Richard Aviles

10/31/2017

Wireshark Lab #5 - ICMP

1) The IP address of the host is 192.168.1.101. The IP address of the destination host is 143.89.14.34.

2) There is not a source and destination port number because the architecture is designed so that the information is communicated between the host and the routers.

3) The type is 8 and the code number is 0. Other fields include checksum, identifier (BE), identifier (LE), sequence number (BE), sequence number (LE), and data. The checksum, sequence number, and identifier fields are all 2 bytes.

4) The type is 0 and the code is 0. Other fields include checksum, identifier (BE), identifier (LE), sequence number (BE), sequence number (LE), and data. The checksum, sequence number, and identifier fields are all 2 bytes.

5) The IP address of the host is 192.168.1.101. The IP address of the destination host is 138.96.146.2

6) No, the IP protocol number would be 0x11 instead of 01.

7) Contains all the same fields as the first part of the lab.

8) It has a type, code and checksum for the error message. Also the header file and its fields that normally are with it.

9) The last there packets made it to the destination and thus didn’t get the error message for the TTL expired.

10) The delay between 9 and 10 is much greater than any other two. Based off the names, I can see that one of the ends is New York City (NYC) and the other end is Pastourelle.