Vanessa Ulloa

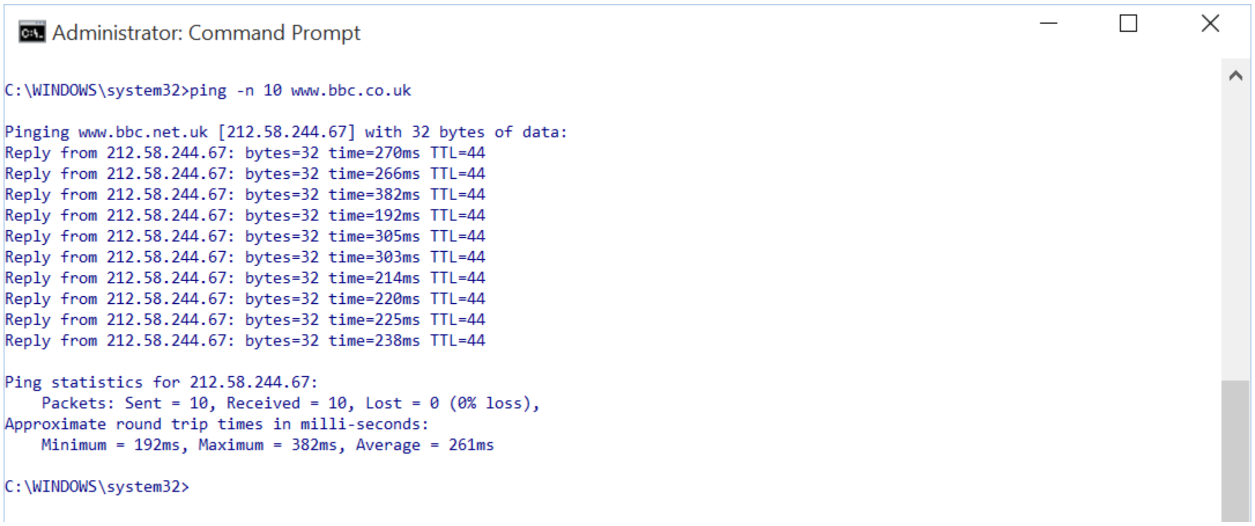
Daniel Kushner

CST 311

16 Jun 2015

Lab 7

ICMP and Ping



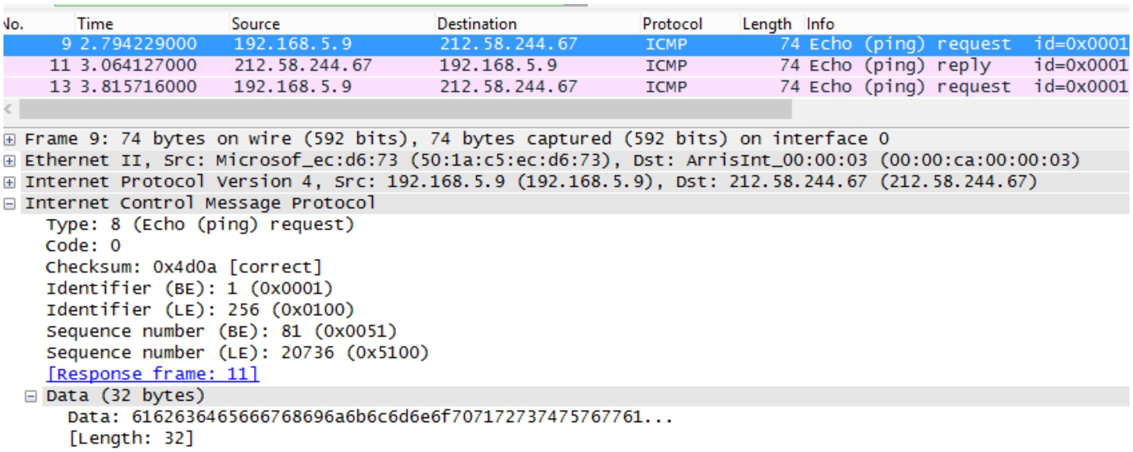
```
C:\WINDOWS\system32>ping -n 10 www.bbc.co.uk

Pinging www.bbc.net.uk [212.58.244.67] with 32 bytes of data:
Reply from 212.58.244.67: bytes=32 time=270ms TTL=44
Reply from 212.58.244.67: bytes=32 time=266ms TTL=44
Reply from 212.58.244.67: bytes=32 time=382ms TTL=44
Reply from 212.58.244.67: bytes=32 time=192ms TTL=44
Reply from 212.58.244.67: bytes=32 time=305ms TTL=44
Reply from 212.58.244.67: bytes=32 time=303ms TTL=44
Reply from 212.58.244.67: bytes=32 time=214ms TTL=44
Reply from 212.58.244.67: bytes=32 time=220ms TTL=44
Reply from 212.58.244.67: bytes=32 time=225ms TTL=44
Reply from 212.58.244.67: bytes=32 time=238ms TTL=44

Ping statistics for 212.58.244.67:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 192ms, Maximum = 382ms, Average = 261ms

C:\WINDOWS\system32>
```

1. What is the IP address of your host? What is the IP address of the destination host?
    a. IP address of my host: 192.168.5.9
    b. IP address of destination host: 212.58.244.67
2. Why is it that an ICMP packet does not have source and destination port numbers?
    a. The ICMP packet operations on the network layer instead of the application layer. Only application layer messages have a source and destination port numbers.
3. Examine one of the ping request packets sent by your host. What are the ICMP type and code numbers? What other fields does this ICMP packet have? How many bytes are the checksum, sequence number and identifier fields?



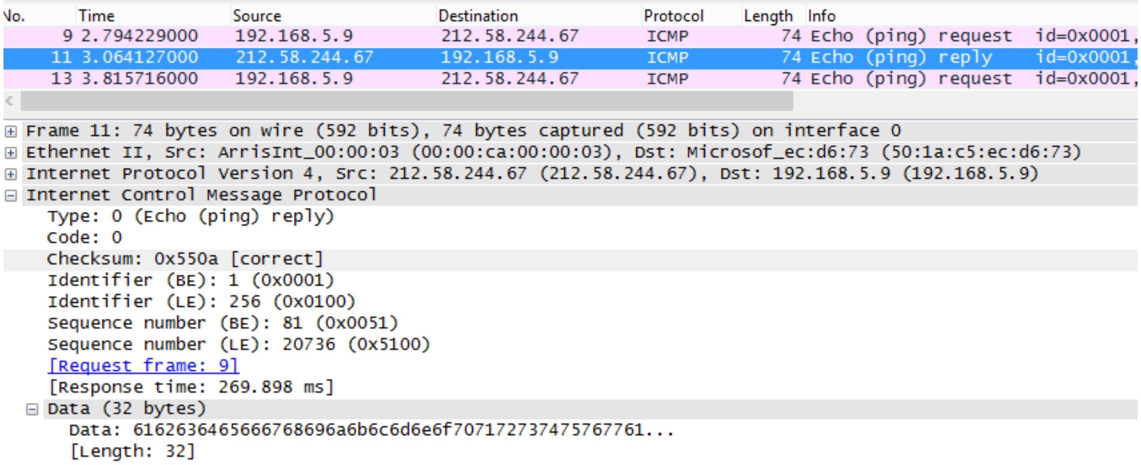
```
No.   Time            Source          Destination      Protocol   Length  Info
    9 2.794229000     192.168.5.9     212.58.244.67    ICMP           74  Echo (ping) request   id=0x0001
   11 3.064127000     212.58.244.67   192.168.5.9      ICMP           74  Echo (ping) reply     id=0x0001
   13 3.815716000     192.168.5.9     212.58.244.67    ICMP           74  Echo (ping) request   id=0x0001

⊞ Frame 9: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
⊞ Ethernet II, Src: Microsof_ec:d6:73 (50:1a:c5:ec:d6:73), Dst: ArrisInt_00:00:03 (00:00:ca:00:00:03)
⊞ Internet Protocol Version 4, Src: 192.168.5.9 (192.168.5.9), Dst: 212.58.244.67 (212.58.244.67)
⊟ Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x4d0a [correct]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence number (BE): 81 (0x0051)
    Sequence number (LE): 20736 (0x5100)
    [Response frame: 11]
  ⊟ Data (32 bytes)
      Data: 6162636465666768696a6b6c6d6e6f7071727374757677 61...
      [Length: 32]
```

a. Type: 8, code 0

b. 2 bytes each

4. Examine the corresponding pint reply packet. What are the ICMP type and code numbers? What other fields does this ICMP packet have? How many bytes are the checksum, sequence number and identifier fields?



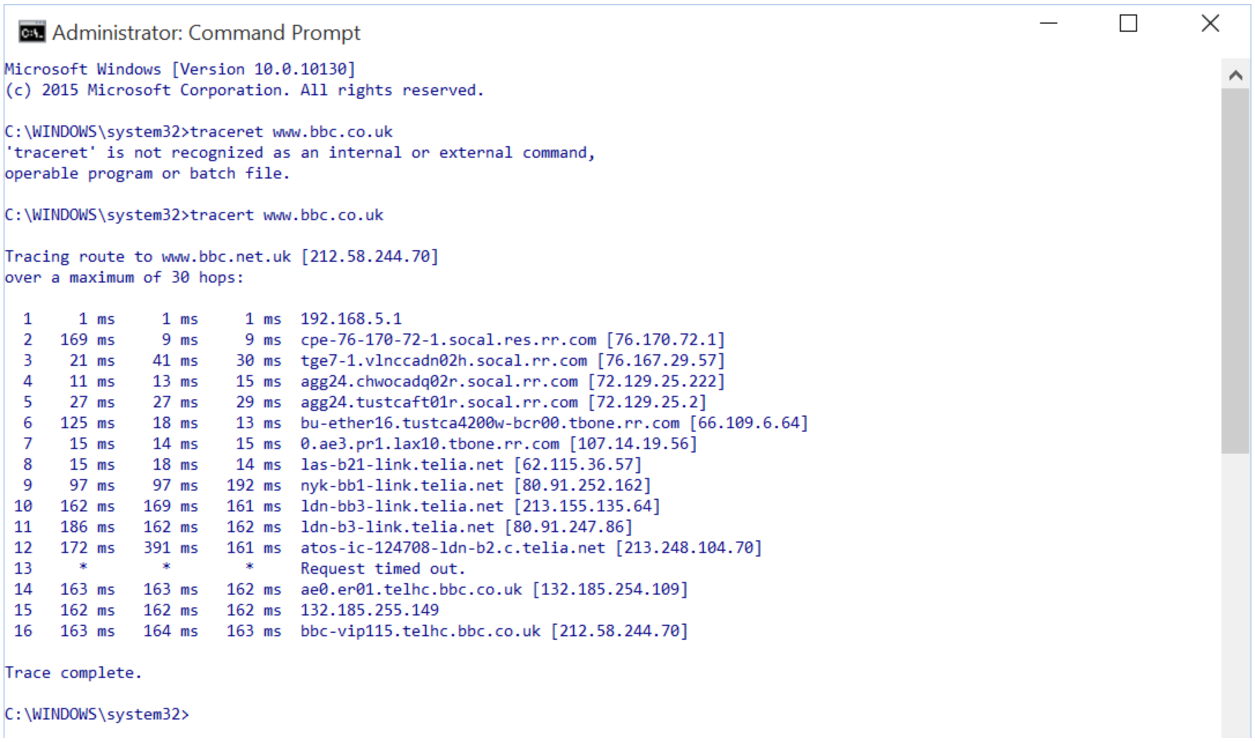
```
No.   Time            Source          Destination      Protocol   Length  Info
    9 2.794229000     192.168.5.9     212.58.244.67    ICMP           74  Echo (ping) request   id=0x0001,
   11 3.064127000     212.58.244.67   192.168.5.9      ICMP           74  Echo (ping) reply     id=0x0001,
   13 3.815716000     192.168.5.9     212.58.244.67    ICMP           74  Echo (ping) request   id=0x0001,

⊞ Frame 11: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
⊞ Ethernet II, Src: ArrisInt_00:00:03 (00:00:ca:00:00:03), Dst: Microsof_ec:d6:73 (50:1a:c5:ec:d6:73)
⊞ Internet Protocol Version 4, Src: 212.58.244.67 (212.58.244.67), Dst: 192.168.5.9 (192.168.5.9)
⊟ Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0x550a [correct]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence number (BE): 81 (0x0051)
    Sequence number (LE): 20736 (0x5100)
    [Request frame: 9]
    [Response time: 269.898 ms]
  ⊟ Data (32 bytes)
      Data: 6162636465666768696a6b6c6d6e6f7071727374757677 61...
      [Length: 32]
```

a. Type: 0, code: 0

b. Checksum, identifier, sequence number at 2 bytes each

ICMP and Traceroute



```
Microsoft Windows [Version 10.0.10130]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>traceret www.bbc.co.uk
'traceret' is not recognized as an internal or external command,
operable program or batch file.

C:\WINDOWS\system32>tracert www.bbc.co.uk

Tracing route to www.bbc.net.uk [212.58.244.70]
over a maximum of 30 hops:

  1     1 ms     1 ms     1 ms  192.168.5.1
  2   169 ms     9 ms     9 ms  cpe-76-170-72-1.socal.res.rr.com [76.170.72.1]
  3    21 ms    41 ms    30 ms  tge7-1.vlnccadn02h.socal.rr.com [76.167.29.57]
  4    11 ms    13 ms    15 ms  agg24.chwocadq02r.socal.rr.com [72.129.25.222]
  5    27 ms    27 ms    29 ms  agg24.tustcaft01r.socal.rr.com [72.129.25.2]
  6   125 ms    18 ms    13 ms  bu-ether16.tustca4200w-bcr00.tbone.rr.com [66.109.6.64]
  7    15 ms    14 ms    15 ms  0.ae3.pr1.lax10.tbone.rr.com [107.14.19.56]
  8    15 ms    18 ms    14 ms  las-b21-link.telia.net [62.115.36.57]
  9    97 ms    97 ms   192 ms  nyk-bb1-link.telia.net [80.91.252.162]
 10   162 ms   169 ms   161 ms  ldn-bb3-link.telia.net [213.155.135.64]
 11   186 ms   162 ms   162 ms  ldn-b3-link.telia.net [80.91.247.86]
 12   172 ms   391 ms   161 ms  atos-ic-124708-ldn-b2.c.telia.net [213.248.104.70]
 13     *        *        *     Request timed out.
 14   163 ms   163 ms   162 ms  ae0.er01.telhc.bbc.co.uk [132.185.254.109]
 15   162 ms   162 ms   162 ms  132.185.255.149
 16   163 ms   164 ms   163 ms  bbc-vip115.telhc.bbc.co.uk [212.58.244.70]

Trace complete.

C:\WINDOWS\system32>
```

5. What is the IP address of your host? What is the IP address of the target destination host?
   a. Host: 192.168.5.9
   b. Destination Host: 212.58.244.70
6. If ICMP sent UDP packets instead (as in Unix/Linux), would the IP protocol number still be 01 for the probe packets? If not, what would it be?
   a. No, 0x11
7. Examine the ICMP echo packet in your screenshot. Is this different from the ICMP ping query packets in the first half of this lab? If yes, how so?
   a. No, same fields
8. Examine the ICMP error packet in your screenshot. It has more fields than the ICMP echo packet. What is included in those fields?
   a. Not the same.
   b. Contains: IP header, first 8 bytes of the packet the error is for
9. Examine the last three ICMP packets received by the source host. How are these packets different from the ICMP error packets? Why are they different?
   a. The type is 0 and there is no Time to live exceeded message
10. Within the tracert measurements, is there a link whose delay is significantly longer than others? Refer to the screenshot in Figure 4, is there a link whose delay is significantly longer than others? On the basis of the router names, can you guess the location of the two routers on the end of this link?
    a. Between link 12 and 13 where the request timed out (so 12 to 14). Link from Telia (Sweden) to UK