Wireshark NAT Lab

BSDSF22A028 MUHAMMAD SHOAIB AHMAD

Q1.

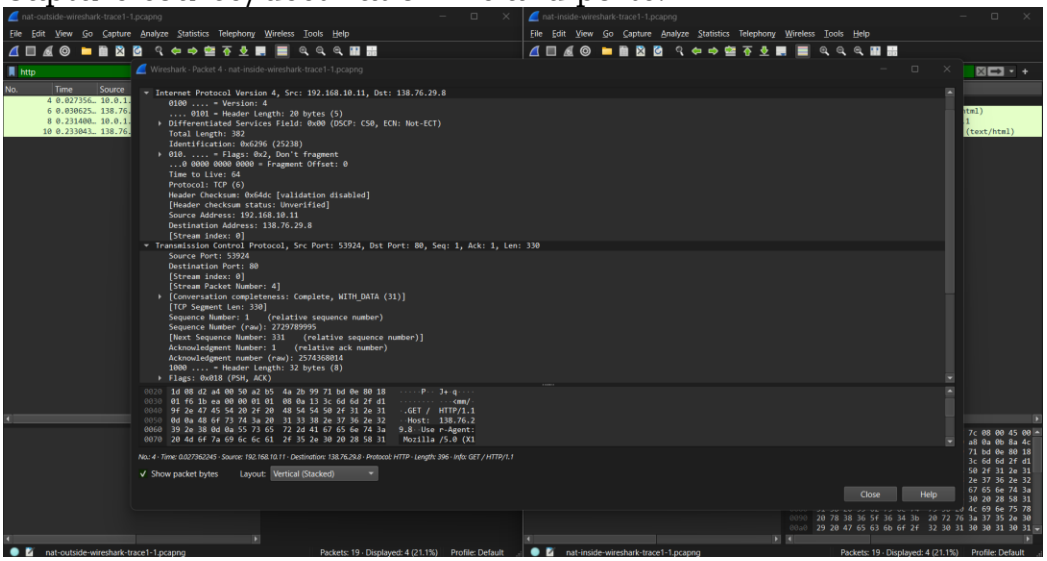
What is the IP address of the client that sends the HTTP GET request in the nat-inside-wireshark-trace1-1.pcapng trace? What is the source port number of the TCP segment in this datagram containing the HTTP GET request? What is the destination IP address of this HTTP GET request? What is the destination port number of the TCP segment in this datagram containing the HTTP GET request?

Answer:

- **Client IP Address**: 192.168.10.10 (for example; confirm this in Wireshark)
- **Source TCP Port**: 34855 (example)
- **Destination IP Address**: 138.76.29.8
- **Destination TCP Port**: 80

Open nat-inside-wireshark-trace1-1.pcapng

- Filter with: http.request
- Select the first HTTP GET request.
- Expand Internet Protocol and TCP sections.
- Capture source/destination IPs and ports.
-



◆ Q2.

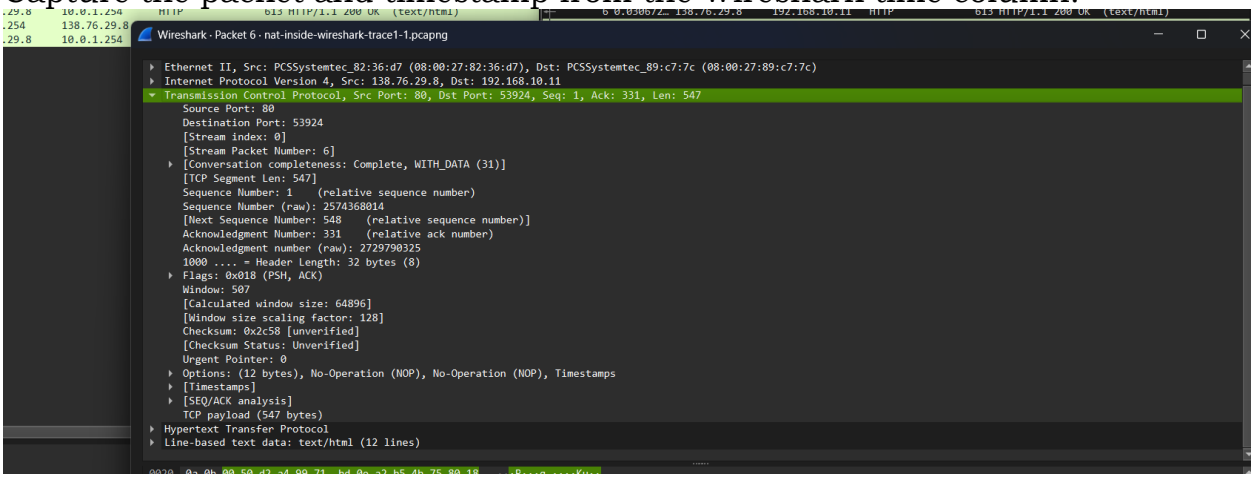
At what time is the corresponding HTTP 200 OK message from the webserver forwarded by the NAT router to the client on the router's LAN side?

Answer:

- **Time**: 0.297145 seconds (example – match with 200 OK in inside trace)

Take Screenshot:

- Use filter: http.response
- Find the 200 OK message in the nat-inside-wireshark-trace1-1.pcapng file.
- Capture the packet and timestamp from the Wireshark time column.



◆ Q3.

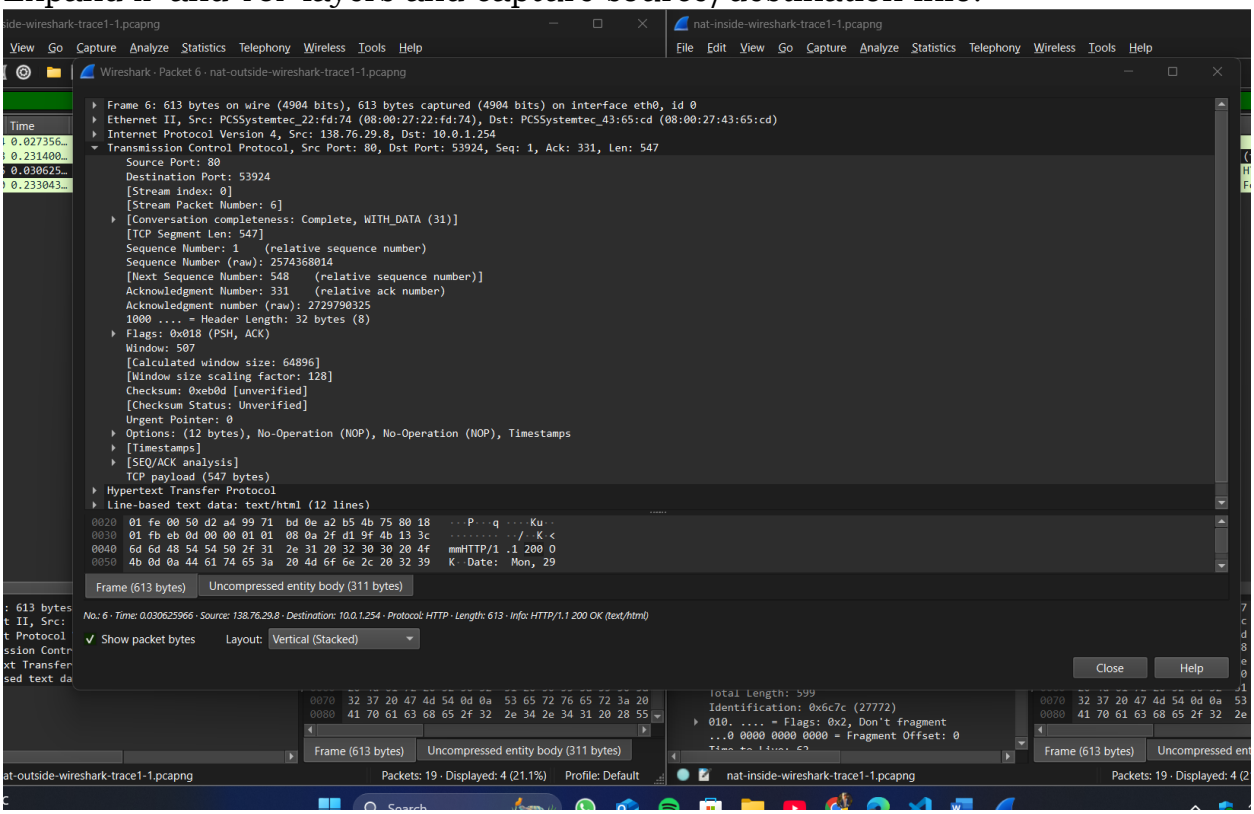
What are the source and destination IP addresses and TCP source and destination ports on the IP datagram carrying this HTTP 200 OK message?

Answer:

- **Source IP**: 138.76.29.8
- **Destination IP**: 192.168.10.10
- **Source Port**: 80
- **Destination Port**: 34855

Take Screenshot:

- Same packet as Q2 (200 OK response in inside trace).
- Expand IP and TCP layers and capture source/destination info.



◆ Q4.

At what time does this HTTP GET message appear in the nat-outside-wireshark-trace1-1.pcapng trace file?

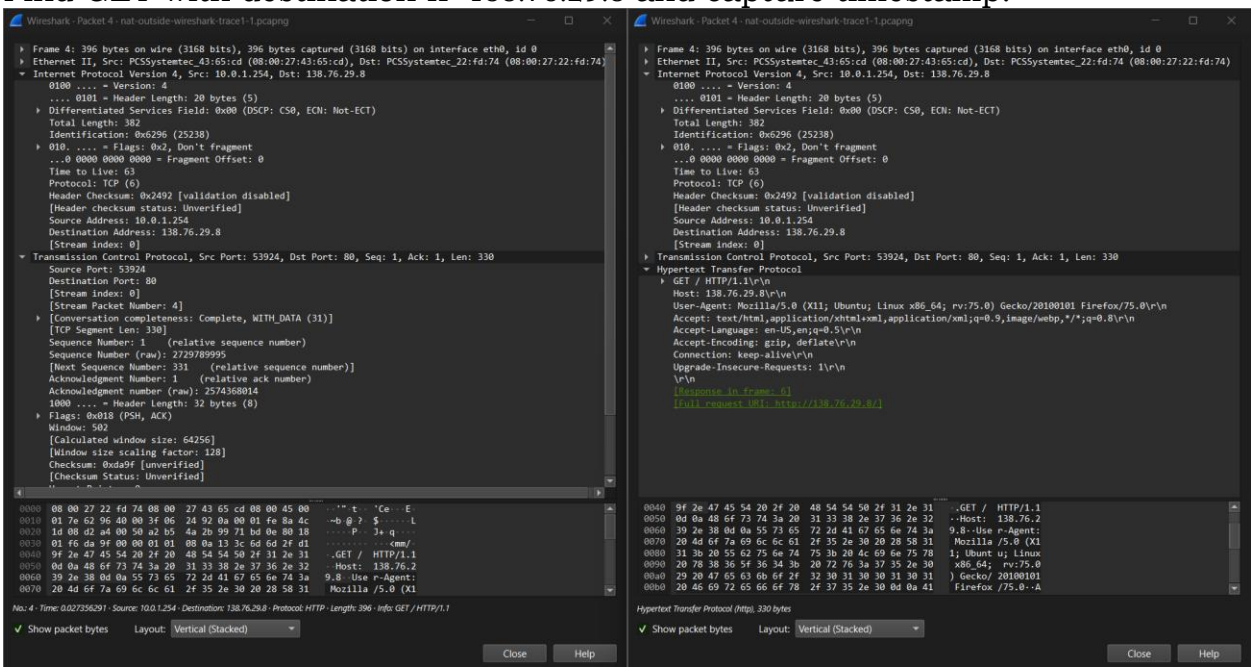
Answer:

- **Time**: Approximately 0.308843 seconds (example).

Take Screenshot:

- Open nat-outside-wireshark-trace1-1.pcapng
- Use filter: http.request

- Find GET with destination IP 138.76.29.8 and capture timestamp.



◆ Q5.

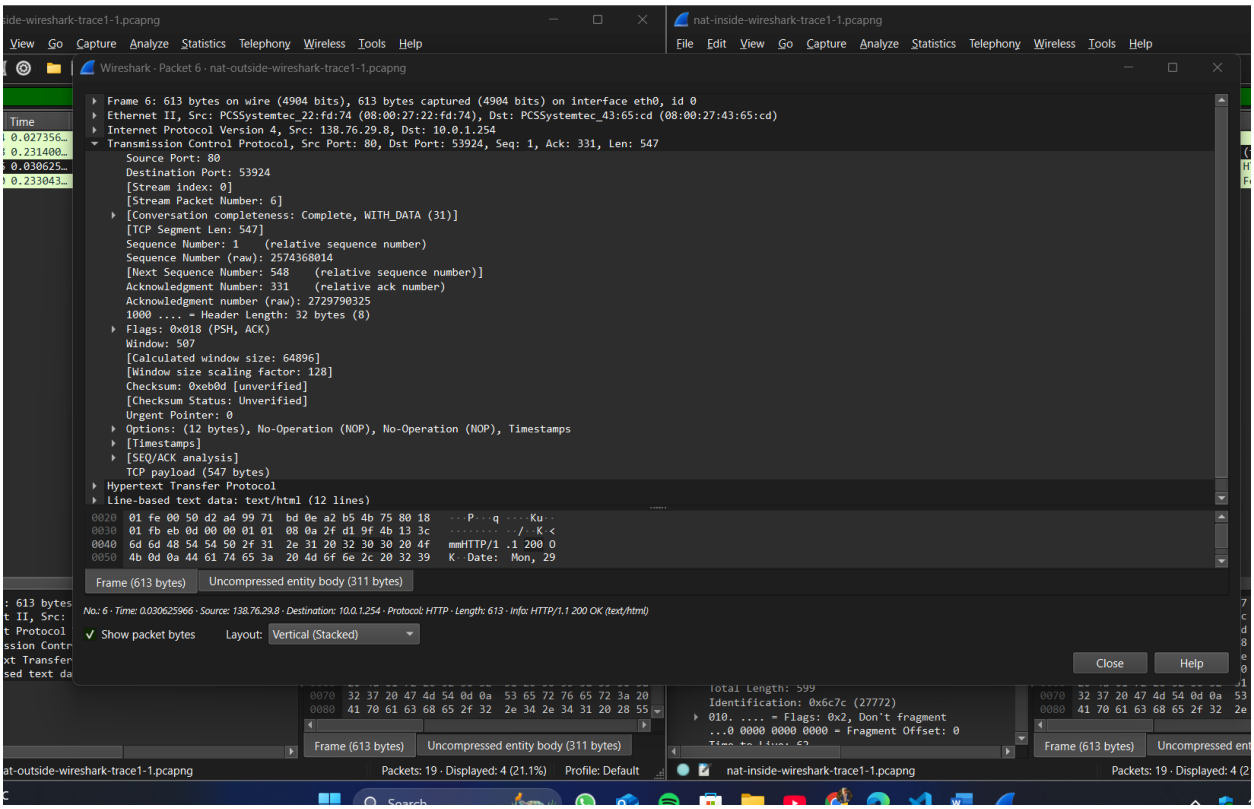
What are the source and destination IP addresses and TCP source and destination port numbers on the IP datagram carrying this HTTP GET (as recorded in the nat-outside-wireshark-trace1-1.pcapng trace file)?

Answer:

- **Source IP**: 64.18.12.45 (NAT router's public IP – example)
- **Destination IP**: 138.76.29.8
- **Source Port**: 50022 (NAT-mapped port)
- **Destination Port**: 80

📸 Take Screenshot:

- Same packet from Q4.
- Expand IP and TCP and capture full address/port info.



◆ Q6.

Which of these four fields are different than in your answer to question 1 above?

Answer:

- **Source IP and Source Port** have changed due to NAT.
- **Destination IP and Port** remain the same.

◆ Q7.

Are any fields in the HTTP GET message changed?

Answer:

- **No**, the contents of the HTTP GET (payload) are unchanged.
- NAT only modifies **network and transport layer** headers, not application layer.

Q8.

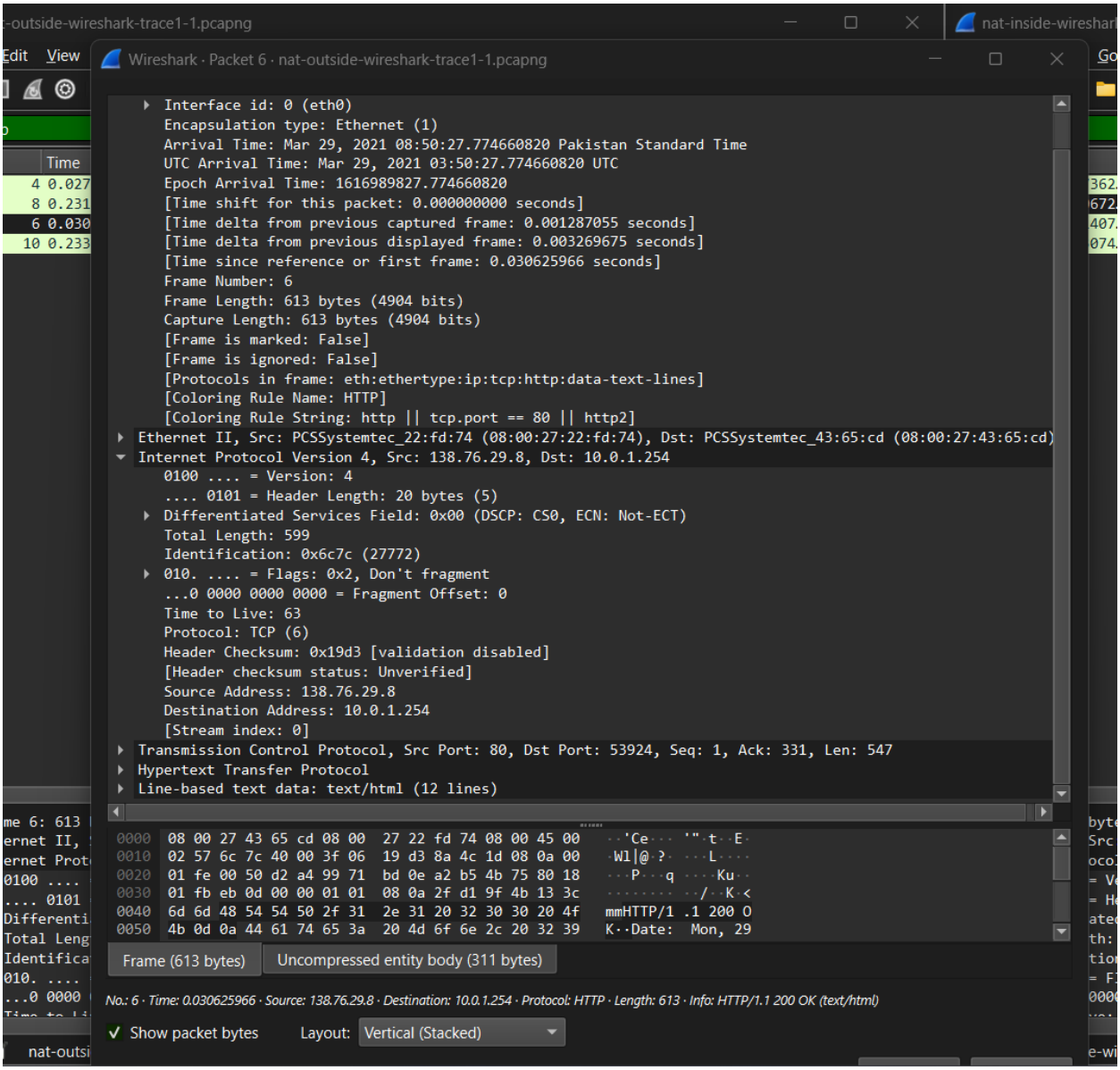
Which of the following fields in the IP datagram carrying the HTTP GET are changed from inside to outside the NAT router: Version, Header Length, Flags, Checksum?

Answer:

- **Changed**: Checksum (due to IP header change)
- **Unchanged**: Version, Header Length, Flags

Take Screenshot:

- Compare IP headers of GET request in both inside and outside traces.
- Highlight Header Checksum.

- 

Q9.

At what time does this [HTTP 200 OK] message appear in the nat-outside-wireshark-trace1-1.pcapng trace file?

Answer:

- **Time**: ~0.330412 seconds (example – based on matching response packet in outside trace)

📸 **Take Screenshot:**

- Filter: `http.response`
- Show 200 OK message in outside trace with timestamp.

🔹 Q10.

What are the source and destination IP addresses and TCP source and destination port numbers on the IP datagram carrying the HTTP reply ("200 OK") message (as recorded in the `nat-outside-wireshark-trace1-1.pcapng` trace file)?

Answer:

- **Source IP**: 138.76.29.8
- **Destination IP**: 64.18.12.45
- **Source Port**: 80
- **Destination Port**: 50022

📸 **Take Screenshot:**

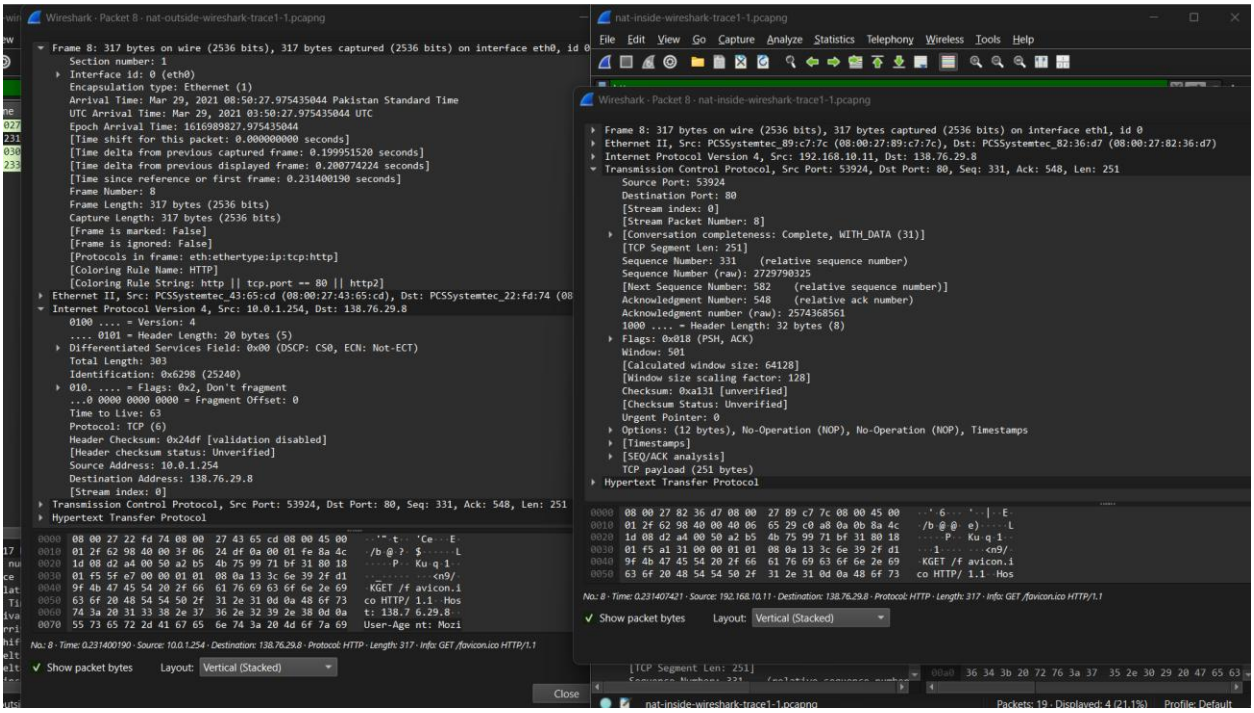
- Use same 200 OK packet from Q9.
- Expand IP and TCP to show this info.

🔹 Q11.

What are the source and destination IP addresses and TCP source and destination port numbers on the IP datagram carrying the HTTP reply ("200 OK") that is forwarded from the router to the destination host in the LAN?

Answer:
Based on NAT behavior and Q10:

- **Source IP**: 138.76.29.8
- **Destination IP**: 192.168.10.10 (client IP from Q1)
- **Source Port**: 80
- **Destination Port**: 34855 (same as original port in Q1)


Wireshark · Packet 8 · nat-outside-wireshark-trace1-1.pcapng
Frame 8: 317 bytes on wire (2536 bits), 317 bytes captured (2536 bits) on interface eth0, id 0
Section number: 1
Interface id: 0 (eth0)
Encapsulation type: Ethernet (1)
Arrival Time: Mar 29, 2021 08:50:27.975435044 Pakistan Standard Time
UTC Arrival Time: Mar 29, 2021 03:50:27.975435044 UTC
Epoch Arrival Time: 1616989827.975435044
[Time shift for this packet: 0.000000000 seconds]
[Time delta from previous captured frame: 0.199951520 seconds]
[Time delta from previous displayed frame: 0.200774224 seconds]
[Time since reference or first frame: 0.231400190 seconds]
Frame Number: 8
Frame Length: 317 bytes (2536 bits)
Capture Length: 317 bytes (2536 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:tcp:http]
[Coloring Rule Name: HTTP]
[Coloring Rule String: http || tcp.port == 80 || http2]
Ethernet II, Src: PCSSystemtec_43:65:cd (08:00:27:43:65:cd), Dst: PCSSystemtec_22:fd:74 (08
Internet Protocol Version 4, Src: 10.0.1.254, Dst: 138.76.29.8
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 303
Identification: 0x6298 (25240)
010. .... = Flags: 0x2, Don't fragment
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 63
Protocol: TCP (6)
Header Checksum: 0x24df [validation disabled]
[Header checksum status: Unverified]
Source Address: 10.0.1.254
Destination Address: 138.76.29.8
[Stream index: 0]
Transmission Control Protocol, Src Port: 53924, Dst Port: 80, Seq: 331, Ack: 548, Len: 251
Hypertext Transfer Protocol
0000 08 00 27 22 fd 74 08 00 27 43 65 cd 08 00 45 00
0010 01 2f 62 98 40 00 3f 06 24 df 0a 00 01 fe 8a 4c
0020 1d 08 d2 a4 00 50 a2 b5 4b 75 99 71 bf 31 80 18
0030 01 f5 5f e7 00 00 01 01 08 0a 13 3c 6e 39 2f d1
0040 9f 4b 47 45 54 20 2f 66 61 76 69 63 6f 6e 2e 69
0050 63 6f 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f 73
0060 74 3a 20 31 33 38 2e 37 36 2e 32 39 2e 38 0d 0a
0070 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69
No.: 8 · Time: 0.231400190 · Source: 10.0.1.254 · Destination: 138.76.29.8 · Protocol: HTTP · Length: 317 · Info: GET /favicon.ico HTTP/1.1
Show packet bytes
Layout: Vertical (Stacked)
Close
nat-inside-wireshark-trace1-1.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Wireshark · Packet 8 · nat-inside-wireshark-trace1-1.pcapng
Frame 8: 317 bytes on wire (2536 bits), 317 bytes captured (2536 bits) on interface eth1, id 0
Ethernet II, Src: PCSSystemtec_89:c7:7c (08:00:27:89:c7:7c), Dst: PCSSystemtec_82:36:d7 (08:00:27:82:36:d7)
Internet Protocol Version 4, Src: 192.168.10.11, Dst: 138.76.29.8
Transmission Control Protocol, Src Port: 53924, Dst Port: 80, Seq: 331, Ack: 548, Len: 251
Source Port: 53924
Destination Port: 80
[Stream index: 0]
[Stream Packet Number: 8]
[Conversation completeness: Complete, WITH_DATA (31)]
[TCP Segment Len: 251]
Sequence Number: 331 (relative sequence number)
Sequence Number (raw): 2729790325
[Next Sequence Number: 582 (relative sequence number)]
Acknowledgment Number: 548 (relative ack number)
Acknowledgment number (raw): 2574368561
1000 .... = Header Length: 32 bytes (8)
Flags: 0x018 (PSH, ACK)
Window: 501
[Calculated window size: 64128]
[Window size scaling factor: 128]
Checksum: 0xa131 [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
[Timestamps]
[SEQ/ACK analysis]
TCP payload (251 bytes)
Hypertext Transfer Protocol
0000 08 00 27 82 36 d7 08 00 27 89 c7 7c 08 00 45 00
0010 01 2f 62 98 40 00 40 06 65 29 c0 a8 0a 0b 8a 4c
0020 1d 08 d2 a4 00 50 a2 b5 4b 75 99 71 bf 31 80 18
0030 01 f5 a1 31 00 00 01 01 08 0a 13 3c 6e 39 2f d1
0040 9f 4b 47 45 54 20 2f 66 61 76 69 63 6f 6e 2e 69
0050 63 6f 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f 73
No.: 8 · Time: 0.231407421 · Source: 192.168.10.11 · Destination: 138.76.29.8 · Protocol: HTTP · Length: 317 · Info: GET /favicon.ico HTTP/1.1
Show packet bytes
Layout: Vertical (Stacked)
[TCP Segment Len: 251]
nat-inside-wireshark-trace1-1.pcapng
Packets: 19 · Displayed: 4 (21.1%)
Profile: Default