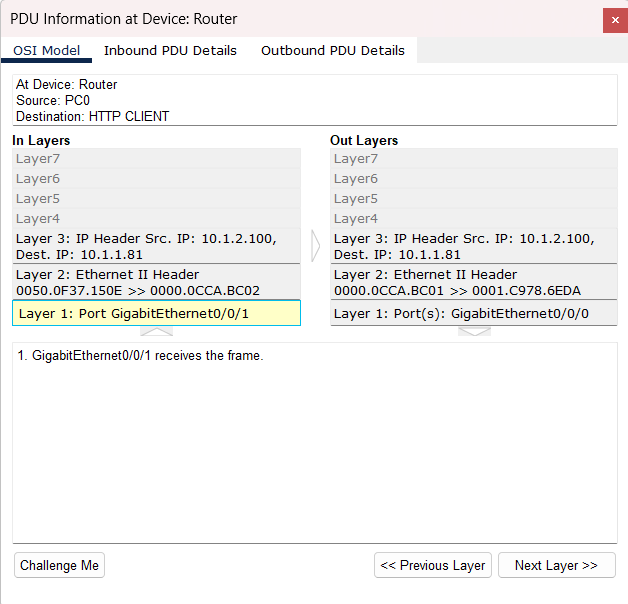
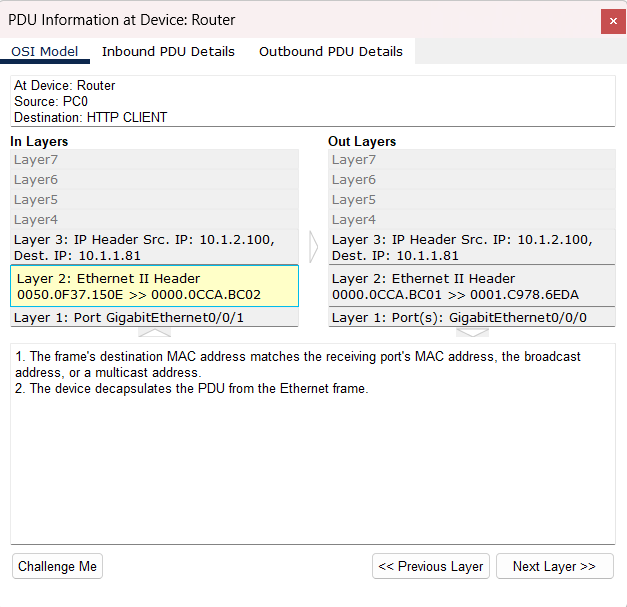
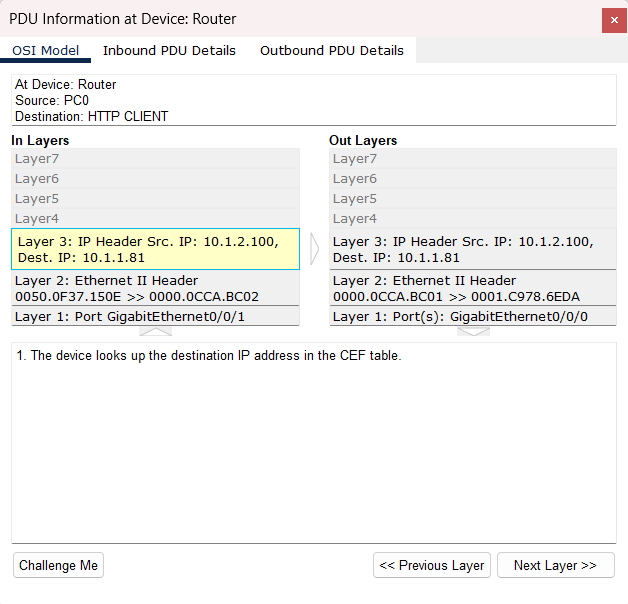
**In the transport layer:** Since it is a new Ethernet frame to be sent back for the HTTP reply, the ACK number (100) is different along side the data length (471)

**In the network layer:** Since the destination IP address is not the same subnet as the sending device. The IP packet will be sent to another device using the default gateway that was set on the server. Now the device has set the next-hop for the packet to the next device which is from the server to the router.

**In the network access layer:** The IP address is associated with a single device on the network and since the next-hop IP address is a unicast, the device must use the ARP process and look up the MAC address in the ARP table to ensure that both the IP address in the next-hop IP address is related to the MAC address. After that the ARP table will set the frame’s destination MAC address onto the IP address found in the next-hop IP address. After all that process and it’s confirmed. The device will then encapsulate the PDU into an Ethernet frame by adding an updated header and trailers that include information such as MAC address and source MAC address so that the Ethernet frame can travel smoothly back to the source IP without any failures.

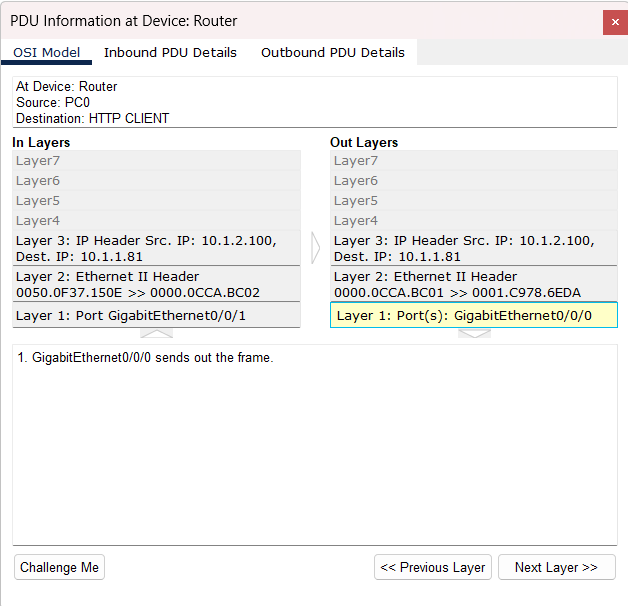
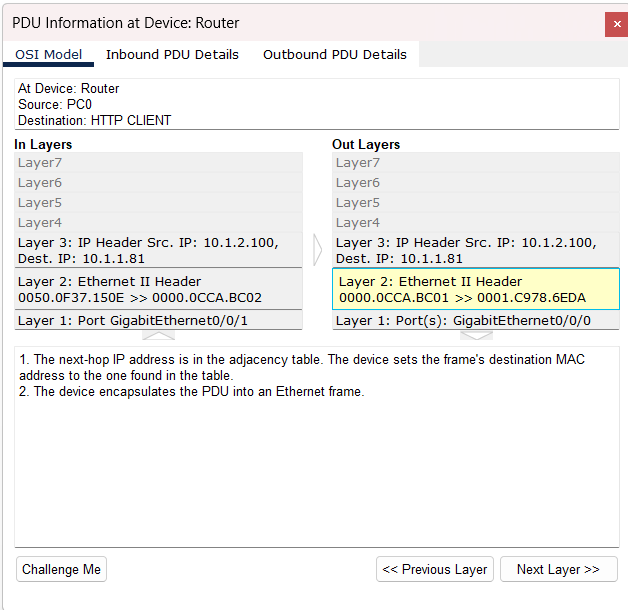
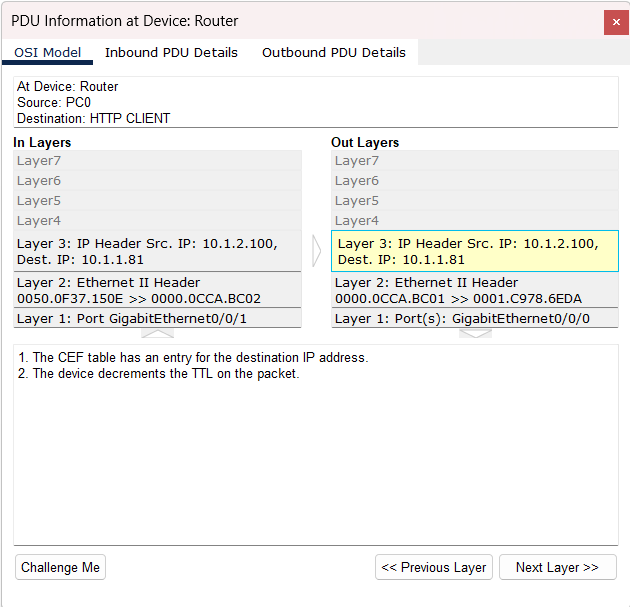
**In the network access layer:** After the PDU gets encapsulated into an Ethernet frame, it is then forward through the FastEthernet0 port to another device connected.

## From Router to Switch0



**In the network access layer:** The frame’s destination MAC address matches the receiving port’s MAC address as the device uses its network interface card (NIC) to examine the frame’s header that includes the destination MAC address. Once that both addresses match, the PDU will be decapsulated by the device for the next layer of the OSI model to further process it. The next layer would be the **network layer** which uses the CEP table.

**In the network access layer:** The device receives the Ethernet frame through GigabitEthernet0/0/1 port.

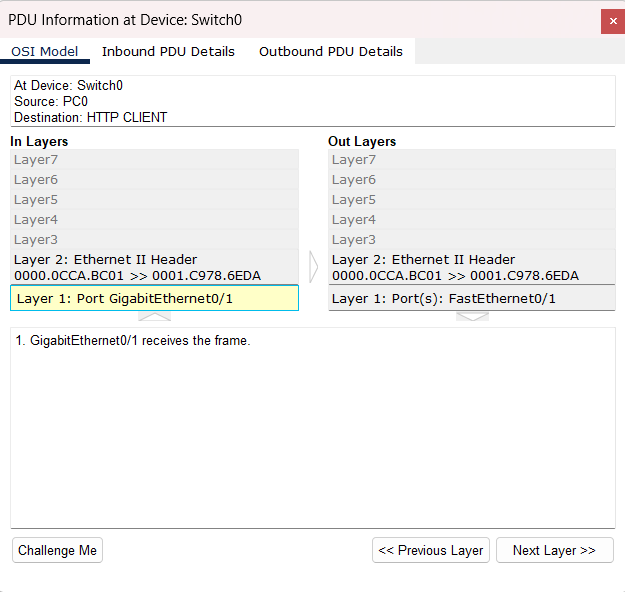
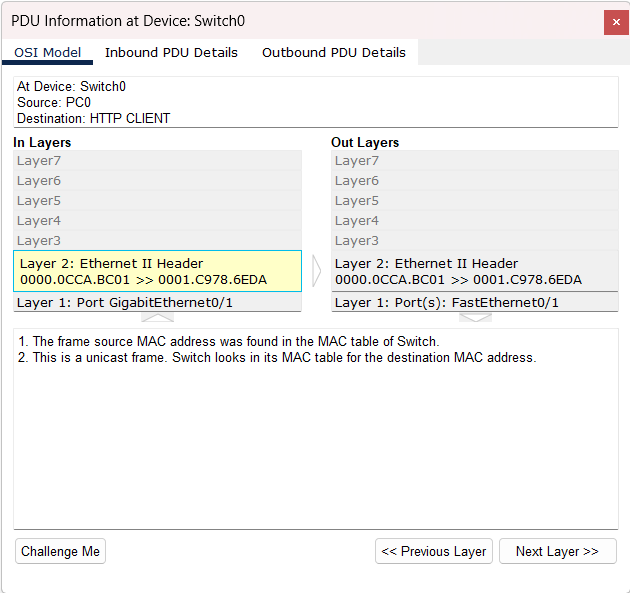


**In the internet layer:** Now that the device decapsulates the PDU for further processing, the router will then consult the packet with the CEF table to determine the next-hop IP address. This process will extract the destination IP from the packet to look up a matching prefix. Once this is done, the destination IP is returned back into the packet.  
The device will now repeat the process of TTL by decrementing the packet by one, this is to ensure that the packet does not loop indefinitely in the network if there is any error.

**In the network access layer:** As for the next step after the TTL, the router will confer the adjacency table to ensure that the MAC address in next-hop IP address is matching and correct. Once the adjacency table looks up the data list in its data structure to find the corresponding MAC address so that they can determine the next-hop IP address destination.

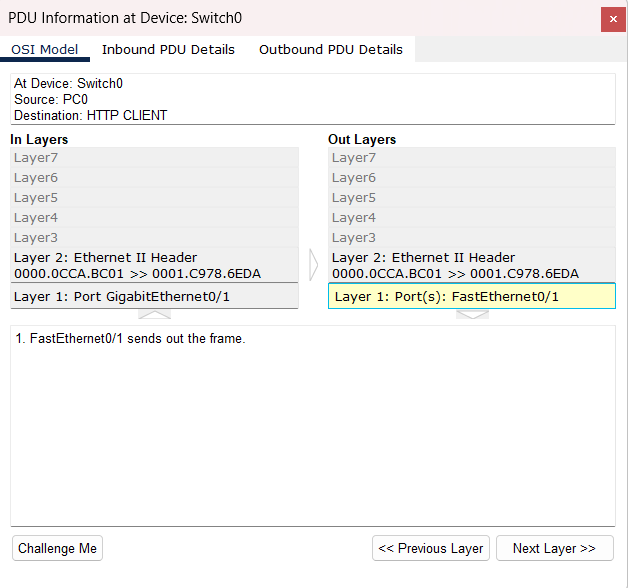
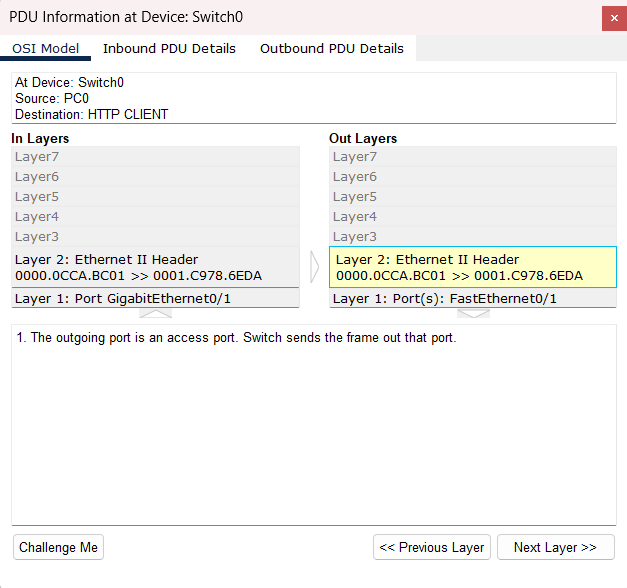
**In the network access layer:** Now that the router has the next-hop IP address, the device will encapsulate the PDU packet into an Ethernet frame to be then transmitted through the GigabitEthernet0/0/0 port.

## From Switch0 to PC0



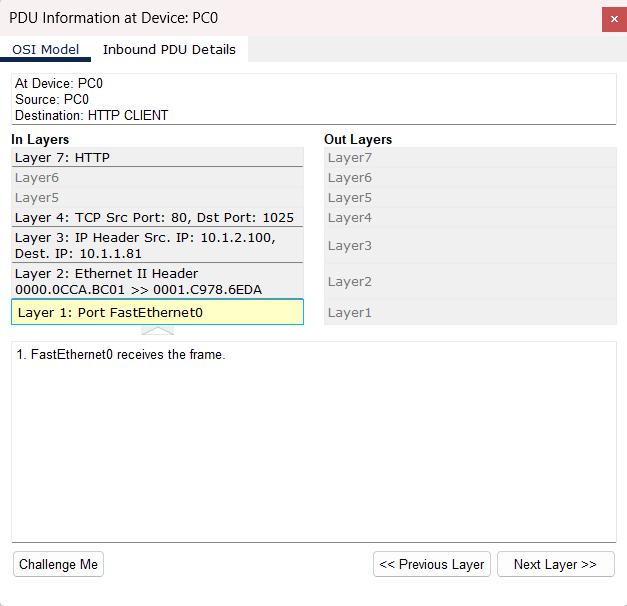
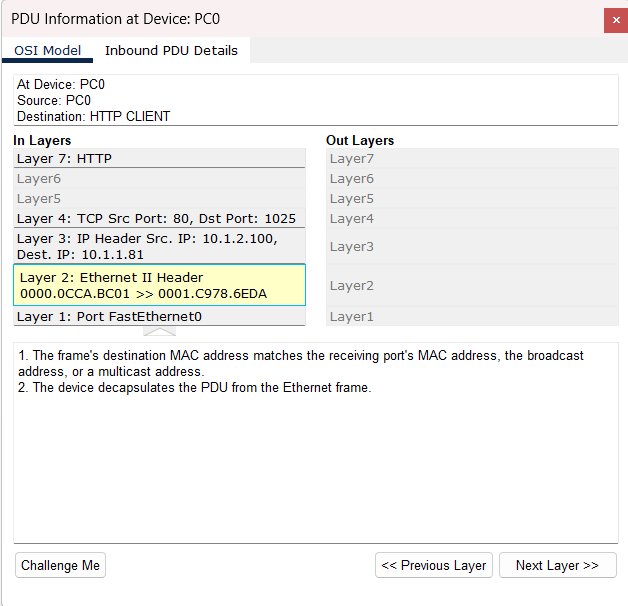
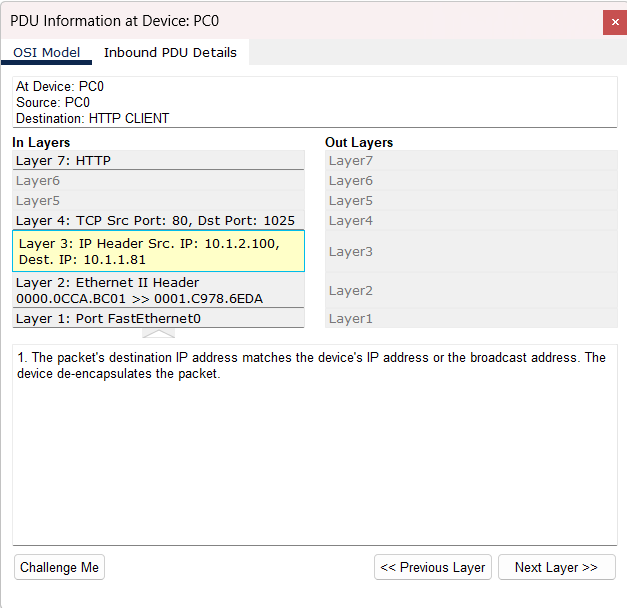
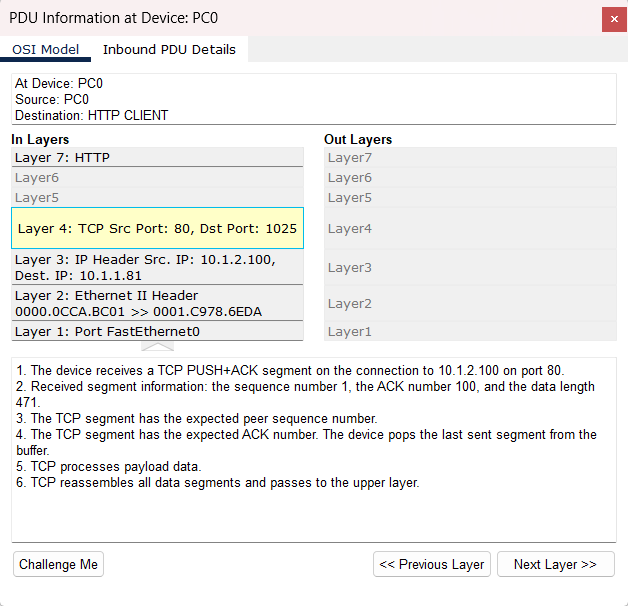
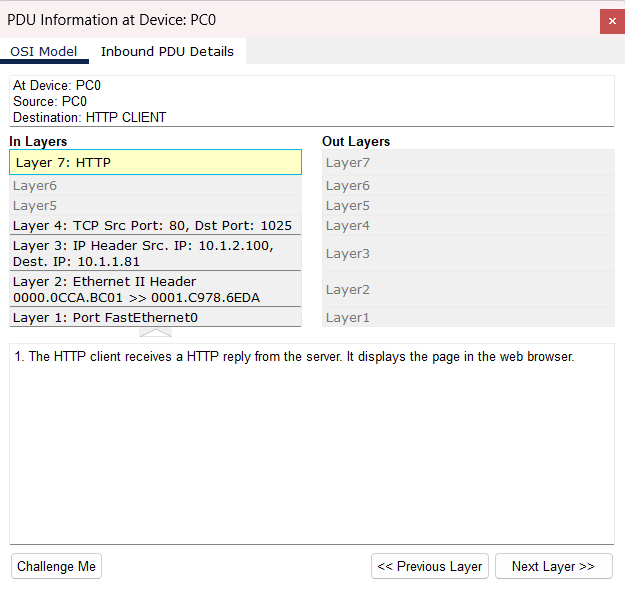
**In the network access layer:** The MAC address assigned to the Ethernet Frame is then checked by the MAC table, this process will examine the Ethernet Frame header to check for its source and destination IP. The main purpose for the MAC table is to map the MAC address in the Ethernet Frame to match the switch ports. The Ethernet frame is also a unicast frame since it is included inside the header. If the source IP address is found in the Ethernet Frame, the switch will be able to identify which device sent the Ethernet Frame and also identify the next destination to send the Ethernet Frame to.

**In the network access layer:** The Switch0 received the Ethernet frame through GigabitEthernet0/1 port.



**In the network access layer:** Since this is an end device (Switch), the switch will have an outgoing port that is an access port. This port is usually used for unicast frames forwarding and since the destination MAC address is found in the MAC table, the switch will allow the Ethernet frame to be sent out through the FastEthernet0/1 port to the next device.

## Displaying the web browser



**The application layer:** PC0 had received the HTTP reply from the server which in turn displayed the page of the web browser.  
**During the transport layer**, the device receives all the segment information that is transmitted from the server. The server port (80) and destination IP (10.1.2.100) are also the same from the beginning. The TCP segment has the same sequence number and since the received ACK number (100) has been acknowledged, the buffered segment is removed for a better data flow and increased memory. Once the transport layer has processed the payload data from the TCP segment. The updated payload data is then passed to the upper **application layer** for display.

**The network layer** now does the same in the **network access layer** but instead the device de-encapsulates the packet by removing the network header.

**The network access layer** now determines if the packet’s destination IP address matches the device’s IP address by using the MAC address header. After ensuring that both IP addresses match, the device de-encapsulates the packet by removing header and trailer.

**In the network access layer:** The device receives the Ethernet frame through the FastEthernet0 port.

# Conclusion

This assignment's main focus requires me to explain the TCP/IP model based on the TCP layer found in the simulation and, since the assignment requirement only requires me to do encapsulation and decapsulation. I managed to figure out how the TCP/IP model correlates with encapsulation and decapsulation and how I can apply the TCP/IP model.

Here are some features that TCP/IP model does, routing, encapsulation/decapsulation, addressing of IP model and checking for error.

When using the TCP/IP reference model, I learned that encapsulation and decapsulation is used on every layer of the model, this means that each time a packet is passed on to another layer, information would be added each time. For example; network layer adds source and destination port to the packet, the internet layer adds source IP and destination IP to the packet, and the network access layer adds a MAC address to the packet. This ensures information is up to date and keeps its data security and integrity everytime it gets passed onto the next device.

Looking through the cisco packet tracer for the assignment made me realize that the TCP/IP model is very beneficial in ensuring good network communication. Here are some benefits I saw when working on the assignment.

The first benefit that I saw from the simulation is how the TCP/IP model proves its reliability in making sure data is secured and reliable. The TCP/IP model contains multiple mechanisms to aid this purpose such as the routing table for efficient forwarding of packets, the CEF table to ensure quality of service policies are enforced. TTL to ensure there is no network congestion whenever there is an error in transmitting the data packet.

The second benefit would be how the TCP/IP model provides a different type of framework as it has a very flexible design. The TCP/IP model supports different types of topologies and protocols, such as HTTP, TCP/IP and many more. This is how the device is able to get the end result which would then be displayed in the application layer.

In conclusion, I have gained a valuable lesson on how the TCP/IP model works as a protocol suite. This entire assignment has taught me about how the TCP/IP model contributes greatly to network communication. The TCP/IP model reliability can ensure that whenever data is being transmitted from one device to another, it will make sure that the data packet keeps its integrity without any delay of transmission or communication.