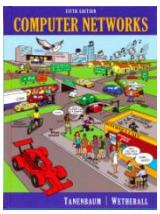
Solutions – ICMP



The solutions below are based on our capture and use of tools. Your answers will differ in the details if they are based on your own capture and use of tools in a different network setting. Nonetheless, we expect our solutions to help you understand whether your answers are correct.

Step 2: Echo (ping) Packets

Answers to the questions:

1. Echo request has Type/Code of 8/0. Echo reply has Type/Code of 0/0.
2. Each echo request and corresponding echo reply have the same Identifier value and the same Sequence Number value. The values are used to match the echo request to the right echo reply.
3. Typically, the Identifier is kept the same and the Sequence Number is incremented. This ensures that as a pair, successive echo requests will have different Identifier/Sequence Number values so they (and their corresponding replies) can be distinguished.
4. The data is the same. The echo request sender can use any convenient data, and the echo reply sender will copy its data from the request so that the payload returns to the original sender.

Step 3: TTL Exceeded (traceroute) Packets

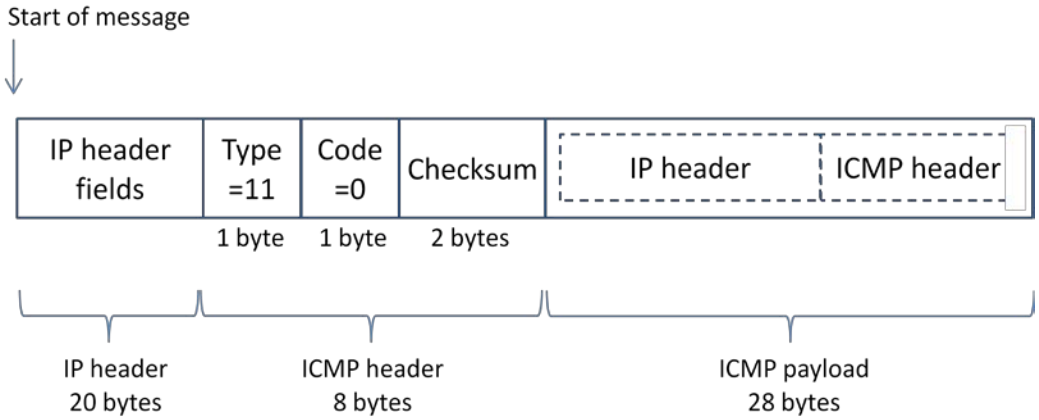


Figure 1: Format of an ICMP TTL Exceeded Message

There are several features to note:

- The length of 20 bytes is for a typical IPv4 header with no IP option fields.
- The Type and Code values are for an ICMP TTL Exceeded in transit message.
- The ICMP header is given as 8 bytes, yet the fields only add up to 4 bytes. There are an extra four bytes after the checksum that are historically unused. They are not shown in the figure because they are not shown in most versions of Wireshark.

- The size of the ICMP payload depends on the router implementation. The value of 28 bytes is what we saw in practice. The start of an IP packet is shown in these bytes, including an IP header and ICMP header for the echo request packet that triggered the ICMP TTL Exceeded message.

Answers to the questions:

1. Type=11 (Time Exceeded) and Code=0 (TTL Exceeded in transit)
2. All ICMP messages start with the same Type/Code (and Checksum) fields, so the receiver can process these fields. Their value tells the receiver the kind of ICMP message, and hence what fields follow.
3. The Type/Code and Checksum fields take up 4 bytes. However, the ICMP header is actually 8 bytes long. These fields are followed by 4 bytes that are unused (except for recent ICMP extensions) and hence do not show up in Wireshark as named fields. You can still see that they are there by selecting the ICMP block and the payload, and observing that they differ by 8 bytes.
4. The inner IP packet has TTL=1 in our case, but depending on the router implementation it is possible that you will see TTL=0. It must be one of these values for the case of an ICMP TTL Exceeded message because the message is triggered when the TTL is decremented during processing and reaches 0, i.e., the TTL held a value of 1 when the packet arrived at the router.

Step 4: Internet Paths

Answers to the questions:

1. The IP source address of the TTL Exceeded packet is the IP address of the router. This is because the router created the TTL Exceeded packet, putting its own IP address in the source field.
2. Traceroute probes each hop along the path more than once, in case of packet loss. Typically it probes three times, in which case you will see a pattern of triples of echo / TTL exceeded from a given router. This pattern will not be exact because some TTL Exceeded packets may be lost, and some routers may not reply with TTL exceeded. These lost TTL Exceeded packets correspond to the "*" entries in the traceroute text output.
3. The echo request packet should have an IP source of your computer, an IP destination of the far end of the path, and a TTL value set to N. The last part is the key; routers will decrement the TTL and it will reach zero N hops away from the source towards the destination. The ICMP TTL Exceeded message will be sent back to the source. Note that the contents of the ICMP fields in the echo request packet do not matter. They are there only in case the packet reaches the destination (which would then send an echo reply).

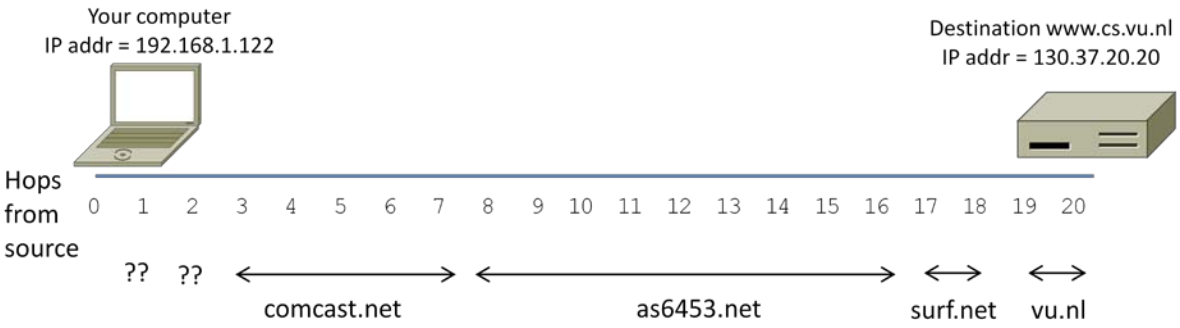


Figure 2: Path from computer to www.cs.vu.nl found by `traceroute`

There are several features to note:

- The start of the path is not named because it starts within a home; the address 192.168.xx.xx is in private address space that is NATed to reach the public Internet. This will likely be the case if you run the traceroute from a home.
- as6453.net is Tata Communications, comcast.net is Comcast, surf.net is SURFnet, and vu.nl is Vrijie Universitiet Amsterdam. You can often find names like this with a Web search and an educated guess, or by using a WhoIS lookup service such as whois.net to consult domain registration records.

[END]