CSCD58H3 Winter 2018

Tutorial: 005

Week: 6

Date: February 13th, 2018

Ethernet and IP Packet headers

This material covers general knowledge about Ethernet and IP packet headers.

- ## Ethernet Headers

```
▶ Frame 1: 135 bytes on wire (1080 bits), 135 bytes captured (1080 bits)
▼ Ethernet II, Src: Apple_23:3b:57 (f4:0f:24:23:3b:57), Dst: LannerEl_34:af:1d (00:90:0b:34:af:1d)
  ▼ Destination: LannerEl_34:af:1d (00:90:0b:34:af:1d)
      Address: LannerEl_34:af:1d (00:90:0b:34:af:1d)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  ▼ Source: Apple_23:3b:57 (f4:0f:24:23:3b:57)
      Address: Apple_23:3b:57 (f4:0f:24:23:3b:57)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
▶ Internet Protocol Version 4, Src: 138.51.63.115, Dst: 17.249.76.82
▶ Transmission Control Protocol, Src Port: 59031, Dst Port: 5223, Seq: 1, Ack: 1, Len: 69
▶ Data (69 bytes)
```

  - Destination Address

    MAC address of the target system. The `ff:ff:ff:ff:ff:ff` address signifies all hosts within the LAN. This address is commonly called the broadcast address

  - Source Address

    MAC address of the transmitting system.

  - Type

    The protocol being carried in the data section. TCP/IP, ARP etc

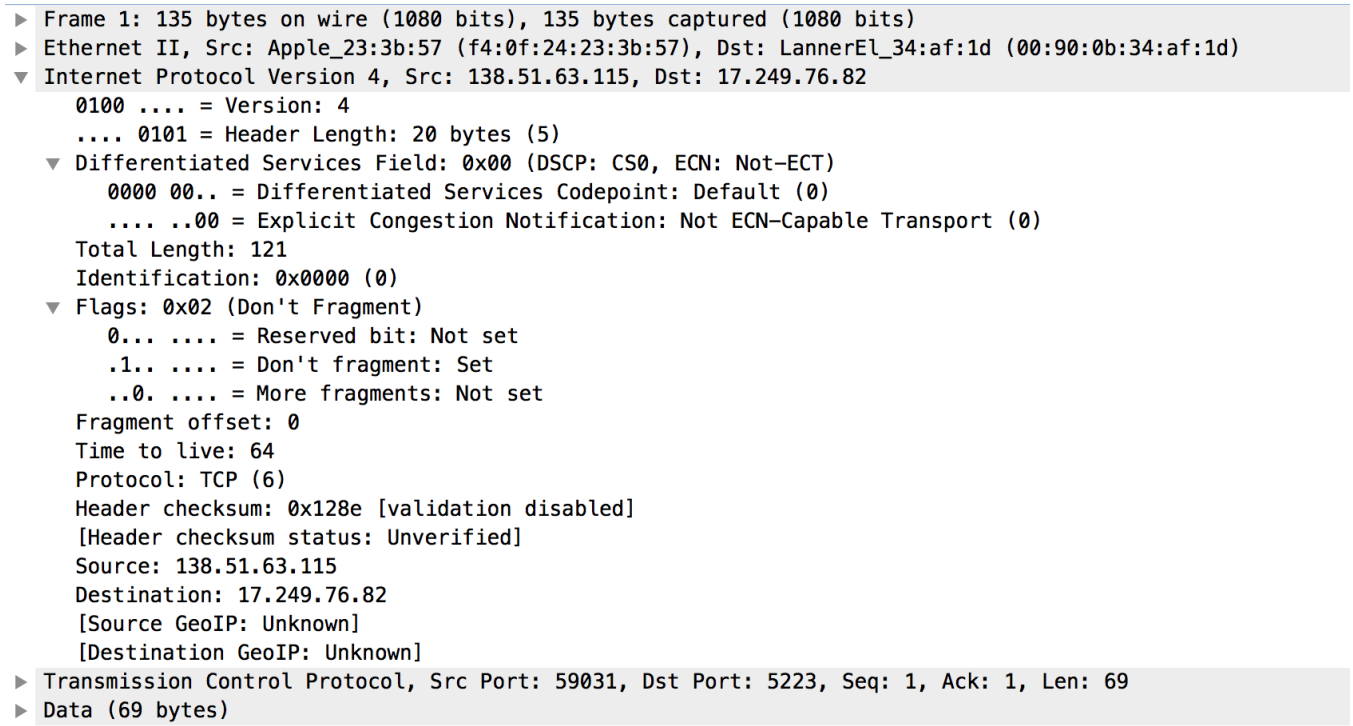
  - Data

    The data being transmitted. Maximum size is 1500 bytes and a minimum of 46 bytes.

  - Frame Check Sequence

    This is a 32 bit value computed using the Cyclic Redundancy Checksum Algorithm. Used to verify the integrity of the packet at its destination.

- ## IP Headers



- Version

  The IP protocol version. Could be IPv4 or IPv6. With regards to A2, focus on IPv4. Uses 4 bits.

- Header Length

  IP header length, this is the size of the header. The value is the size of the header in 32-bits words. This field uses 4-bits. This implies the max value is 15 (1111). The min value however is 5 (1010). Making 20bytes the smallest size of an IP Header and the largest is 60bytes.

- TOS

  Occupies 8 bits

  - DHCP

    Differentiated Services Code Point. Uses 6 bits. Indicates to the router how packets waiting to be forwarded should be queued. Might be set to 0.

  - ECN

    Explicit Congestion Notification, occupies 2 bits.

    - `00`: The packet does not use ECN
    - `01`: The packets is a part of an ECN capable transport flow
    - `10`: The packetart
    - `11`: The packet is experiencing congestion

- Total Length

  Total length of the packet; header and data. This field is 16 bits

- Identification

  Since packets may be de-fragmented, a unique identification is required to reassemble these packets. The uniqueness is achieved by combining the source

address with this value. This field requires 16 bits.

- Flags

  These flags are concerned with fragmentation of packets. There are 3 flags each using 1 bit. The first flag is unused and reserved. One flag indicates whether the router can fragment this packet and the other indicates whether this is a fragmented packet.

- Offset

  For a fragmented packet, this is the byte offset from the beginning of the first packet. This is set by the router performing the fragmentation. This field occupies 13 bits.

- Time To Live

  The maximum amount of hops the packet is allowed to be routed through. This field occupies 6 bits. If you recall, this is one of the fields used by `traceroute` to implement the hops count and listing.

- Protocol

  Indicates the type of transport in the data section of the IP packet. Defined in the Service Access Point (SAP). Examples: ICMP, TCP, UDP etc. This field requires 8 bits.

- Header checksum

  This field contains a checksum for the IP header (excluding the checksum itself (set to 0 before computation).) This field occupies 16 bits. It is necessary for detecting error introduced during transport. Routers drop packets whose checksums do not agree with the checksum computed by the router.

  Below is a simple trace. It is your task to get an idea of the algorithm from a trace.

  Let the bytes to be checksum-ed be the following: `DEADBEEFBEADF00DDEADC0DE`

  - Step 1. `DEAD` `BEEF` `BEAD` `F00D` `DEAD` `C0DE`
  - Step 2. `19D9C` = `DEAD` + `BEEF` (carry over, what to do?)
  - Step 3. `15C49` = (`9D9C` + `0001`) + `BEAD`
  - Step 4. `14C57` = (`5C49` + `0001`) + `F00D`
  - Step 5. `12B05` = (`4C57` + `0001`) + `DEAD`
  - Step 6. `EBE4` = (`2B05` + `0001`) + `C0DE`
  - Step 7. `141B` = `EBE4` ^ `FFFF`

  The value `141B` is the checksum for `DEADBEEFBEADF00DDEADC0DE` assuming these where the contents of an IP header excluding the checksum value. This value will always be 16 bits

- Source addr

  This is the IP address of the node the packet originally originated from. This field is 32 bits

- Destination addr

  This is the IP address of the final destination node of this packet. This field is 32 bits

- Options

  Mostly unused. The header length can be used to detect if this field is in use. If it is, the header length will be more than the minimum 20 bytes of header length

Useful Resources

0. Routers
1. Router Operation
2. IP packet Processing