Zachary Kaplan
CS356
ICMP Lab
4/13/17

Command Line:

```
PING www.ust.hk (143.89.14.2) 56(84) bytes of data.
64 bytes from www.ust.hk (143.89.14.2): icmp_seq=1 ttl=51 time=313 ms
64 bytes from www.ust.hk (143.89.14.2): icmp_seq=2 ttl=51 time=354 ms
64 bytes from www.ust.hk (143.89.14.2): icmp_seq=3 ttl=51 time=297 ms
64 bytes from www.ust.hk (143.89.14.2): icmp_seq=4 ttl=51 time=446 ms
64 bytes from www.ust.hk (143.89.14.2): icmp_seq=5 ttl=51 time=281 ms
64 bytes from www.ust.hk (143.89.14.2): icmp_seq=6 ttl=51 time=325 ms
64 bytes from www.ust.hk (143.89.14.2): icmp_seq=7 ttl=51 time=265 ms
64 bytes from www.ust.hk (143.89.14.2): icmp_seq=8 ttl=51 time=309 ms
64 bytes from www.ust.hk (143.89.14.2): icmp_seq=9 ttl=51 time=353 ms
64 bytes from www.ust.hk (143.89.14.2): icmp_seq=10 ttl=51 time=293 ms

--- www.ust.hk ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9002ms
rtt min/avg/max/mdev = 265.117/324.010/446.189/48.945 ms
```

Questions:

```
Frame 51: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on
interface 0
Ethernet II, Src: HonHaiPr_59:00:19 (34:68:95:59:00:19), Dst:
Cisco_77:e4:00 (00:25:46:77:e4:00)
Internet Protocol Version 4, Src: 10.200.206.179, Dst: 143.89.14.2
Internet Control Message Protocol
      Type: 8 (Echo (ping) request)
      Code: 0
      Checksum: 0x8ca9 [correct]
      [Checksum Status: Good]
      Identifier (BE): 4395 (0x112b)
      Identifier (LE): 11025 (0x2b11)
      Sequence number (BE): 1 (0x0001)
      Sequence number (LE): 256 (0x0100)
      [Response frame: 52]
      Timestamp from icmp data: Apr 13, 2017 15:33:15.000000000 EDT
      [Timestamp from icmp data (relative): 0.863284430 seconds]
      Data (48 bytes)
```

1. The IP address of my computer is 10.200.206.179, while the destination IP address is 143.89.14.2.
2. ICMP is a network layer protocol, and therefore does not need port numbers because the packets are never handed up to the application level. However, the type and code

fields within the protocol are used at the network level to uniquely identify the message type / how the message should be handled.

3. The ICMP type and code are 8 and 0 respectively. The other fields are listed above. The checksum is 2 bytes, the sequence numbers are each 2 bytes, and the identifiers are each 2 bytes.

```
Frame 52: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on
interface 0
Ethernet II, Src: Cisco_77:e4:00 (00:25:46:77:e4:00), Dst:
HonHaiPr_59:00:19 (34:68:95:59:00:19)
Internet Protocol Version 4, Src: 143.89.14.2, Dst: 10.200.206.179
Internet Control Message Protocol
      Type: 0 (Echo (ping) reply)
      Code: 0
      Checksum: 0x94a9 [correct]
      [Checksum Status: Good]
      Identifier (BE): 4395 (0x112b)
      Identifier (LE): 11025 (0x2b11)
      Sequence number (BE): 1 (0x0001)
      Sequence number (LE): 256 (0x0100)
      [Request frame: 51]
      [Response time: 313.156 ms]
      Timestamp from icmp data: Apr 13, 2017 15:33:15.000000000 EDT
      [Timestamp from icmp data (relative): 1.176440647 seconds]
      Data (48 bytes)
```

4. The ICMP type and code are 0 and 0 respectively. The other fields are listed above. The checksum is 2 bytes, the sequence numbers are each 2 bytes, and the identifiers are each 2 bytes.

Using Downloaded Traces for the Following (Can't Replicate on Linux):

```
Frame 1: 106 bytes on wire (848 bits), 106 bytes captured (848 bits)
Ethernet II, Src: Dell_4f:36:23 (00:08:74:4f:36:23), Dst:
LinksysG_da:af:73 (00:06:25:da:af:73)
Internet Protocol Version 4, Src: 192.168.1.101, Dst: 138.96.146.2
Internet Control Message Protocol
      Type: 8 (Echo (ping) request)
      Code: 0
      Checksum: 0x51fe [correct]
      [Checksum Status: Good]
      Identifier (BE): 512 (0x0200)
```

```
        Identifier (LE): 2 (0x0002)
        Sequence number (BE): 41985 (0xa401)
        Sequence number (LE): 420 (0x01a4)
        [No response seen]
        Data (64 bytes)
```

5. The IP address of the host is 192.168.1.101, and the IP address of the target is 138.96.146.2.
6. No, the protocol number would instead be 17, for UDP.
7. These ping packets appear to be structured identically to the ping packets from the prior section of the lab, so no they are not different.

```
Frame 2: 70 bytes on wire (560 bits), 70 bytes captured (560 bits)
Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst:
Dell_4f:36:23 (00:08:74:4f:36:23)
Internet Protocol Version 4, Src: 10.216.228.1, Dst: 192.168.1.101
Internet Control Message Protocol
      Type: 11 (Time-to-live exceeded)
      Code: 0 (Time to live exceeded in transit)
      Checksum: 0x2c16 [correct]
      [Checksum Status: Good]
      Internet Protocol Version 4, Src: 192.168.1.101, Dst:
138.96.146.2
      Internet Control Message Protocol
      Type: 8 (Echo (ping) request)
      Code: 0
      Checksum: 0x51fe [unverified] [in ICMP error packet]
      [Checksum Status: Unverified]
      Identifier (BE): 512 (0x0200)
      Identifier (LE): 2 (0x0002)
      Sequence number (BE): 41985 (0xa401)
      Sequence number (LE): 420 (0x01a4)
```

8. The error packet has only the type, code, and checksum fields as compared to the ping packet. However, it also includes a copy of the IP frame that contains the ICMP ping packet that caused the error.
9. The last three packets all made it to the host they were trying to get to. The TTL was large enough to finally reach the destination, and therefore these packets aren't errors and instead are valid requests that are then responded to.

Zachary Kaplan
CS356
ICMP Lab
4/13/17

10. The largest difference in delay occurs between ping 9 and ping 10. Judging by these router's names, this link is between a router in New York City and Pastourelle in France.