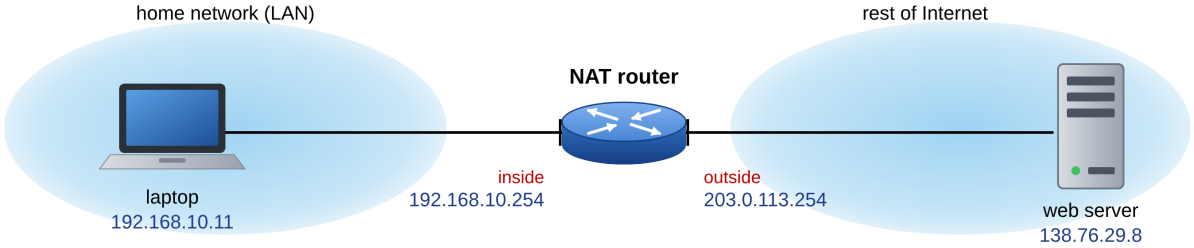
CS 43 NAT worksheet: one request, two sides of the router

A laptop at home opens a web page. We captured the same packets on both sides of the home's NAT router. ▸ marks a collapsed line, as in Wireshark. The Ethernet (link-layer) line is left out.



Part 1. The request leaves home

Packet A was captured on the LAN side of the router. Packet B is the same packet, captured on the Internet side.

Packet A (captured on the LAN side, inside the home)

```
No.  Source           Destination      Protocol  Length  Info
7    192.168.10.11    138.76.29.8      HTTP      396     GET / HTTP/1.1

▸ Frame 7: 396 bytes on wire (3168 bits), 396 bytes captured (3168 bits)
▾ Internet Protocol Version 4, Src: 192.168.10.11, 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: 382
      Identification: 0x6296 (25238)
    ▸ 010. .... = Flags: 0x2, Don't fragment
      ...0 0000 0000 0000 = Fragment Offset: 0
      Time to Live: 64
      Protocol: TCP (6)
      Header Checksum: 0x64dc
      Source Address: 192.168.10.11
      Destination Address: 138.76.29.8
▾ Transmission Control Protocol, Src Port: 53924, Dst Port: 80, Seq: 1, Ack:
1, Len: 330
      Source Port: 53924
      Destination Port: 80
      Sequence Number: 1    (relative sequence number)
      Acknowledgment Number: 1    (relative ack number)
      1000 .... = Header Length: 32 bytes (8)
    ▸ Flags: 0x018 (PSH, ACK)
      Checksum: 0x1bea
    ▸ Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
▾ Hypertext Transfer Protocol
      GET / HTTP/1.1\r\n
      Host: 138.76.29.8\r\n
      ...
```

Packet B (captured on the Internet side, outside the home)

```
No.  Source           Destination      Protocol  Length  Info
8    203.0.113.254    138.76.29.8      HTTP      396     GET / HTTP/1.1

▸ Frame 8: 396 bytes on wire (3168 bits), 396 bytes captured (3168 bits)
▾ Internet Protocol Version 4, Src: 203.0.113.254, 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: 382
      Identification: 0x6296 (25238)
    ▸ 010. .... = Flags: 0x2, Don't fragment
      ...0 0000 0000 0000 = Fragment Offset: 0
      Time to Live: 63
      Protocol: TCP (6)
      Header Checksum: 0xf390
      Source Address: 203.0.113.254
      Destination Address: 138.76.29.8
▾ Transmission Control Protocol, Src Port: 60000, Dst Port: 80, Seq: 1, Ack:
1, Len: 330
      Source Port: 60000
      Destination Port: 80
      Sequence Number: 1    (relative sequence number)
      Acknowledgment Number: 1    (relative ack number)
      1000 .... = Header Length: 32 bytes (8)
    ▸ Flags: 0x018 (PSH, ACK)
      Checksum: 0xa99e
    ▸ Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
▾ Hypertext Transfer Protocol
      GET / HTTP/1.1\r\n
      Host: 138.76.29.8\r\n
      ...
```

1. Circle every value in Packet B that is different from Packet A.

Part 1 questions

2. There are two changes that happen at every router or NAT. Which ones? Explain why.

A. Source IP address and source port
B. Identification and header checksum
C. Time to Live and header checksum
D. Time to Live and source IP address
E. Header checksum and TCP checksum

Every router will decrement the TTL and since the TTL is decremented it will have to recompute the IP header checksum.

3. Which changes happen only because this router is a NAT?

The Source IP address, the source port, and the TCP checksum.

4. Compare the TCP checksum in Packets A and B. The TCP checksum is computed over the TCP segment plus the source and destination IP addresses. Did it change? Why? What does that say about which layers a NAT has to touch?

Yes it changed. The NAT router had to re-write the source port showing that it has to touch the TCP header.

Part 2. The reply comes back

Packet C is the server's reply, captured on the Internet side. Fill in the blanks (_____) in Packet D, the same reply after the NAT forwards it onto the LAN. You cannot compute the checksums by hand; for those, write "same as C" or "changed". The ? values repeat fields you fill in below them.

Packet C (captured on the Internet side, outside the home)

```
No.  Source           Destination      Protocol  Length  Info
11   138.76.29.8      203.0.113.254    HTTP      613     HTTP/1.1 200 OK


▸ Frame 11: 613 bytes on wire (4904 bits), 613 bytes captured (4904 bits)
▾ Internet Protocol Version 4, Src: 138.76.29.8, Dst: 203.0.113.254
      0100 .... = Version: 4
      .... 0101 = Header Length: 20 bytes (5)
    ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      Total Length: 599
      Identification: 0x6c7c (27772)
    ▸ 010. .... = Flags: 0x2, Don't fragment
      ...0 0000 0000 0000 = Fragment Offset: 0
      Time to Live: 63
      Protocol: TCP (6)
      Header Checksum: 0xe8d1
      Source Address: 138.76.29.8
      Destination Address: 203.0.113.254
▾ Transmission Control Protocol, Src Port: 80, Dst Port: 60000, Seq: 1, Ack:
331, Len: 547
      Source Port: 80
      Destination Port: 60000
      Sequence Number: 1    (relative sequence number)
      Acknowledgment Number: 331    (relative ack number)
      1000 .... = Header Length: 32 bytes (8)
    ▸ Flags: 0x018 (PSH, ACK)
      Checksum: 0xba0c
    ▸ Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
▾ Hypertext Transfer Protocol
      HTTP/1.1 200 OK\r\n
      Date: Mon, 29 Mar 2021 03:50:27 GMT\r\n
      ...
```

Packet D (captured on the LAN side, inside the home)

```
No.  Source           Destination      Protocol  Length  Info
12   ?                ?                HTTP      613     HTTP/1.1 200 OK


▸ Frame 12: 613 bytes on wire (4904 bits), 613 bytes captured (4904 bits)
▾ Internet Protocol Version 4, Src: ?, Dst: ?
      0100 .... = Version: 4
      .... 0101 = Header Length: 20 bytes (5)
    ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      Total Length: 599
      Identification: 0x6c7c (27772)
    ▸ 010. .... = wFlags: 0x2, Don't fragment
      ...0 0000 0000 0000 = Fragment Offset: 0

      Time to Live: ______62_______
      Protocol: TCP (6)
      Header Checksum: 0x5c1d

      Source Address: ___138.76.29.8_____

      Destination Address: __192.168.10.11____
▾ Transmission Control Protocol, Src Port: ?, Dst Port: ?, Seq: 1, Ack: 331,
Len: 547
      Source Port: ______80_______

      Destination Port: ___53924_____
      Sequence Number: 1    (relative sequence number)
      Acknowledgment Number: 331    (relative ack number)
      1000 .... = Header Length: 32 bytes (8)
    ▸ Flags: 0x018 (PSH, ACK)
      Checksum: 0xa99e
    ▸ Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
▾ Hypertext Transfer Protocol
      HTTP/1.1 200 OK\r\n
      Date: Mon, 29 Mar 2021 03:50:27 GMT\r\n
      ...
```

5. Write the NAT translation table entry the router used to turn C into D.

Outside (WAN) side: address, port	Inside (LAN) side: address, port
203.0.113.254, 60000	**192.168.10.11, 53924**