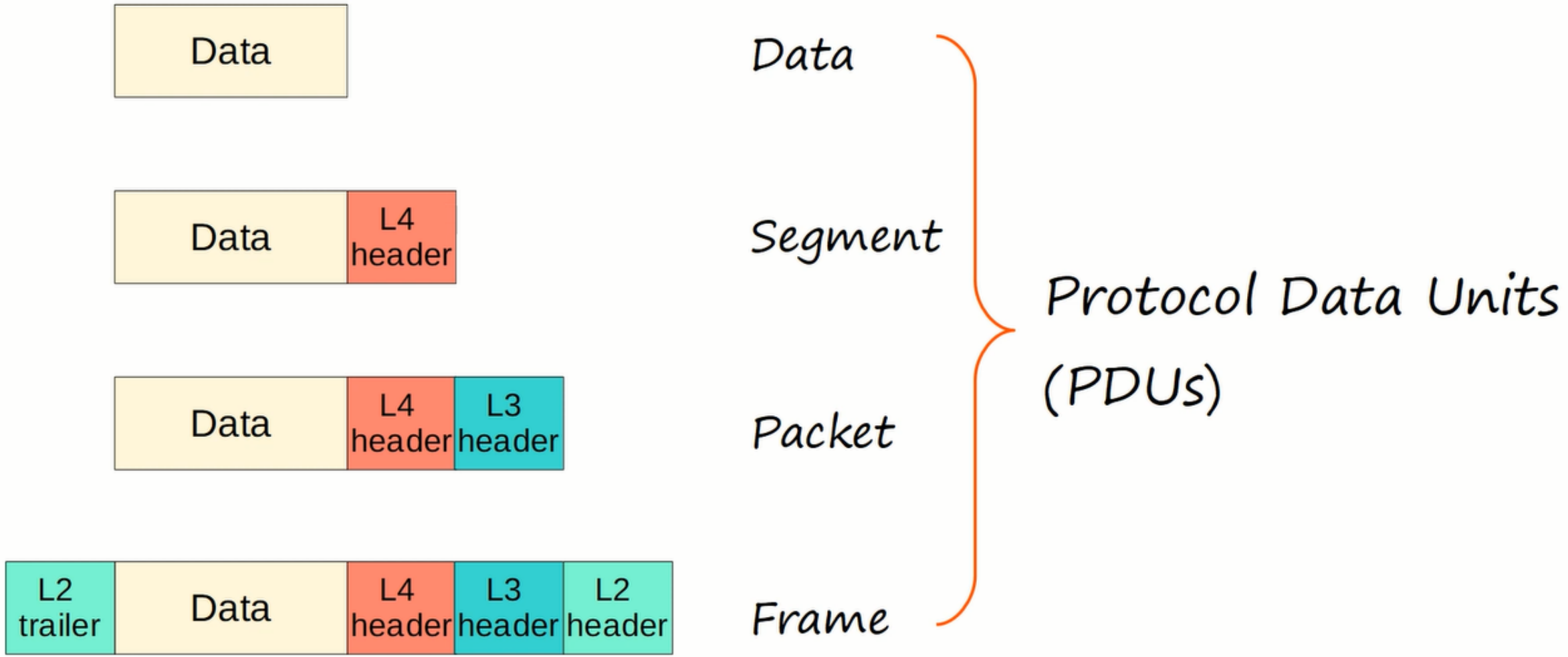
Badji Mokhtar University Annaba
Electronics Department

Lecture 5: IPV4 Header

Contact:
seifallah.nasri@univ-annaba.org

2022, Annaba, Algeria

OSI Model – PDUs



IPv4 Header

Offsets	Octet	0								1								2								3							
Octet	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Version				IHL				DSCP						ECN		Total Length															
4	32	Identification																Flags			Fragment Offset											
8	64	Time To Live								Protocol								Header Checksum															
12	96	Source IP Address																															
16	128	Destination IP Address																															
20	160	Options (if IHL > 5)																															
24	192																																
28	224																																
32	256																																

IPv4 Header – Version field

Offsets	Octet	0								1								2								3							
Octet	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Version				IHL				DSCP						ECN		Total Length															
4	32	Identification																Flags			Fragment Offset											
8	64	Time To Live								Protocol								Header Checksum															
12	96	Source IP Address																															
16	128	Destination IP Address																															
20	160	Options (if IHL > 5)																															
24	192																																
28	224																																
32	256																																

Length: 4 bits

- Identifies the version of IP used.
- IPv4 = 4 (0 1 0 0)
- IPv6 = 6 (0 1 1 0)

IPv4 Header – Internet Header Length (IHL)

Offsets	Octet	0								1								2								3							
Octet	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Version				IHL				DSCP						ECN		Total Length															
4	32	Identification																Flags			Fragment Offset											
8	64	Time To Live								Protocol								Header Checksum															
12	96	Source IP Address																															
16	128	Destination IP Address																															
20	160	Options (if IHL > 5)																															
24	192																																
28	224																																
32	256																																

Length: 4 bits

- The final field of the IPv4 header (Options) is variable in length, so this field is necessary to indicate the total length of the header.
- Identifies the length of the header **in 4-byte increments**
- Value of 5 = 5 x 4-bytes = 20 bytes

IPv4 Header – Internet Header Length (IHL)

Offsets	Octet	0								1								2								3							
Octet	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Version				IHL				DSCP						ECN		Total Length															
4	32	Identification																Flags			Fragment Offset											
8	64	Time To Live								Protocol								Header Checksum															
12	96	Source IP Address																															
16	128	Destination IP Address																															
20	160	Options (if IHL > 5)																															
24	192																																
28	224																																
32	256																																

Length: 4 bits

- Minimum value is 5 (= 20 bytes)
- Maximum value is 15 (15 x 4-bytes = 60 bytes)

1	1	1	1	
8	+ 4	+ 2	+ 1	= 15

- MINIMUM IPv4 HEADER LENGTH = 20 BYTES
- MAXIMUM IPv4 HEADER LENGTH = 60 BYTES

IPv4 Header – DSCP field

Offsets	Octet	0								1								2								3							
Octet	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Version				IHL				DSCP						ECN		Total Length															
4	32	Identification																Flags			Fragment Offset											
8	64	Time To Live								Protocol								Header Checksum															
12	96	Source IP Address																															
16	128	Destination IP Address																															
20	160	Options (if IHL > 5)																															
24	192																																
28	224																																
32	256																																

'Differentiated Services Code Point'

Length: 6 bits

- Used for QoS (Quality of Service)
- Used to prioritize delay-sensitive data (streaming voice, video, etc.)

IPv4 Header – ECN field

Offsets	Octet	0								1								2								3							
Octet	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Version				IHL				DSCP						ECN		Total Length															
4	32	Identification																Flags			Fragment Offset											
8	64	Time To Live								Protocol								Header Checksum															
12	96	Source IP Address																															
16	128	Destination IP Address																															
20	160	Options (if IHL > 5)																															
24	192																																
28	224																																
32	256																																

'Explicit Congestion Notification'

Length: 2 bits

- Provides end-to-end (between two endpoints) notification of network congestion **without dropping packets.**
- Optional feature that requires both endpoints, as well as the underlying network infrastructure, to support it.

IPv4 Header – Total Length field

Offsets	Octet	0								1								2								3							
Octet	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Version				IHL				DSCP						ECN		Total Length															
4	32	Identification																Flags			Fragment Offset											
8	64	Time To Live								Protocol								Header Checksum															
12	96	Source IP Address																															
16	128	Destination IP Address																															
20	160	Options (if IHL > 5)																															
24	192																																
28	224																																
32	256																																

Length: 16 bits

- Indicates the total length of the packet (L3 header + L4 segment)
- Measured in bytes (**not 4-byte increments like IHL**)
- Minimum value of 20 (=IPv4 header with no encapsulated data)
- Maximum value of 65,535 (maximum 16-bit value)

IPv4 Header – Identification field

Offsets	Octet	0								1								2								3							
Octet	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Version				IHL				DSCP						ECN		Total Length															
4	32	Identification																Flags			Fragment Offset											
8	64	Time To Live								Protocol								Header Checksum															
12	96	Source IP Address																															
16	128	Destination IP Address																															
20	160	Options (if IHL > 5)																															
24	192																																
28	224																																
32	256																																

Length: 16 bits

- If a packet is fragmented due to being too large, this field is used to identify which packet the fragment belongs to.
- All fragments of the same packet will have their own IPv4 header with the same value in this field.
- Packets are fragmented if larger than the **MTU** (Maximum Transmission Unit)

IPv4 Header – Identification field

Offsets	Octet	0								1								2								3							
Octet	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Version				IHL				DSCP						ECN		Total Length															
4	32	Identification																Flags			Fragment Offset											
8	64	Time To Live								Protocol								Header Checksum															
12	96	Source IP Address																															
16	128	Destination IP Address																															
20	160	Options (if IHL > 5)																															
24	192																																
28	224																																
32	256																																

Length: 16 bits

- The MTU is usually **1500 bytes**
- Remember the maximum size of an Ethernet frame?
- Fragments are reassembled by the receiving host

IPv4 Header – Flags field

Offsets	Octet	0								1								2								3							
Octet	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Version				IHL				DSCP						ECN		Total Length															
4	32	Identification																Flags			Fragment Offset											
8	64	Time To Live								Protocol								Header Checksum															
12	96	Source IP Address																															
16	128	Destination IP Address																															
20	160	Options (if IHL > 5)																															
24	192																																
28	224																																
32	256																																

Length: 3 bits

*Unfragmented packets will always have their MF bit set to 0

- Used to control/identify fragments.
- Bit 0: Reserved, always set to 0
- Bit 1: Don't Fragment (DF bit), used to indicate a packet that should not be fragmented
- Bit 2: More Fragments (MF bit), set to 1 if there are more fragments in the packet, set to 0 for the last fragment

IPv4 Header – Fragment Offset field

Offsets	Octet	0								1								2								3							
Octet	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Version				IHL				DSCP						ECN		Total Length															
4	32	Identification																Flags		Fragment Offset													
8	64	Time To Live								Protocol								Header Checksum															
12	96	Source IP Address																															
16	128	Destination IP Address																															
20	160	Options (if IHL > 5)																															
24	192																																
28	224																																
32	256																																

Length: 13 bits

- Used to indicate the position of the fragment within the original, unfragmented IP packet.
- Allows fragmented packets to be reassembled even if the fragments arrive out of order.

IPv4 Header – Time To Live field

Offsets	Octet	0								1								2								3							
Octet	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Version				IHL				DSCP						ECN		Total Length															
4	32	Identification																Flags			Fragment Offset											
8	64	Time To Live								Protocol								Header Checksum															
12	96	Source IP Address																															
16	128	Destination IP Address																															
20	160	Options (if IHL > 5)																															
24	192																																
28	224																																
32	256																																

Length: 8 bits

Recommended default TTL is 64.

- A router will drop a packet with a TTL of 0
- Used to prevent infinite loops
- Originally designed to indicate the packet's maximum lifetime in seconds
- In practice, indicates a 'hop count': each time the packet arrives at a router, the router decreases the TTL by 1.

IPv4 Header – Protocol field

Offsets	Octet	0								1								2								3							
Octet	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Version				IHL				DSCP						ECN		Total Length															
4	32	Identification																Flags			Fragment Offset											
8	64	Time To Live								Protocol								Header Checksum															
12	96	Source IP Address																															
16	128	Destination IP Address																															
20	160	Options (if IHL > 5)																															
24	192																																
28	224																																
32	256																																

Length: 8 bits

- Indicates the protocol of the encapsulated L4PDU
- Value of 6: TCP
- Value of 17: UDP
- Value of 1: ICMP
- Value of 89: OSPF (dynamic routing protocol)

IPv4 Header – Header Checksum field

Offsets	Octet	0								1								2								3							
Octet	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Version				IHL				DSCP						ECN		Total Length															
4	32	Identification																Flags			Fragment Offset											
8	64	Time To Live								Protocol								Header Checksum															
12	96	Source IP Address																															
16	128	Destination IP Address																															
20	160	Options (if IHL > 5)																															
24	192																																
28	224																																
32	256																																

Length: 16 bits

- A calculated checksum used to check for errors in the IPv4 header.
- When a router receives a packet, it calculates the checksum of the header and compares it to the one in this field of the header.
- If they do not match, the router drops the packet.

IPv4 Header – Header Checksum field

Offsets	Octet	0								1								2								3							
Octet	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Version				IHL				DSCP						ECN		Total Length															
4	32	Identification																Flags			Fragment Offset											
8	64	Time To Live								Protocol								Header Checksum															
12	96	Source IP Address																															
16	128	Destination IP Address																															
20	160	Options (if IHL > 5)																															
24	192																																
28	224																																
32	256																																

Length: 16 bits

- Used to check for errors only in the IPv4 header.
- IP relies on the encapsulated protocol to detect errors in the encapsulated data.
- Both TCP and UDP have their own checksum fields to detect errors in the encapsulated data.

IPv4 Header – Source/Destination IP Address fields

Offsets	Octet	0								1								2								3							
Octet	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Version				IHL				DSCP						ECN		Total Length															
4	32	Identification																Flags			Fragment Offset											
8	64	Time To Live								Protocol								Header Checksum															
12	96	Source IP Address																															
16	128	Destination IP Address																															
20	160	Options (if IHL > 5)																															
24	192																																
28	224																																
32	256																																

Length: 32 bits (each)

- Source IP Address = IPv4 address of the sender of the packet.
- Destination IP Address = IPv4 address of the intended receiver of the packet.

IPv4 Header – Options fields

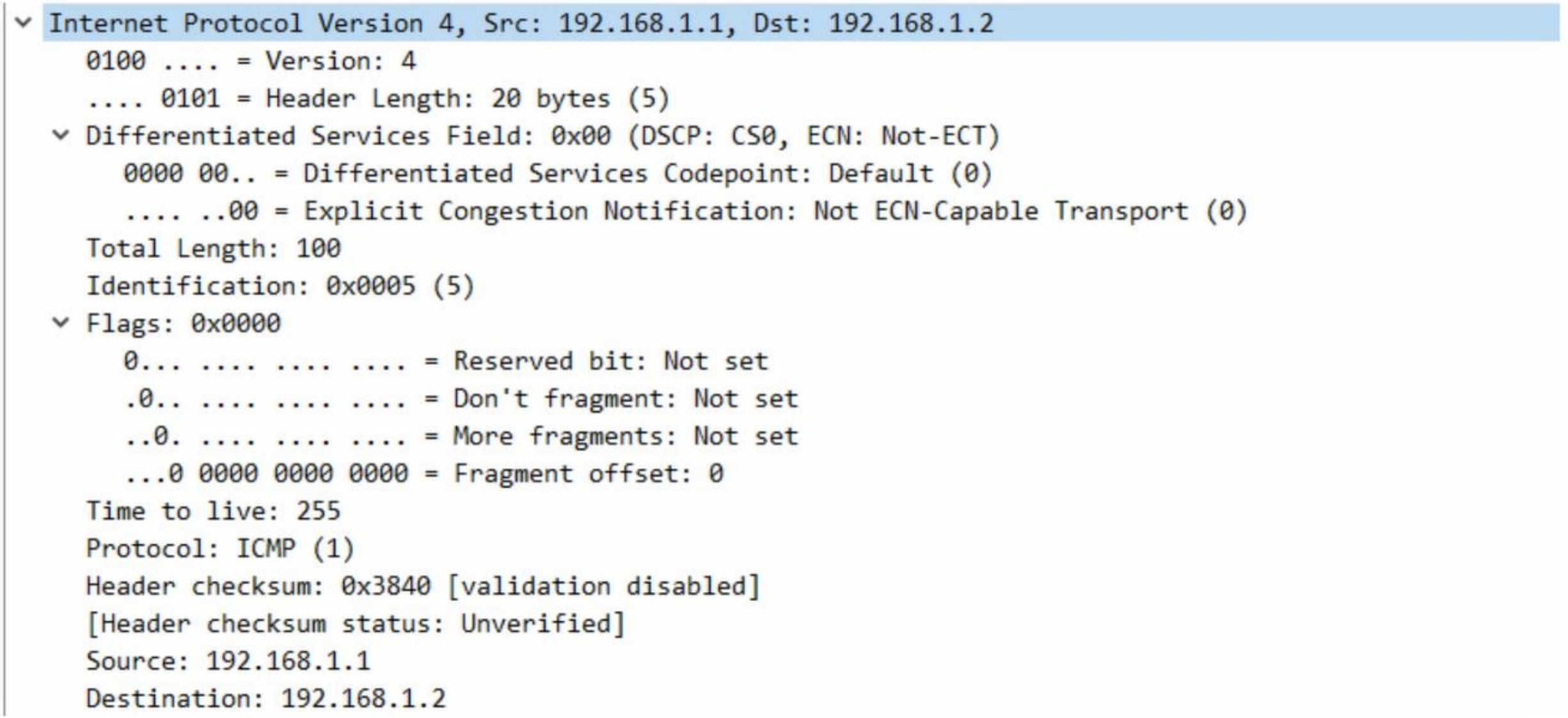
Offsets	Octet	0								1								2								3							
Octet	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Version				IHL				DSCP						ECN		Total Length															
4	32	Identification																Flags			Fragment Offset											
8	64	Time To Live								Protocol								Header Checksum															
12	96	Source IP Address																															
16	128	Destination IP Address																															
20	160	Options (if IHL > 5)																															
24	192																																
28	224																																
32	256																																

Length: 0 - 320 bits

- Rarely used.
- If the IHL field is greater than 5, it means that Options are present.

Field	Size (bits)	Description
Copied	1	Set to 1 if the options need to be copied into all fragments of a fragmented packet.
Option Class	2	A general options category. 0 is for "control" options, and 2 is for "debugging and measurement". 1 and 3 are reserved.
Option Number	5	Specifies an option.
Option Length	8	Indicates the size of the entire option (including this field). This field may not exist for simple options.
Option Data	Variable	Option-specific data. This field may not exist for simple options.

Wireshark Packet Capture



Wireshark Packet Capture

```
R1#ping 192.168.1.2 size 10000
```

7	17.411175	192.168.1.1	192.168.1.2	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=0001) [Reassembled in #13]
8	17.412827	192.168.1.1	192.168.1.2	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=0001) [Reassembled in #13]
9	17.414347	192.168.1.1	192.168.1.2	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=2960, ID=0001) [Reassembled in #13]
10	17.415913	192.168.1.1	192.168.1.2	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=4440, ID=0001) [Reassembled in #13]
11	17.417560	192.168.1.1	192.168.1.2	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=5920, ID=0001) [Reassembled in #13]
12	17.419203	192.168.1.1	192.168.1.2	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=7400, ID=0001) [Reassembled in #13]
13	17.420793	192.168.1.1	192.168.1.2	ICMP	1134	Echo (ping) request id=0x0000, seq=1/256, ttl=255 (reply in 20)

Wireshark Packet Capture

```
Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.2
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
▾ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    0000 00.. = Differentiated Services Codepoint: Default (0)
          00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
  Total Length: 1500
  Identification: 0x0001 (1)
▾ Flags: 0x2000, More fragments
    0... .... .... .... = Reserved bit: Not set
    .0.. .... .... .... = Don't fragment: Not set
    ..1. .... .... .... = More fragments: Set
    ...0 0000 0000 0000 = Fragment offset: 0
  Time to live: 255
  Protocol: ICMP (1)
  Header checksum: 0x12cc [validation disabled]
  [Header checksum status: Unverified]
  Source: 192.168.1.1
  Destination: 192.168.1.2
  Reassembled IPv4 in frame: 13
```

```
Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.2
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
▾ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    0000 00.. = Differentiated Services Codepoint: Default (0)
          00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
  Total Length: 1500
  Identification: 0x0001 (1)
▾ Flags: 0x20b9, More fragments
    0... .... .... .... = Reserved bit: Not set
    .0.. .... .... .... = Don't fragment: Not set
    ..1. .... .... .... = More fragments: Set
    ...0 0000 1011 1001 = Fragment offset: 185
  Time to live: 255
  Protocol: ICMP (1)
  Header checksum: 0x1213 [validation disabled]
  [Header checksum status: Unverified]
  Source: 192.168.1.1
  Destination: 192.168.1.2
  Reassembled IPv4 in frame: 13
```

Wireshark Packet Capture

```
R1#ping 192.168.1.2 df-bit
```

```
▾ Flags: 0x4000, Don't fragment
      0... .... .... .... = Reserved bit: Not set
      .1.. .... .... .... = Don't fragment: Set
      ..0. .... .... .... = More fragments: Not set
      ...0 0000 0000 0000 = Fragment offset: 0
```

```
R1#ping 192.168.1.2 size 10000 df-bit
Type escape sequence to abort.
Sending 5, 10000-byte ICMP Echos to 192.168.1.2, timeout is 2 seconds:
Packet sent with the DF bit set
.....
Success rate is 0 percent (0/5)
```

Quiz Question 1

What is the fixed binary value of the first field of an IPv4 header?

a) 0010

b) 0110

c) 0001

d) 0100

Quiz Question 1

What is the fixed binary value of the first field of an IPv4 header?

a) 0010

b) 0110

c) 0001

d) 0100

Offsets	Octet	0								1								2								3							
Octet	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Version				IHL				DSCP						ECN		Total Length															
4	32	Identification																Flags			Fragment Offset											
8	64	Time To Live								Protocol								Header Checksum															
12	96	Source IP Address																															
16	128	Destination IP Address																															
20	160	Options (if IHL > 5)																															
24	192																																
28	224																																
32	256																																

Quiz Question 2

Which field will cause the packet to be dropped if it has a value of 0?

a) TTL

b) DSCP

c) IHL

d) ECN

Quiz Question 2

Which field will cause the packet to be dropped if it has a value of 0?

a) TTL

b) DSCP

c) IHL

d) ECN

TTL stands for Time To Live. It is reduced by 1 at each router the packet passes through. If it reaches 0, the packet is dropped.

Quiz Question 3

How are errors in an IPv4 packet's encapsulated data detected?

a) The IPv4 **Header Checksum** field checks for errors.

b) The encapsulated protocol (TCP, UDP) checks for errors.

c) Errors in the encapsulated data cannot be detected.

Quiz Question 3

How are errors in an IPv4 packet's encapsulated data detected?

a) The IPv4 **Header Checksum** field checks for errors.

b) The encapsulated protocol (TCP, UDP) checks for errors.

c) Errors in the encapsulated data cannot be detected.

The IPv4 **Header Checksum** field only checks for errors in the IPv4 header itself. However, Layer 4 protocols like TCP or UDP can use their checksum to check for errors in the encapsulated data.

Quiz Question 4

Which field of an IPv4 header is variable in length?

a) Options

b) Header Checksum

c) Total Length

d) IHL

Quiz Question 4

Which field of an IPv4 header is variable in length?

a) Options

b) Header Checksum

c) Total Length

d) IHL

The **Options** field can vary in length from 0 bits to 320 bits. The other fields are fixed-length. Although the **Total Length** and **IHL** fields are used to represent the variable length of the IPv4 header and packet, the fields themselves are fixed in length.

Quiz Question 5

Which bit will be set to 1 on all IPv4 packet fragments except the last fragment?

a) Fragment Offset bit

b) More Fragments bit

c) Don't Fragment bit

d) Packet Fragment bit

Quiz Question 5

Which bit will be set to 1 on all IPv4 packet fragments except the last fragment?

a) Fragment Offset bit

b) More Fragments bit

c) Don't Fragment bit

d) Packet Fragment bit

The **More Fragments** bit, part of the **Flags** field of the IPv4 header, is used to indicate that the current fragment is not the last fragment of a fragmented packet. It is set to 1 on all fragments except the last, which will set it to 0.