Wireshark Lab: IP

Trevor Bramwell
CS372 - Introduction to Computer Networks
Professor Bechir Hamdaoui

May 24, 2012

2 A look at the capture trace

1. **Question** Select the first ICMP Echo Request message sent by your computer, and expand the Internet Protocol part of the packet in the packet details window. What is the IP address of your computer?

   Answer 192.168.1.100

```
No.     Time        Source                Destination           Protocol
    Length Info
     13 0.214898    192.168.1.1           192.168.1.100         ICMP      98
        Time-to-live exceeded (Time to live exceeded in transit)

Frame 13: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
Ethernet II, Src: Cisco-Li_66:aa:5d (00:25:9c:66:aa:5d), Dst: Azurewav_66:dd:8
    f (00:25:d3:66:dd:8f)
Internet Protocol Version 4, Src: 192.168.1.1 (192.168.1.1), Dst: 192.168.1.100
    (192.168.1.100)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-
       ECT (Not ECN-Capable Transport))
    Total Length: 84
    Identification: 0x0169 (361)
    Flags: 0x00
    Fragment offset: 0
    Time to live: 64
    Protocol: ICMP (1)
    Header checksum: 0xf58a [correct]
    Source: 192.168.1.1 (192.168.1.1)
    Destination: 192.168.1.100 (192.168.1.100)
Internet Control Message Protocol
```

2. **Question** Within the IP packet header, what is the value in the upper layer protocol field?

   Answer ICMP (1)

3. **Question** How many bytes are in the IP header? How many bytes are in the payload *of the IP datagram*? Explain how you determined the number of payload bytes.

   Answer The IP header contains 20 bytes, the payload of the IP datagram contains 64 bytes. The payload bytes can be determined by selecting the payload header (Internet Control Message Protocol) and counting the number of bytes that are selected in the raw packet window.

4. **Question** Has this IP datagram been fragmented? Explain how you determined whether or not the datagram has been fragmented.

   Answer No. The fragment offset is set to 0.

5. **Question** Which fields in the IP datagram *always* change from one datagram to the next within this series of ICMP messages sent by your computer?

   Answer Identification, Header Checksum, Time to Live, Source and Destination Port.

6. **Question** Which fields stay constant? Which of the fields *must* stay constant? Which fields must change? Why?

   Answer Source and Destination stay constant. These much stay constant while Time to Live changes because we are only interested in the route between our host and gaia.cs.umass.edu.

7. **Question** Describe the pattern you see in the values in the Identification field of the IP datagram

   Answer It increases by 1 every time.

8. **Question** What is the value in the Identification field and the TTL field?

   Answer Identification: 0x0169 (361) and TTL: 64

```
No.     Time        Source                Destination           Protocol
    Length Info
     13 0.214898    192.168.1.1           192.168.1.100         ICMP     98
            Time-to-live exceeded (Time to live exceeded in transit)

Frame 13: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
Ethernet II, Src: Cisco-Li_66:aa:5d (00:25:9c:66:aa:5d), Dst: Azurewav_66:dd:8
    f (00:25:d3:66:dd:8f)
Internet Protocol Version 4, Src: 192.168.1.1 (192.168.1.1), Dst:
    192.168.1.100 (192.168.1.100)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-
       ECT (Not ECN-Capable Transport))
    Total Length: 84
    Identification: 0x0169 (361)
    Flags: 0x00
    Fragment offset: 0
    Time to live: 64
    Protocol: ICMP (1)
    Header checksum: 0xf58a [correct]
    Source: 192.168.1.1 (192.168.1.1)
    Destination: 192.168.1.100 (192.168.1.100)
Internet Control Message Protocol
```

9. **Question** Do these values remain unchanged for all of the ICMP TTL-exceeded replies sent to your computer by the nearest (first hop) router? Why?

   Answer The TTL does not change from 64, but each Identification number does.

Fragmentation

10. **Question** Find the first ICMP Echo Request message that was sent by your computer after you changed the *Packet Size* in *pingplotter* to be 2000. Has that message been fragmented across more than one IP datagram?

    Answer Yes it has as indicated by the [2 IPv4 Fragments ...] item.

```
No.     Time        Source                Destination           Protocol
   Length Info
    756 1.987063    140.211.167.30        128.119.245.12        UDP      534
          Source port: 50205  Destination port: traceroute

Frame 756: 534 bytes on wire (4272 bits), 534 bytes captured (4272 bits)
Ethernet II, Src: Dell_b0:2f:34 (00:25:64:b0:2f:34), Dst: Cisco_ae:b0:50 (58:
   bc:27:ae:b0:50)
Internet Protocol Version 4, Src: 140.211.167.30 (140.211.167.30), Dst:
   128.119.245.12 (128.119.245.12)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-
       ECT (Not ECN-Capable Transport))
    Total Length: 520
    Identification: 0xf3e8 (62440)
    Flags: 0x00
    Fragment offset: 1480
    Time to live: 1
    Protocol: UDP (17)
    Header checksum: 0x19ce [correct]
    Source: 140.211.167.30 (140.211.167.30)
    Destination: 128.119.245.12 (128.119.245.12)
    [2 IPv4 Fragments (1980 bytes): 755(1480), 756(500)]
        [Frame: 755, payload: 0-1479 (1480 bytes)]
        [Frame: 756, payload: 1480-1979 (500 bytes)]
        [Fragment count: 2]
        [Reassembled IPv4 length: 1980]
User Datagram Protocol, Src Port: 50205 (50205), Dst Port: traceroute (33434)
Data (1972 bytes)
```

11. **Question** Print out the first fragment of the fragmented IP datagram. What information in the IP header indicates that the datagram been fragmented? What information in the IP header indicates whether this is the first fragment versus a latter fragment? How long is this IP datagram?

    Answer The flags have been set to 0x01 (More Fragments). This is the first fragment because the fragment offset is set to 0. This IP datagram is 1480 bytes

```
No.     Time        Source                Destination           Protocol
    Length Info
    755 1.987056    140.211.167.30        128.119.245.12        IPv4      1514
         Fragmented IP protocol (proto=UDP 0x11, off=0, ID=f3e8) [Reassembled
        in #756]

Frame 755: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)
Ethernet II, Src: Dell_b0:2f:34 (00:25:64:b0:2f:34), Dst: Cisco_ae:b0:50 (58:
    bc:27:ae:b0:50)
Internet Protocol Version 4, Src: 140.211.167.30 (140.211.167.30), Dst:
    128.119.245.12 (128.119.245.12)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-
        ECT (Not ECN-Capable Transport))
    Total Length: 1500
    Identification: 0xf3e8 (62440)
    Flags: 0x01 (More Fragments)
    Fragment offset: 0
    Time to live: 1
    Protocol: UDP (17)
    Header checksum: 0xf6b2 [correct]
    Source: 140.211.167.30 (140.211.167.30)
    Destination: 128.119.245.12 (128.119.245.12)
    Reassembled IPv4 in frame: 756
Data (1480 bytes)
```

12. **Question** Print out the second fragment of the fragmented IP datagram. What information in the IP header indicates that this is not the first datagram fragment? Are the more fragments? How can you tell?

    Answer This is not the first datagram fragment because the fragment offset is set to 1480. There are no more fragments because the flags are set to 0x00. If there were more fragments the flags would be set to 0x01 as in the first fragment.

```
No.     Time        Source                Destination           Protocol
   Length Info
    756 1.987063    140.211.167.30        128.119.245.12        UDP      534
          Source port: 50205  Destination port: traceroute

Frame 756: 534 bytes on wire (4272 bits), 534 bytes captured (4272 bits)
Ethernet II, Src: Dell_b0:2f:34 (00:25:64:b0:2f:34), Dst: Cisco_ae:b0:50 (58:
   bc:27:ae:b0:50)
Internet Protocol Version 4, Src: 140.211.167.30 (140.211.167.30), Dst:
   128.119.245.12 (128.119.245.12)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-
       ECT (Not ECN-Capable Transport))
    Total Length: 520
    Identification: 0xf3e8 (62440)
    Flags: 0x00
    Fragment offset: 1480
    Time to live: 1
    Protocol: UDP (17)
    Header checksum: 0x19ce [correct]
    Source: 140.211.167.30 (140.211.167.30)
    Destination: 128.119.245.12 (128.119.245.12)
    [2 IPv4 Fragments (1980 bytes): #755(1480), #756(500)]
        [Frame: 755, payload: 0-1479 (1480 bytes)]
        [Frame: 756, payload: 1480-1979 (500 bytes)]
        [Fragment count: 2]
        [Reassembled IPv4 length: 1980]
User Datagram Protocol, Src Port: 50205 (50205), Dst Port: traceroute (33434)
Data (1972 bytes)
```

13. **Question** What fields change in the IP header between the first and second fragment?

    Answer Total Length, Flags, Identification, and Header Checksum.

14. **Question** How many fragments were created from the original datagram?

    Answer 3

```
No.     Time        Source                Destination           Protocol
   Length Info
    814 2.397458    140.211.167.30        128.119.245.12        IPv4      1514
         Fragmented IP protocol (proto=UDP 0x11, off=0, ID=f41f) [Reassembled
        in #816]

Frame 814: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)
Ethernet II, Src: Dell_b0:2f:34 (00:25:64:b0:2f:34), Dst: Cisco_ae:b0:50 (58:
   bc:27:ae:b0:50)
Internet Protocol Version 4, Src: 140.211.167.30 (140.211.167.30), Dst:
   128.119.245.12 (128.119.245.12)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-
       ECT (Not ECN-Capable Transport))
    Total Length: 1500
    Identification: 0xf41f (62495)
    Flags: 0x01 (More Fragments)
    Fragment offset: 0
    Time to live: 1
    Protocol: UDP (17)
    Header checksum: 0xf67b [correct]
    Source: 140.211.167.30 (140.211.167.30)
    Destination: 128.119.245.12 (128.119.245.12)
    Reassembled IPv4 in frame: 816
Data (1480 bytes)
```

```
No.     Time        Source                Destination           Protocol
   Length Info
    815 2.397466    140.211.167.30        128.119.245.12        IPv4      1514
         Fragmented IP protocol (proto=UDP 0x11, off=1480, ID=f41f) [
       Reassembled in #816]

Frame 815: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)
Ethernet II, Src: Dell_b0:2f:34 (00:25:64:b0:2f:34), Dst: Cisco_ae:b0:50 (58:
   bc:27:ae:b0:50)
Internet Protocol Version 4, Src: 140.211.167.30 (140.211.167.30), Dst:
   128.119.245.12 (128.119.245.12)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-
       ECT (Not ECN-Capable Transport))
    Total Length: 1500
    Identification: 0xf41f (62495)
    Flags: 0x01 (More Fragments)
    Fragment offset: 1480
```

```
    Time to live: 1
    Protocol: UDP (17)
    Header checksum: 0xf5c2 [correct]
    Source: 140.211.167.30 (140.211.167.30)
    Destination: 128.119.245.12 (128.119.245.12)
    Reassembled IPv4 in frame: 816
Data (1480 bytes)

No.     Time        Source                Destination           Protocol
   Length Info
    816 2.397469    140.211.167.30        128.119.245.12        UDP      554
          Source port: 52724  Destination port: traceroute

Frame 816: 554 bytes on wire (4432 bits), 554 bytes captured (4432 bits)
Ethernet II, Src: Dell_b0:2f:34 (00:25:64:b0:2f:34), Dst: Cisco_ae:b0:50 (58:
   bc:27:ae:b0:50)
Internet Protocol Version 4, Src: 140.211.167.30 (140.211.167.30), Dst:
   128.119.245.12 (128.119.245.12)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-
       ECT (Not ECN-Capable Transport))
    Total Length: 540
    Identification: 0xf41f (62495)
    Flags: 0x00
    Fragment offset: 2960
    Time to live: 1
    Protocol: UDP (17)
    Header checksum: 0x18ca [correct]
    Source: 140.211.167.30 (140.211.167.30)
    Destination: 128.119.245.12 (128.119.245.12)
    [3 IPv4 Fragments (3480 bytes): #814(1480), #815(1480), #816(520)]
        [Frame: 814, payload: 0-1479 (1480 bytes)]
        [Frame: 815, payload: 1480-2959 (1480 bytes)]
        [Frame: 816, payload: 2960-3479 (520 bytes)]
        [Fragment count: 3]
        [Reassembled IPv4 length: 3480]
User Datagram Protocol, Src Port: 52724 (52724), Dst Port: traceroute (33434)
Data (3472 bytes)
```

15. **Question** What fields change in the IP header among the fragments?

    Answer Total Length, Flags, Identification, and Header Checksum.