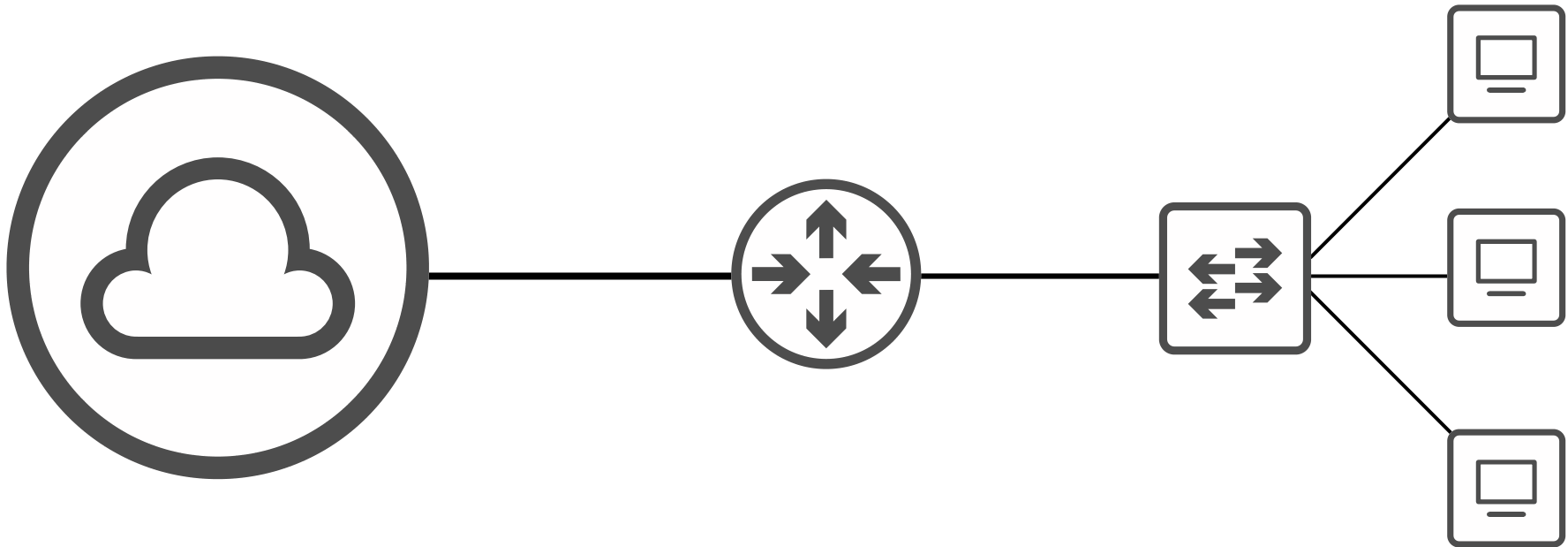


CCNA 200-301 Day 10

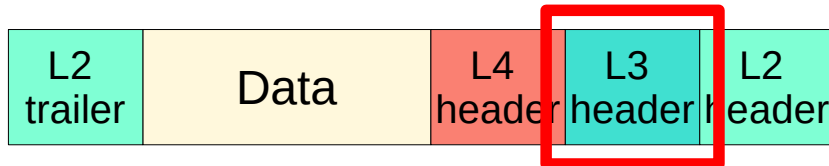
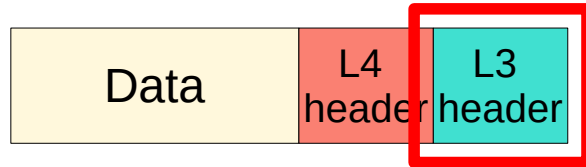
IPv4 Header



Things we'll cover

- IPv4 packet structure
- Fields of the IPv4 header

OSI Model – PDUs



Data

Segment

Packet

Frame

Protocol Data Units
(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	<input type="checkbox"/>	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																															<input type="checkbox"/>	

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)

$$\begin{array}{cccc}
 \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} \\
 \mathbf{8} & + & \mathbf{4} & + & \mathbf{2} & + & \mathbf{1} & = & \mathbf{15}
 \end{array}$$

- 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 – 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

1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
 32768 16384 8192 4096 2048 1024 512 256 128 64 32 16 8 4 2 1

= 65535

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																																
24	192																																
28	224																																
32	256	Options (if IHL > 5)																															

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																																
24	192																																
28	224																																
32	256																																

Length: 3 bits

- 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

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

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)
- https://en.wikipedia.org/wiki/List_of_IP_protocol_numbers

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																																
24	192																																
28	224	Options (if IHL > 5)																															
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								Destination IP Address																							
16	128	Destination IP Address								Options (if IHL > 5)																							
20	160	Options (if IHL > 5)								Options (if IHL > 5)																							
24	192	Options (if IHL > 5)								Options (if IHL > 5)																							
28	224	Options (if IHL > 5)								Options (if IHL > 5)																							
32	256	Options (if IHL > 5)								Options (if IHL > 5)																							

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.

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																																

Wireshark Packet Capture

Wireshark interface showing a packet capture of ICMP ping requests and replies between 192.168.1.1 and 192.168.1.2. Packet 5 is highlighted in red.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	0c:99:2a:f2:55:00	0c:99:2a:f2:55:00	LOOP	60	Reply
2	1.390201	0c:99:2a:8a:bd:00	0c:99:2a:8a:bd:00	LOOP	60	Reply
3	10.100463	0c:99:2a:f2:55:00	0c:99:2a:f2:55:00	LOOP	60	Reply
4	11.454510	0c:99:2a:8a:bd:00	0c:99:2a:8a:bd:00	LOOP	60	Reply
5	12.265055	192.168.1.1	192.168.1.2	ICMP	114	Echo (ping) request id=0x0001, seq=0/0, ttl=255 (reply in 6)
6	12.267629	192.168.1.2	192.168.1.1	ICMP	114	Echo (ping) reply id=0x0001, seq=0/0, ttl=255 (request in 5)
7	12.271809	192.168.1.1	192.168.1.2	ICMP	114	Echo (ping) request id=0x0001, seq=1/256, ttl=255 (reply in 8)
8	12.273420	192.168.1.2	192.168.1.1	ICMP	114	Echo (ping) reply id=0x0001, seq=1/256, ttl=255 (request in 7)
9	12.276097	192.168.1.1	192.168.1.2	ICMP	114	Echo (ping) request id=0x0001, seq=2/512, ttl=255 (reply in 10)
10	12.277896	192.168.1.2	192.168.1.1	ICMP	114	Echo (ping) reply id=0x0001, seq=2/512, ttl=255 (request in 9)
11	12.280969	192.168.1.1	192.168.1.2	ICMP	114	Echo (ping) request id=0x0001, seq=3/768, ttl=255 (reply in 12)
12	12.282918	192.168.1.2	192.168.1.1	ICMP	114	Echo (ping) reply id=0x0001, seq=3/768, ttl=255 (request in 11)
13	12.287860	192.168.1.1	192.168.1.2	ICMP	114	Echo (ping) request id=0x0001, seq=4/1024, ttl=255 (reply in 14)
14	12.289538	192.168.1.2	192.168.1.1	ICMP	114	Echo (ping) reply id=0x0001, seq=4/1024, ttl=255 (request in 13)

Frame 5: 114 bytes on wire (912 bits), 114 bytes captured (912 bits) on interface 0

- Ethernet II, Src: 0c:99:2a:f2:55:00 (0c:99:2a:f2:55:00), Dst: 0c:99:2a:8a:bd:00 (0c:99:2a:8a:bd:00)
- Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.2
- Internet Control Message Protocol

```
0000 0c 99 2a 8a bd 00 0c 99 2a f2 55 00 08 00 45 00  .*.U...E-
0010 00 64 00 05 00 00 ff 01 38 40 c0 a8 01 01 c0 a8  .d....8@....
0020 01 02 08 00 80 7a 00 01 00 00 00 00 00 00 01  .z.....
0030 fd cd ab cd ab cd ab cd ab cd ab cd ab cd ab cd  .....
0040 ab cd ab cd ab cd ab cd ab cd ab cd ab cd ab cd  .....
0050 ab cd ab cd ab cd ab cd ab cd ab cd ab cd ab cd  .....
0060 ab cd ab cd ab cd ab cd ab cd ab cd ab cd ab cd  .....
0070 ab cd
```

Wireshark Packet Capture

Wireshark interface showing a packet capture on interface eth0. The main pane displays a list of 14 ICMP Echo (ping) packets. Packet 5 is selected, showing its details in the middle pane and its raw bytes in the bottom pane.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	0c:99:2a:f2:55:00	0c:99:2a:f2:55:00	LOOP	60	Reply
2	1.390201	0c:99:2a:8a:bd:00	0c:99:2a:8a:bd:00	LOOP	60	Reply
3	10.100463	0c:99:2a:f2:55:00	0c:99:2a:f2:55:00	LOOP	60	Reply
4	11.454510	0c:99:2a:8a:bd:00	0c:99:2a:8a:bd:00	LOOP	60	Reply
5	12.265055	192.168.1.1	192.168.1.2	ICMP	114	Echo (ping) request id=0x0001, seq=0/0, ttl=255 (reply in 6)
6	12.267829	192.168.1.2	192.168.1.1	ICMP	114	Echo (ping) reply id=0x0001, seq=0/0, ttl=255 (request in 5)
7	12.271809	192.168.1.1	192.168.1.2	ICMP	114	Echo (ping) request id=0x0001, seq=1/256, ttl=255 (reply in 8)
8	12.273420	192.168.1.2	192.168.1.1	ICMP	114	Echo (ping) reply id=0x0001, seq=1/256, ttl=255 (request in 7)
9	12.276097	192.168.1.1	192.168.1.2	ICMP	114	Echo (ping) request id=0x0001, seq=2/512, ttl=255 (reply in 10)
10	12.277896	192.168.1.2	192.168.1.1	ICMP	114	Echo (ping) reply id=0x0001, seq=2/512, ttl=255 (request in 9)
11	12.280969	192.168.1.1	192.168.1.2	ICMP	114	Echo (ping) request id=0x0001, seq=3/768, ttl=255 (reply in 12)
12	12.282918	192.168.1.2	192.168.1.1	ICMP	114	Echo (ping) reply id=0x0001, seq=3/768, ttl=255 (request in 11)
13	12.287860	192.168.1.1	192.168.1.2	ICMP	114	Echo (ping) request id=0x0001, seq=4/1024, ttl=255 (reply in 14)
14	12.289538	192.168.1.2	192.168.1.1	ICMP	114	Echo (ping) reply id=0x0001, seq=4/1024, ttl=255 (request in 13)

Packet 5 details:

- Ethernet II, Src: 0c:99:2a:f2:55:00 (0c:99:2a:f2:55:00), Dst: 0c:99:2a:8a:bd:00 (0c:99:2a:8a:bd:00)
- Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.2
- Internet Control Message Protocol

Raw bytes (hex):

```
0000 0c 99 2a 8a bd 00 0c 99 2a f2 55 00 08 00 45 00  ..*....*.U...E-
0010 00 64 00 05 00 00 ff 01 38 40 c0 a8 01 01 c0 a8  -d.....8@.....
0020 01 02 08 00 80 7a 00 01 00 00 00 00 00 00 01  .....z.....
0030 fd cd ab cd ab cd ab cd ab cd ab cd ab cd ab cd  .....
0040 ab cd ab cd ab cd ab cd ab cd ab cd ab cd ab cd  .....
0050 ab cd ab cd ab cd ab cd ab cd ab cd ab cd ab cd  .....
0060 ab cd ab cd ab cd ab cd ab cd ab cd ab cd ab cd  .....
0070 ab cd  ..
```


Wireshark Packet Capture

Wireshark interface showing a packet capture on interface [R1 Gi0/0 to R2 Gi0/0]. The main pane displays a list of 14 packets. Packet 5 is selected, showing details for Ethernet II, Internet Protocol Version 4, and Internet Control Message Protocol. The hex dump pane shows the raw bytes of the selected packet, with a red box highlighting the IP header fields.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	0c:99:2a:f2:55:00	0c:99:2a:f2:55:00	LOOP	60	Reply
2	1.390201	0c:99:2a:8a:bd:00	0c:99:2a:8a:bd:00	LOOP	60	Reply
3	10.100463	0c:99:2a:f2:55:00	0c:99:2a:f2:55:00	LOOP	60	Reply
4	11.454510	0c:99:2a:8a:bd:00	0c:99:2a:8a:bd:00	LOOP	60	Reply
5	12.265055	192.168.1.1	192.168.1.2	ICMP	114	Echo (ping) request id=0x0001, seq=0/0, ttl=255 (reply in 6)
6	12.267829	192.168.1.2	192.168.1.1	ICMP	114	Echo (ping) reply id=0x0001, seq=0/0, ttl=255 (request in 5)
7	12.271809	192.168.1.1	192.168.1.2	ICMP	114	Echo (ping) request id=0x0001, seq=1/256, ttl=255 (reply in 8)
8	12.273420	192.168.1.2	192.168.1.1	ICMP	114	Echo (ping) reply id=0x0001, seq=1/256, ttl=255 (request in 7)
9	12.276097	192.168.1.1	192.168.1.2	ICMP	114	Echo (ping) request id=0x0001, seq=2/512, ttl=255 (reply in 10)
10	12.277896	192.168.1.2	192.168.1.1	ICMP	114	Echo (ping) reply id=0x0001, seq=2/512, ttl=255 (request in 9)
11	12.280969	192.168.1.1	192.168.1.2	ICMP	114	Echo (ping) request id=0x0001, seq=3/768, ttl=255 (reply in 12)
12	12.282918	192.168.1.2	192.168.1.1	ICMP	114	Echo (ping) reply id=0x0001, seq=3/768, ttl=255 (request in 11)
13	12.287860	192.168.1.1	192.168.1.2	ICMP	114	Echo (ping) request id=0x0001, seq=4/1024, ttl=255 (reply in 14)
14	12.289538	192.168.1.2	192.168.1.1	ICMP	114	Echo (ping) reply id=0x0001, seq=4/1024, ttl=255 (request in 13)

Frame 5: 114 bytes on wire (912 bits), 114 bytes captured (912 bits) on interface 0
Ethernet II, Src: 0c:99:2a:f2:55:00 (0c:99:2a:f2:55:00), Dst: 0c:99:2a:8a:bd:00 (0c:99:2a:8a:bd:00)

Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.2

Internet Control Message Protocol

```
0000 0c 99 2a 8a bd 00 0c 99 2a f2 55 00 08 00 45 00  *U...E-
0010 00 64 00 05 00 00 ff 01 38 40 c0 a8 01 01 c0 a8  d....8@....
0020 01 02 08 00 80 7a 00 01 00 00 00 00 00 00 01  z.....
0030 fd cd ab cd ab cd ab cd ab cd ab cd ab cd ab cd  ....
0040 ab cd ab cd ab cd ab cd ab cd ab cd ab cd ab cd  ....
0050 ab cd ab cd ab cd ab cd ab cd ab cd ab cd ab cd  ....
0060 ab cd ab cd ab cd ab cd ab cd ab cd ab cd ab cd  ....
0070 ab cd ..
```



Wireshark Packet Capture

Wireshark interface showing a packet capture on interface [R1 Gi0/0 to R2 Gi0/0]. The main display area shows a list of packets, with packet 5 selected. The packet list table is as follows:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	0c:99:2a:f2:55:00	0c:99:2a:f2:55:00	LOOP	60	Reply
2	1.390201	0c:99:2a:8a:bd:00	0c:99:2a:8a:bd:00	LOOP	60	Reply
3	10.100463	0c:99:2a:f2:55:00	0c:99:2a:f2:55:00	LOOP	60	Reply
4	11.454510	0c:99:2a:8a:bd:00	0c:99:2a:8a:bd:00	LOOP	60	Reply
5	12.265055	192.168.1.1	192.168.1.2	ICMP	114	Echo (ping) request id=0x0001, seq=0/0, ttl=255 (reply in 6)
6	12.267829	192.168.1.2	192.168.1.1	ICMP	114	Echo (ping) reply id=0x0001, seq=0/0, ttl=255 (request in 5)
7	12.271809	192.168.1.1	192.168.1.2	ICMP	114	Echo (ping) request id=0x0001, seq=1/256, ttl=255 (reply in 8)
8	12.273420	192.168.1.2	192.168.1.1	ICMP	114	Echo (ping) reply id=0x0001, seq=1/256, ttl=255 (request in 7)
9	12.276097	192.168.1.1	192.168.1.2	ICMP	114	Echo (ping) request id=0x0001, seq=2/512, ttl=255 (reply in 10)
10	12.277896	192.168.1.2	192.168.1.1	ICMP	114	Echo (ping) reply id=0x0001, seq=2/512, ttl=255 (request in 9)
11	12.280969	192.168.1.1	192.168.1.2	ICMP	114	Echo (ping) request id=0x0001, seq=3/768, ttl=255 (reply in 12)
12	12.282918	192.168.1.2	192.168.1.1	ICMP	114	Echo (ping) reply id=0x0001, seq=3/768, ttl=255 (request in 11)
13	12.287860	192.168.1.1	192.168.1.2	ICMP	114	Echo (ping) request id=0x0001, seq=4/1024, ttl=255 (reply in 14)
14	12.289538	192.168.1.2	192.168.1.1	ICMP	114	Echo (ping) reply id=0x0001, seq=4/1024, ttl=255 (request in 13)

The packet details pane for Frame 5 shows:

- Frame 5: 114 bytes on wire (912 bits), 114 bytes captured (912 bits) on interface 0
- Ethernet II, Src: 0c:99:2a:f2:55:00 (0c:99:2a:f2:55:00), Dst: 0c:99:2a:8a:bd:00 (0c:99:2a:8a:bd:00)
- Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.2
- Internet Control Message Protocol**

The packet bytes pane shows the raw data for the ICMP Echo (ping) request:

```

000  0c 99 2a 8a bd 00 0c 99 2a f2 55 00 08 00 45 00  ..*...*.U...E-
001  00 64 00 05 00 00 ff 01 38 40 c0 a8 01 01 c0 a8  -d.....8@.....
002  01 02 08 00 80 7a 00 01 00 00 00 00 00 00 01  -...z-.....
003  fd cd ab cd ab cd ab cd ab cd ab cd ab cd ab  -.....
004  ab cd ab cd ab cd ab cd ab cd ab cd ab cd ab  -.....
005  ab cd ab cd ab cd ab cd ab cd ab cd ab cd ab  -.....
006  ab cd ab cd ab cd ab cd ab cd ab cd ab cd ab  -.....
007  ab cd
  
```

At the bottom of the interface, the status bar indicates: Internet Control Message Protocol (icmp), 80 bytes | Packets: 22 · Displayed: 22 (100.0%) · Dropped: 0 (0.0%) | Profile: Default

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: 100

Identification: 0x0005 (5)

Flags: 0x0000

0... = Reserved bit: Not set

.0.. = Don't fragment: Not set

..0. = More fragments: Not set

...0 0000 0000 0000 = Fragment offset: 0

Time to live: 255

Protocol: ICMP (1)

Header checksum: 0x3840 [validation disabled]

[Header checksum status: Unverified]

Source: 192.168.1.1

Destination: 192.168.1.2

```
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)
```

Things we covered

- IPv4 packet structure
- Fields of the IPv4 header

QUIZ

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

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.

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

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

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.