**Practical-2**

**AIM:** Understand and identify header fields of layers of TCP/IP protocol stack.

Watch and refer following videos for a better understanding of the header fields of layers of TCP/IP:

1. **Ethernet frame ():** https://www.youtube.com/watch?v=SoTRqDLND6Y
2. **IPv4 header format ()**: https://www.youtube.com/watch?v=3Y70y6dM7Cs
3. **IPv4 Vs IPv6()**: https://www.youtube.com/watch?v=NkE9\_iRPi1I
4. **TCP and UDP ():** https://www.youtube.com/watch?v=r4HbLQuqvrM

Students need to fill the empty table and write answers to questions.

As per the discussion in classroom, any user starts internet access through browser or network applications. Following figure 2.1 explain scenario of receiving data at NIC Card. NIC card receives signals and it converts into sequence of 0’s and 1‘s. After receiving data it sends data for the further processing to TCP/IP protocol stack. In this exercise you need to identify boundaries of fields of headers, describe and understand flow of information in protocol stack.

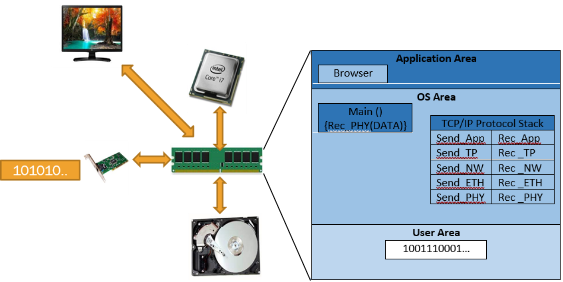


Figure 2.1 Real Scenario

**2.1 Input data stream: TCP**

This is the data stream which receiver NIC card receives from wire and stores into memory. Length of bits stream is 432 bits.

000000000001101010001100011010110111011010101100111010001101100011010001010001101111001111110001000010000000000001000101000000000000000000101000000101011011110101000000000000001000000000000110000000000000000010101100000100000000110001111011100011101111101010110111010011101100010101110011000000011011101101001001111011110111110100011010111100100000100000011010001001110101000000010000000100000000101011111110111011100000000000000000

Abstract view of data with respect to the location of headers and data in the actual data stream.

|  |  |  |  |
| --- | --- | --- | --- |
| Data Link (Ethernet) Header | Network Header | Transport Header | Data |

Initial 112 bits contains Ethernet Header (Refer section 2.2), Next 160 bits contains IP Header (Refer section 2.3), Next 160 bits contains TCP Header (Refer section 2.4).

**2.2 Header format of Ethernet**

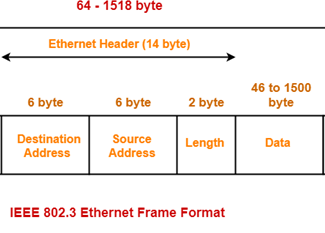
****

Figure 2.2 Ethernet Header Format

Section 2.1 contains bit stream. copy and paste respected number of bits into following table 2.1 to prepare ethernet header field boundary.

Table 2.1 Header format of ethernet

|  |  |  |
| --- | --- | --- |
| 000000000001101010001100011010110111011010101100 | 111010001101100011010001010001101111001111110001 | 0000100000000000 |

From table 2.1, fill table 2.2 with respected value and explanation meaning of each field. Refer the following link for better understanding. Refer video 1 in material 1 for further understanding.

Reference Link : <https://en.wikipedia.org/wiki/Ethernet_frame#Header>

<https://en.wikipedia.org/wiki/EtherType>

Table 2.2 Header fields of Ethernet

|  |  |  |  |
| --- | --- | --- | --- |
| **Header Field Name** | **Length of Field (in bits)** | **Header field Value (Hex Value)** | **Meaning** |
| Destination MAC Address | 48 bits | 00:1A:8C:6B:76:AC | Receiver’s MAC address |
| Source MAC Address | 48 bits | E8:D8:D1:46:F3F1 | Sender’s MAC address |
| Type | 16 bits | 0x800 | 0x800 indicates, Network Header type is IPv4 Header |

**2.3 Header format of Network**

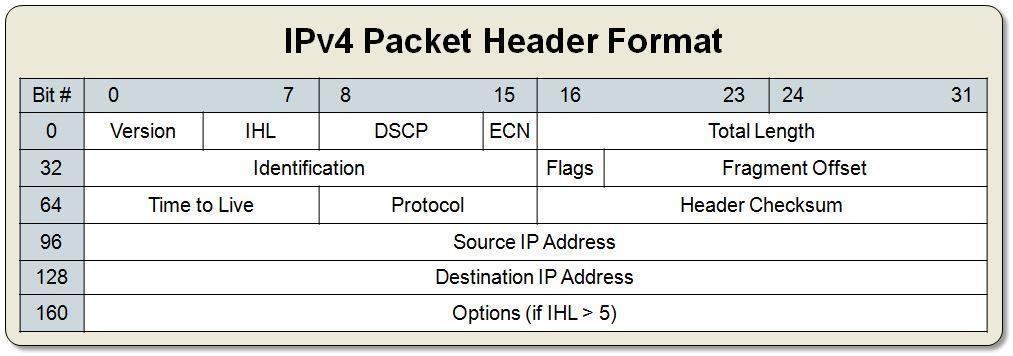


Figure 2.3 IPv4 header format

Section 2.1 contains bit stream. copy and paste respected number of bits into following table 2.3 to prepare ethernet header field boundary.

Table 2.3 Header format of network

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 0100 | 0101 | 000000 | 00 | 0000000000101000 | |
| 0001010110111101 | | | | 010 | 0000000000000 |
| 10000000 | | 00000110 | | 0000000000000000 | |
| 10101100000100000000110001111011 | | | | | |
| 10001110111110101011011101001110 | | | | | |

From table 2.3, fill table 2.4 with respected value and explanation meaning of each field. Refer the following link for better understanding. Refer video 2 in material 2 for further understanding.

Reference Links:

<https://en.wikipedia.org/wiki/IPv4#Header>

DCSP & ECN: <https://en.wikipedia.org/wiki/Type_of_service#DSCP_and_ECN>

Flags: <https://en.wikipedia.org/wiki/IPv4#Flags>

Protocol: <https://en.wikipedia.org/wiki/List_of_IP_protocol_numbers>

Table 2.4 Header fields of Network

|  |  |  |  |
| --- | --- | --- | --- |
| **Header Field Name** | **Length of Field (in bits)** | **Header field Value (Hex Value)** | **Meaning** |
| Version | 4 bits | 0x4 | IP Datagram version 4 |
| IHL | 4 bites | 0x5 | 5\*32bits=160bits=20bytes |
| DSCP | 6 bits | 0x0 | --- |
| ECN | 2 bits | 0x0 | --- |
| Total length | 16 bits | 0x28 | Total length of 40 bytes |
| Identification | 16 bits | 0x15BD |  |
| flags | 3 bits | 0x2 | 2 bit More Fragment (MF) |
| Fragment offset | 13 bits | 0x0 | This packet does not contain fragments. |
| Time to live | 8 bits | 0x80 | 128 Hops / Routers |
| Protocol | 8 bits | 0x06 | This packet should be give to TCP receive procedure. As its value indicates TCP. |
| Header checksum | 16 bits | 0x0 | No checksum included in this header. |
| Source IP Address | 32 bits | 172.16.12.123 | Source IP: 172.16.12.123, its local machine |
| Destination IP Address | 32 bits | 142.250.183.78 | Destination: 142.250.183.78, it is situated in \_\_\_\_ country |

**2.4 Header format of transport layer: TCP**

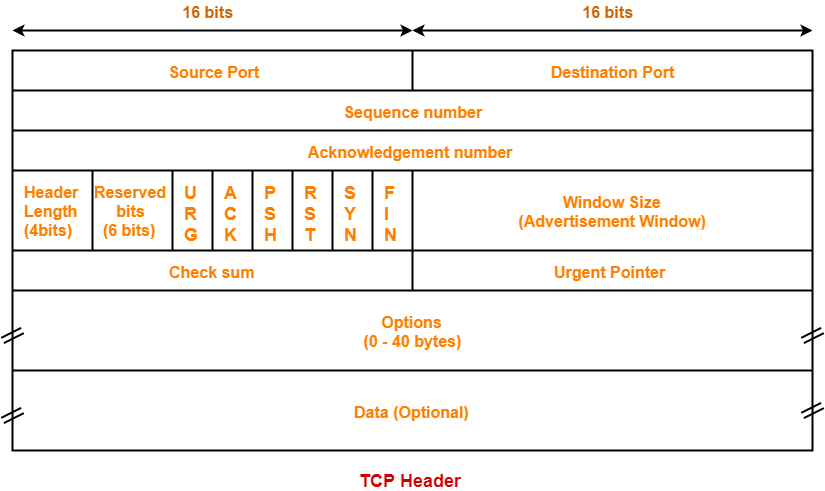


Figure 2.4 TCP Header format

Section 2.1 contains bit stream. copy and paste respected number of bits into following table 2.5 to prepare ethernet header field boundary.

Table 2.5 Header fields of transport layer

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1100010101110011 | | | | | | | | 0000000110111011 |
| 01001001111011110111110100011010 | | | | | | | | |
| 11110010000010000001101000100111 | | | | | | | | |
| 0101 | 000000 | 0 | 1 | 0 | 0 | 0 | 0 | 0001000000001010 |
| 1111111011101110 | | | | | | | | 0000000000000000 |

From table 2.5, fill table 2.6 with respected value and explanation meaning of each field. Refer the following link for better understanding. Refer video 4 in material 4 for further understanding.

Reference Link : <https://en.wikipedia.org/wiki/Transmission_Control_Protocol#TCP_segment_structure>

Flags: <https://www.gatevidyalay.com/transmission-control-protocol-tcp-header/>

Port : <https://www.adminsub.net/tcp-udp-port-finder/>

Table 2.6 Header fields of Transport Layer: \_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |  |  |  |
| --- | --- | --- | --- |
| **Header Field Name** | **Length of Field (in bits)** | **Header field Value (Hex Value)** | **Meaning** |
| Source Port | 16 Bits | 50547 | Sender machine’s application’s logical port number 50547. |
| Destination Port | 16 Bits | 443 | Receiver machine’s receiving logical port number 443 which indicates source wants communicate security using https protocol. |
| Sequence Number | 32 Bits | 0x49EF7D1A | Unique ID assigned by sender to maintain order of packers at receiver side. |
| Acknowledgement Number | 32 Bits | 0xF2081A27 | This is acknowledged of sent packet. |
| Header Length | 4 Bits | 0x5 | Total header Length is 5\*32bits=160bits=20bytes |
| Reserved Bits | 6 Bits | 0x0 | - |
| URG | 1 Bit | 0 |  |
| ACK | 1 Bit | 1 | This packet contains valid acknowledgement number. |
| PSH | 1 Bit | 0 | No Push |
| RST | 1 Bit | 0 | No RST |
| SYN | 1 Bit | 0 | No SYN |
| FIN | 1 Bit | 0 | NO Fin |
| Window Size | 16 Bits | 0x100A | 4106 |
| Checksum | 16 Bits | 0xFEEE | Error identification in packet. |
| Urgent Pointer | 16 Bits | 0x0 | No urgent content in this packet. |

**Exercise-1: Input Sequence TCP**

111010001101100011010001010001101111001111110001000000000001101010001100011010110111011010101100000010000000000001000101000000000000000000101000101111111101001001000000000000000100000000000110110011101101000001100111001110111000110001100110101011000001000000001100011110110000000110111011111100101100100000110001000100000000010111100000111001000000000001000010100110100101000000010000000000001111101110110000100111010000000000000000000000000000000000000000000000000000000000000000

**Header fields of Ethernet**

|  |  |  |  |
| --- | --- | --- | --- |
| **Header Field Name** | **Length of Field (in bits)** | **Header field Value (Hex Value)** | **Meaning** |
| Destination MAC Address | 48 bits | 00: E8:D8: D1:46:F3F1 | Receiver’s MAC address |
| Source MAC Address | 48 bits | 00:1A: 8C:6B:76:AC | Sender’s MAC address |
| Type | 16 bits | 0x800 | 0x800 indicates, Network Header type is IPv4 Header |

**Header fields of Network**

|  |  |  |  |
| --- | --- | --- | --- |
| **Header Field Name** | **Length of Field (in bits)** | **Header field Value (Hex Value)** | **Meaning** |
| Version | 4 bits | 0x4 | IP Datagram version 4 |
| IHL | 4 bits | 0x5 | 5\*32bits=160bits=20bytes |
| DSCP | 6 bits | 0x0 | --- |
| ECN | 2 bits | 0x0 | --- |
| Total length | 16 bits | 0x28 | Total length of 40 bytes |
| Identification | 16 bits | 0xBFD2 |  |
| flags | 3 bits | 0x2 | 2 bit More Fragment (MF) |
| Fragment offset | 13 bits | 0x0 | This packet does not contain fragments. |
| Time to live | 8 bits | 0x40 | 128 Hops / Routers |
| Protocol | 8 bits | 0x06 | This packet should be give to TCP receive procedure. As its value indicates TCP. |
| Header checksum | 16 bits | 0xCED0 | No checksum included in this header. |
| Source IP Address | 32 bits | 173.19.55.814 | Source IP: 173.19.55.814, its local machine |
| Destination IP Address | 32 bits | 288.673.292.3 | Destination: 288.673.292.3, it is situated in \_\_\_\_ country |

**Header fields of Transport Layer: \_\_\_\_\_\_\_**

|  |  |  |  |
| --- | --- | --- | --- |
| **Header Field Name** | **Length of Field (in bits)** | **Header field Value (Hex Value)** | **Meaning** |
| Source Port | 16 Bits | 443 | Sender machine’s application’s logical port number 443. |
| Destination Port | 16 Bits | 62152 | Receiver machine’s receiving logical port number 62152 which indicates source wants communicate security using https protocol. |
| Sequence Number | 32 Bits | 0x311005E0 | Unique ID assigned by sender to maintain order of packers at receiver side. |
| Acknowledgement Number | 32 Bits | 0x311005E0 | This is acknowledge of sent packet. |
| Header Length | 4 Bits | 0x5 | Total header Length is 5\*32bits=160bits=20bytes |
| Reserved Bits | 6 Bits | 0x0 | - |
| URG | 1 Bit | 0 |  |
| ACK | 1 Bit | 1 | This packet contains valid acknowledgement number. |
| PSH | 1 Bit | 0 | No Push |
| RST | 1 Bit | 0 | No RST |
| SYN | 1 Bit | 0 | No SYN |
| FIN | 1 Bit | 0 | NO Fin |
| Window Size | 16 Bits | 0xFB | 4106 |
| Checksum | 16 Bits | 0xB09D | Error identification in packet. |
| Urgent Pointer | 16 Bits | 0x0 | No urgent content in this packet. |

**Exercise-2: Input Sequence of UDP**

1110100011011000110100010100011011110011111100010000000001010000010101101010101111110010011001110000100000000000010001010000000000000000001010000010000101011001010000000000000010000000000100011010100110001001101011000001000000001011010001111010110000010000000011000111101100000001101110110000000001010000000000000001010010111000011000010000000000000000000000010000000000000000010000111111011001000000000000000000000000000000000000000000000000

**Header fields of Ethernet**

|  |  |  |  |
| --- | --- | --- | --- |
| **Header Field Name** | **Length of Field (in bits)** | **Header field Value (Hex Value)** | **Meaning** |
| Destination MAC Address | 48 bits | 00:E8:D8:D1:46:F3F1 | Receiver’s MAC address |
| Source MAC Address | 48 bits | 00:50:56:AB:F267 | Sender’s MAC address |
| Type | 16 bits | 0x800 | 0x800 indicates, Network Header type is IPv4 Header |

**Header fields of Network**

|  |  |  |  |
| --- | --- | --- | --- |
| **Header Field Name** | **Length of Field (in bits)** | **Header field Value (Hex Value)** | **Meaning** |
| Version | 4 bits | 0x4 | IP Datagram version 4 |
| IHL | 4 bits | 0xA | A\*32bits=320bits=40bytes |
| DSCP | 6 bits | 0x0 | --- |
| ECN | 2 bits | 0x0 | --- |
| Total length | 16 bits | 0x28 | Total length of 40 bytes |
| Identification | 16 bits | 0x2159 |  |
| flags | 3 bits | 0x2 | 2 bit More Fragment (MF) |
| Fragment offset | 13 bits | 0x0 | This packet does not contain fragments. |
| Time to live | 8 bits | 0x80 | 256 Hops / Routers |
| Protocol | 8 bits | 0x11 | This packet should be give to TCP receive procedure. As its value indicates TCP. |
| Header checksum | 16 bits | 0xA989 | No checksum included in this header. |
| Source IP Address | 32 bits | 288.673.261.5 | Source IP: 288.673.261.5 its local machine |
| Destination IP Address | 32 bits | 288.673.292.3 | Destination: 288.673.292.3, it is situated in \_\_\_\_ country |

**Header fields of Transport Layer: \_\_\_\_\_\_\_**

|  |  |  |  |
| --- | --- | --- | --- |
| **Header Field Name** | **Length of Field (in bits)** | **Header field Value (Hex Value)** | **Meaning** |
| Source Port | 16 Bits | 443 | Sender machine’s application’s logical port number 443. |
| Destination Port | 16 Bits | 50 | Receiver machine’s receiving logical port number 50 which indicates source wants communicate security using https protocol. |
| Sequence Number | 32 Bits | 0x1357921 | Unique ID assigned by sender to maintain order of packers at receiver side. |
| Acknowledgement Number | 32 Bits | 0x256 | This is acknowledged of sent packet. |
| Header Length | 4 Bits | 0x0 | Total header Length is 0 bytes |
| Reserved Bits | 6 Bits | 0x1 | 1 bit |
| URG | 1 Bit | 0 |  |
| ACK | 1 Bit | 0 | This packet doesn’t contains valid acknowledgement number. |
| PSH | 1 Bit | 0 | No Push |
| RST | 1 Bit | 0 | No RST |
| SYN | 1 Bit | 1 | SYN |
| FIN | 1 Bit | 1 | Fin |
| Window Size | 16 Bits | 0xF640 | 4106 |
| Checksum | 16 Bits | 0x0 | No Error identification in packet. |
| Urgent Pointer | 16 Bits | 0x0 | No urgent content in this packet. |

**Exercise-3: Input Sequence: ARP Broadcast**

111111111111111111111111111111111111111111111111111000000110001111011010010101000111000101000100000010000000011000000000000000010000100000000000000001100000010000000000000000011110000001100011110110100101010001110001010001001010110000010000000010000010000100000000000000000000000000000000000000000000000010101100000100000000011110011101000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000

**Header fields of Ethernet**

|  |  |  |  |
| --- | --- | --- | --- |
| **Header Field Name** | **Length of Field (in bits)** | **Header field Value (Hex Value)** | **Meaning** |
| Destination MAC Address | 48 bits | 00:FF:FF:FF:FF:FFFF | Receiver’s MAC address |
| Source MAC Address | 48 bits | 00:E0:63:DA:54:7144 | Sender’s MAC address |
| Type | 16 bits | 0x806 | 0x806 indicates, Network Header type is IPv4 Header |

**Header fields of Network**

|  |  |  |  |
| --- | --- | --- | --- |
| **Header Field Name** | **Length of Field (in bits)** | **Header field Value (Hex Value)** | **Meaning** |
| Version | 4 bits | 0x4 | IP Datagram version 4 |
| IHL | 4 bits | 0x5 | 5\*32bits=160bits=20bytes |
| DSCP | 6 bits | 0x0 | --- |
| ECN | 2 bits | 0x1 | --- |
| Total length | 16 bits | 0x800 | Total length of 40 bytes |
| Identification | 16 bits | 0x604 |  |
| Flags | 3 bits | 0x0 | - |
| Fragment offset | 13 bits | 0x1 | This packet contain 1bit fragments. |
| Time to live | 8 bits | 0xE0 | 128 Hops / Routers |
| Protocol | 8 bits | 0x63 | This packet should be give to TCP receive procedure. As its value indicates TCP. |
| Header checksum | 16 bits | 0xDA54 | No checksum included in this header. |
| Source IP Address | 32 bits | 190.03.25.904 | Source IP: 190.03.25.904, its local machine |
| Destination IP Address | 32 bits | 136.380.4.1.6 | Destination: 136.380.4.1.6, it is situated in \_\_\_\_ country |

**Exercise-4: Input Sequence: ARP Reply**

111000000110001111011010010101000111000101000100010011000001000110111111100111011111001110001011000010000000011000000000000000010000100000000000000001100000010000000000000000100100110000010001101111111001110111110011100010111010110000010000000001110011101011100000011000111101101001010100011100010100010010101100000100000000100000100001000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000

**Header fields of Ethernet**

|  |  |  |  |
| --- | --- | --- | --- |
| **Header Field Name** | **Length of Field (in bits)** | **Header field Value (Hex Value)** | **Meaning** |
| Destination MAC Address | 48 bits | 00: E0:63:DA:54:7144 | Receiver’s MAC address |
| Source MAC Address | 48 bits | 00: 4C:11:BF:9D:F38B | Sender’s MAC address |
| Type | 16 bits | 0x806 | 0x806 indicates, Network Header type is IPv4 Header |

**Header fields of Network**

|  |  |  |  |
| --- | --- | --- | --- |
| **Header Field Name** | **Length of Field (in bits)** | **Header field Value (Hex Value)** | **Meaning** |
| Version | 4 bits | 0x0 | IP Datagram version 0 |
| IHL | 4 bits | 0x0 | 0\*32bits=0bits=0bytes |
| DSCP | 6 bits | 0x0 | --- |
| ECN | 2 bits | 0x1 | --- |
| Total length | 16 bits | 0x800 | Total length of 40 bytes |
| Identification | 16 bits | 0x604 |  |
| Flags | 3 bits | 0x0 | - |
| Fragment offset | 13 bits | 0x2 | This packet contain 2bit fragments. |
| Time to live | 8 bits | 0x4C | 256 Hops / Routers |

Header fields of transport layer

|  |  |  |  |
| --- | --- | --- | --- |
| **Header Field Name** | **Length of Field (in bits)** | **Header field Value (Hex Value)** | **Meaning** |
| Source Port | 16 Bits | 55892 | Sender machine’s application’s logical port number 55892. |
| Destination Port | 16 Bits | 7144 | Receiver machine’s receiving logical port number 7144 which indicates source wants communicate security using https protocol. |
| Sequence Number | 32 Bits | 0xAC100821 | Unique ID assigned by sender to maintain order of packers at receiver side. |
| Acknowledgement Number | 32 Bits | 0x0 | This is not acknowledged of sent packet. |
| Header Length | 4 Bits | 0x0 | Total header Length is 0 bytes |
| Reserved Bits | 6 Bits | 0x0 | - |
| URG | 1 Bit | 0 |  |
| ACK | 1 Bit | 0 | This packet doesn’t contains valid acknowledgement number. |
| PSH | 1 Bit | 0 | No Push |
| RST | 1 Bit | 0 | No RST |
| SYN | 1 Bit | 0 | No SYN |
| FIN | 1 Bit | 0 | No Fin |
| Window Size | 16 Bits | 0x0 | - |
| Checksum | 16 Bits | 0x0 | No Error identification in packet. |
| Urgent Pointer | 16 Bits | 0x0 | No urgent content in this packet. |