

Figure 9.8: ARP packet

Hardware: LAN or WAN protocol

Protocol: Network-layer protocol

0	8	16	31
Hardware Type		Protocol Type	
Hardware length	Protocol length	Operation Request:1, Reply:2	
Source hardware address			
Source protocol address			
Destination hardware address (Empty in request)			
Destination protocol address			

Activate Windows
Go to Settings to activate Windows.

Ch_11.pdf

File | E:/Study/Du_mca/2nd_semester/Computer_Network/New_ppt/Edited_Pdf_s/Ch_11.pdf

7 of 60

Figure 11.1: A frame in a character-oriented protocol

The diagram illustrates the structure of a frame in a character-oriented protocol. It consists of a sequence of segments: a **Flag** segment, a **Header** segment, a variable number of data segments (represented by three light blue boxes and an ellipsis), a **Trailer** segment, and another **Flag** segment. A double-headed arrow above the data segments is labeled "Data from upper layer" and "Variable number of characters".

11.7

Activate Windows
Go to Settings to activate Windows.

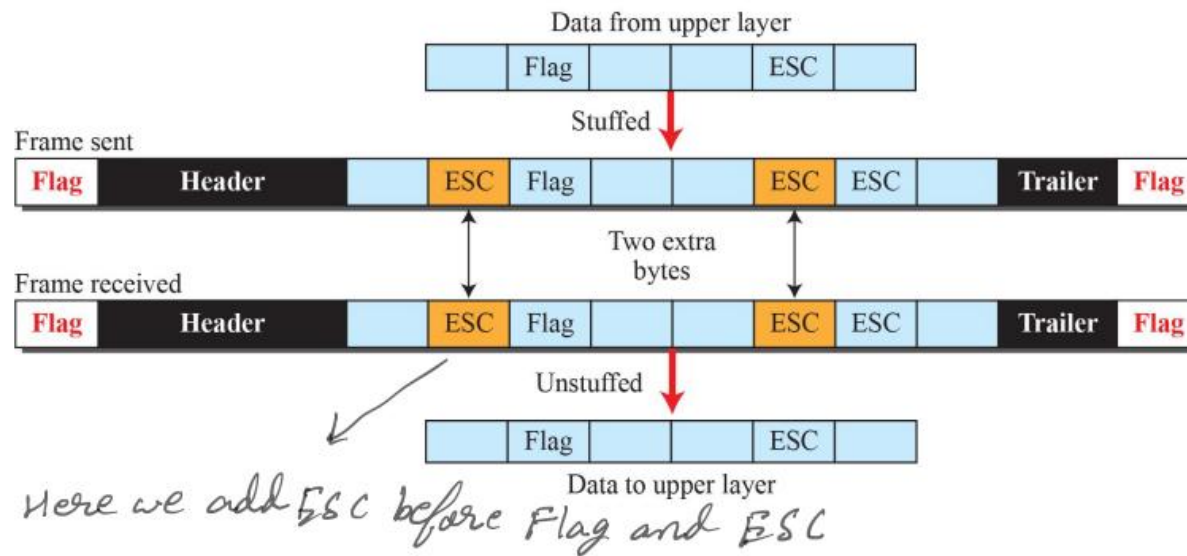
Type here to search

40°C Haze 14:54 25-05-2024

11.7

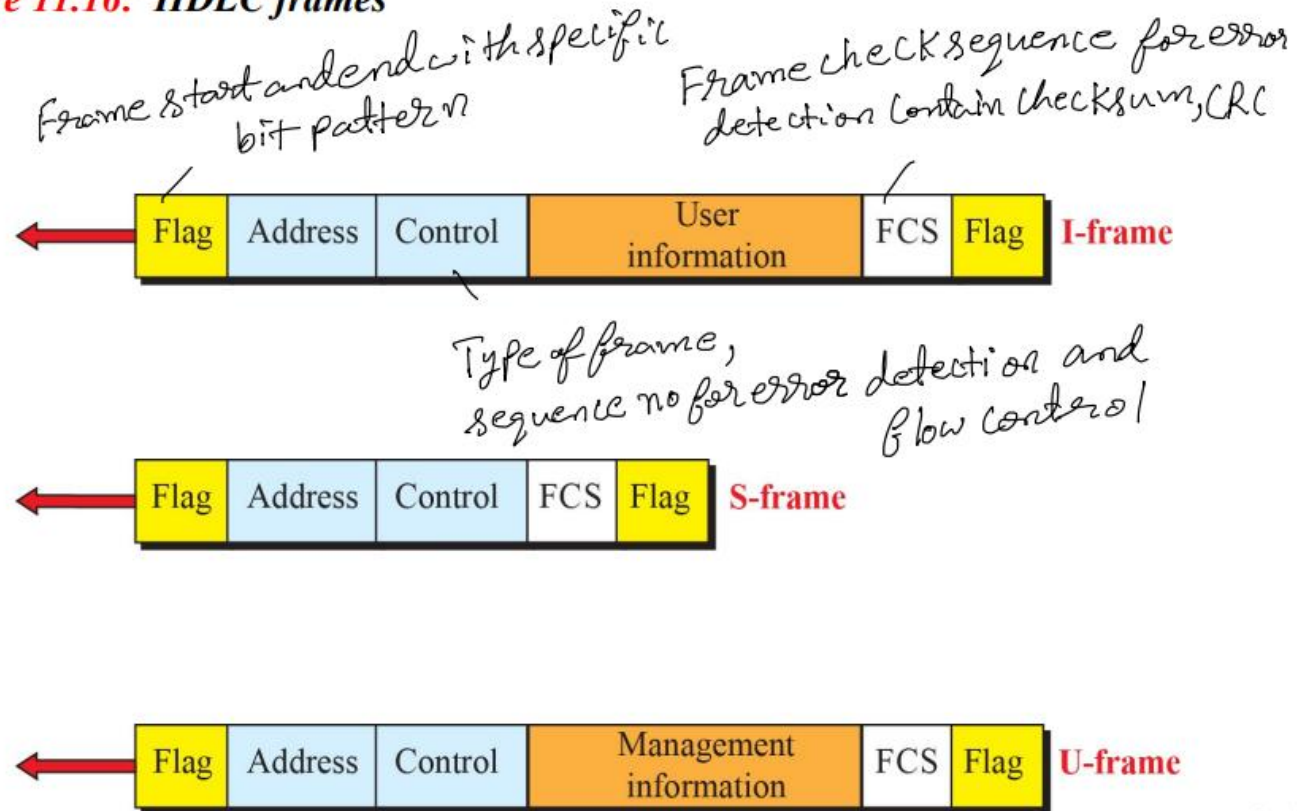
Figure 11.2: Byte stuffing and unstuffing

ESC → Escape sequencing



Activate Windows
Go to Settings to activate Windows.

Figure 11.16: HDLC frames



Activate Windows
Go to Settings to activate Windows.

Ch_11.pdf

File | E:/Study/Du_mca/2nd_semester/Computer_Network/New_ppt/Edited_Pdf_s/Ch_11.pdf

44 of 60

11.43

Figure 11.20: PPP frame format

The diagram illustrates the structure of a PPP (Point-to-Point Protocol) frame. It consists of the following fields in sequence:

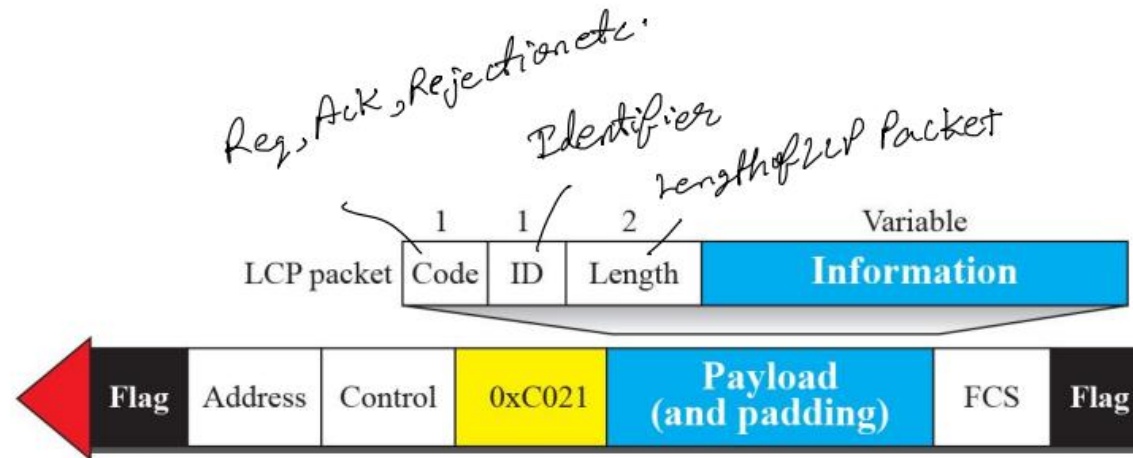
- Flag**: 1 byte. The first flag is marked with a red arrow and the binary value $(11111111)_2$.
- Address**: 1 byte.
- Control**: 1 byte. The third flag is marked with the binary value $(00000011)_2$.
- Protocol**: 1/2 bytes.
- Payload**: Variable length. A handwritten note "It contain data" points to this field.
- FCS**: 2/4 bytes.
- Flag**: 1 byte.

Type here to search

40°C Haze 15:29 25-05-2024 ENG

Figure 11.23: LCP packet encapsulated in a frame

Link Control protocol



Activate Windows
Go to Settings to activate Windows.



Type here to search



40°C Haze



15:32
25-05-2024



Figure 12.29: General rules and examples of creating Walsh tables

$2^n = 2 \ 4 \ 8$ Here $2N \rightarrow$ denote no of rows

$$W_1 = \begin{bmatrix} +1 \end{bmatrix} \quad W_{2N} = \begin{bmatrix} W_N & W_N \\ W_N & \overline{W_N} \end{bmatrix}$$

a. Two basic rules

$$W_2 = \begin{bmatrix} +1 & +1 \\ +1 & -1 \end{bmatrix} \quad W_4 = \begin{bmatrix} +1 & +1 & +1 & +1 \\ +1 & -1 & +1 & -1 \\ +1 & +1 & -1 & -1 \\ +1 & -1 & -1 & +1 \end{bmatrix}$$

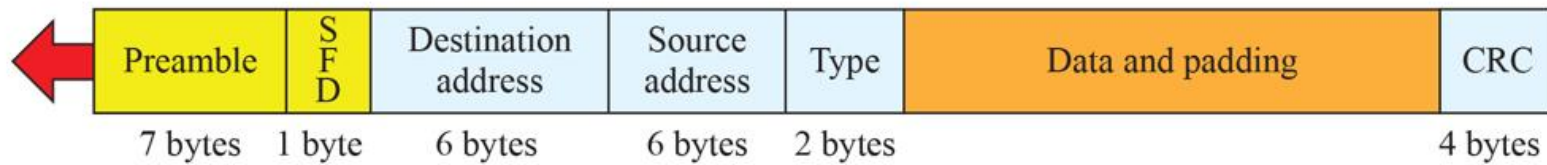
b. Generation of W_1 , W_2 , and W_4

Activate Windows
Go to Settings to activate Windows.

Figure 13.3: Ethernet frame

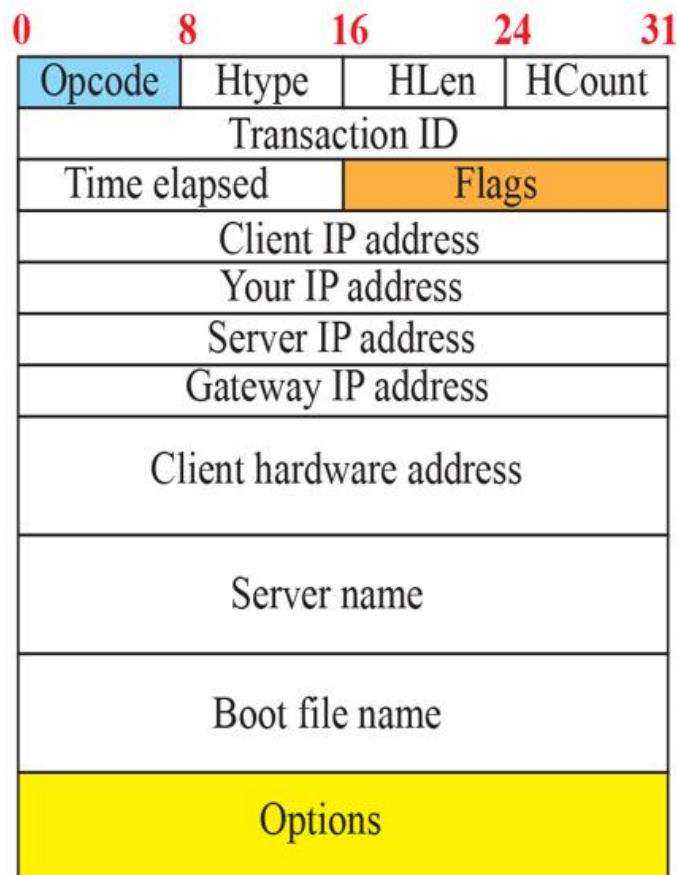
Preamble: 56 bits of alternating 1s and 0s

SFD: Start frame delimiter, flag (10101011)



Activate Windows
Go to Settings to activate Windows.

Figure 18.25: DHCP message format



Fields:

Opcode: Operation code, request (1) or reply (2)

Htype: Hardware type (Ethernet, ...)

HLen: Length of hardware address

HCount: Maximum number of hops the packet can travel

Transaction ID: An integer set by client and repeated by the server

Time elapsed: The number of seconds since the client started to boot

Flags: First bit defines unicast (0) or multicast (1); other 15 bits not used

Client IP address: Set to 0 if the client does not know it

Your IP address: The client IP address sent by the server

Server IP address: A broadcast IP address if client does not know it

Gateway IP address: The address of default router

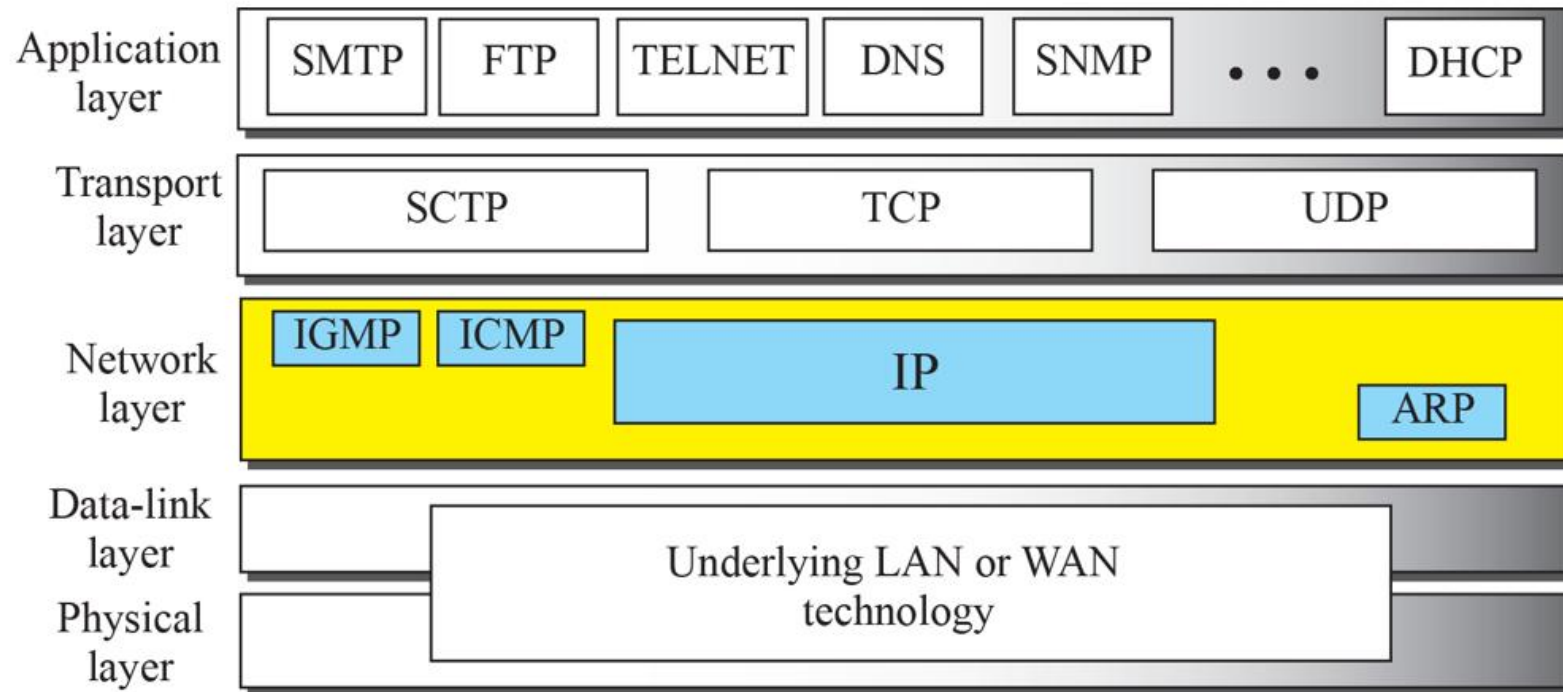
Server name: A 64-byte domain name of the server

Boot file name: A 128-byte file name holding extra information

Options: A 64-byte field with dual purpose described in text

Activate Windows
Go to Settings to activate Windows.

Figure 19.1: *Position of IP and other network-layer protocols in TCP/IP protocol suite*



Activate Windows
Go to Settings to activate Windows.

Figure 19.2: IP datagram

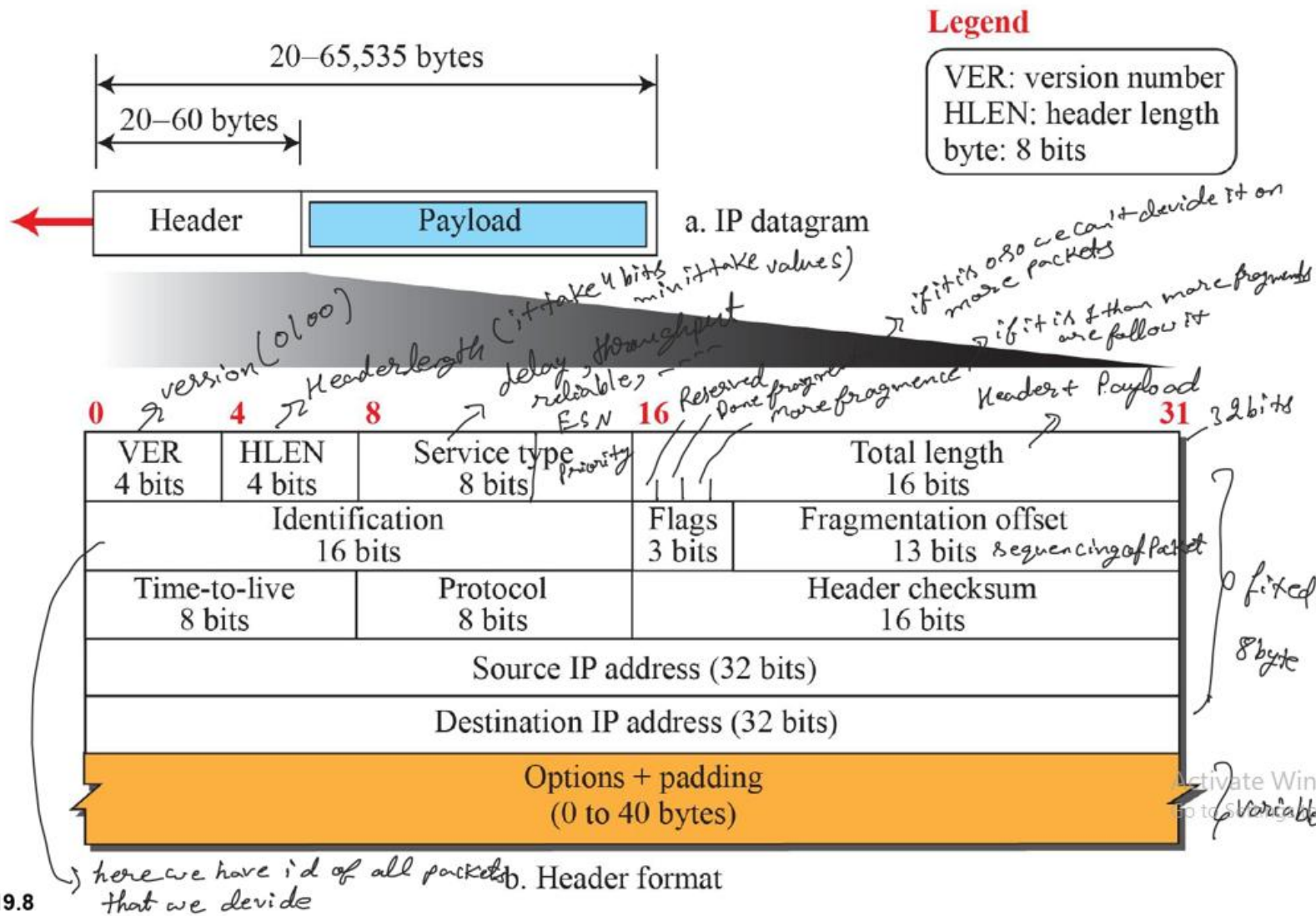
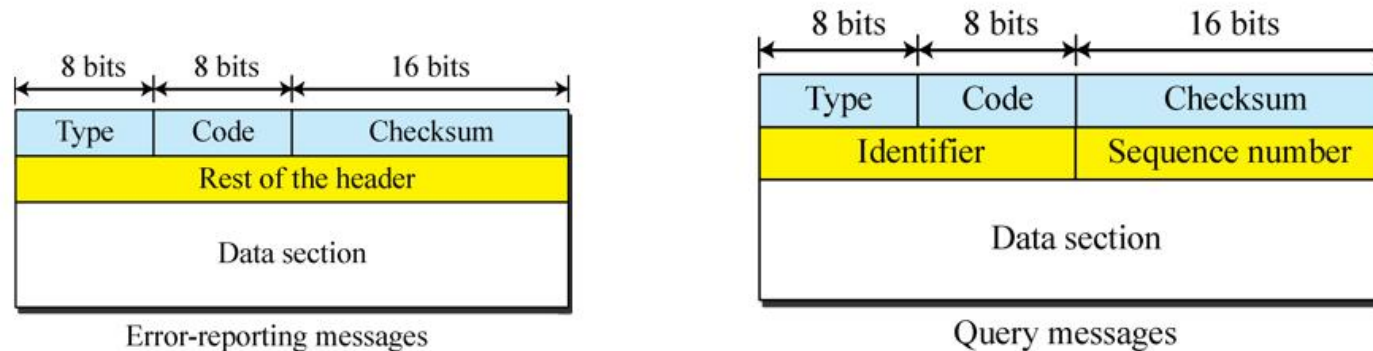


Figure 19.8: General format of ICMP messages



Type and code values

Error-reporting messages

- 03: Destination unreachable (codes 0 to 15)
- 04: Source quench (only code 0)
- 05: Redirection (codes 0 to 3)
- 11: Time exceeded (codes 0 and 1)
- 12: Parameter problem (codes 0 and 1)

Query messages

- 08 and 00: Echo request and reply (only code 0)
- 13 and 14: Timestamp request and reply (only code 0)

Note: See the book website for more explanation about the code values.

Activate Windows
Go to Settings to activate Windows.

Figure 19.14: *Agent advertisement*

ICMP Advertisement message			
Type	Length	Sequence number	
Lifetime		Code	Reserved
Care-of addresses (foreign agent only)			

Activate Windows
Go to Settings to activate Windows.

Figure 19.16: *Registration request format*

Type	Flag	Lifetime
Home address		
Home agent address		
Care-of address		
Identification		
Extensions ...		

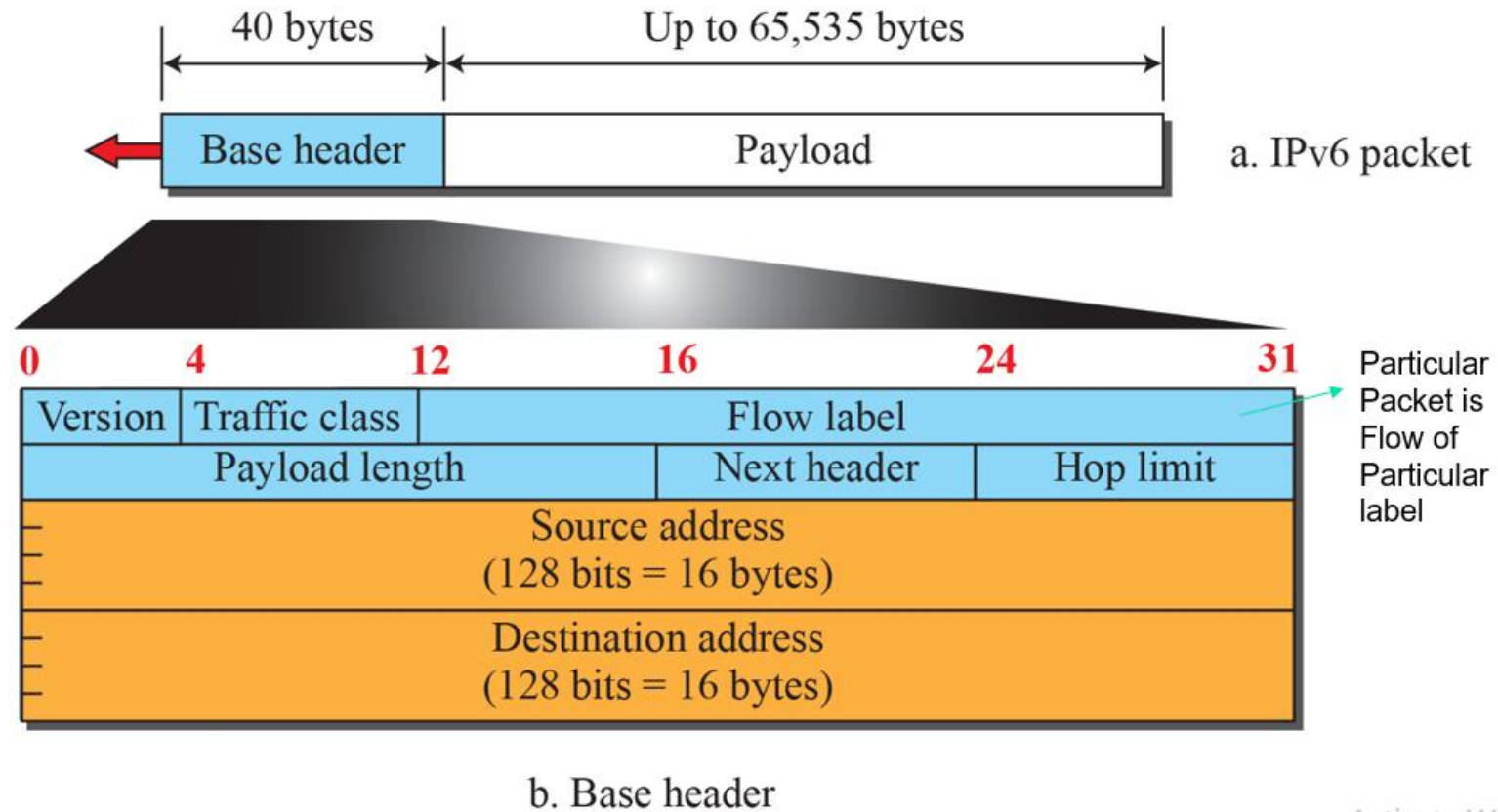
Activate Windows
Go to Settings to activate Windows.

Figure 19,17: Registration reply format

Type	Code	Lifetime
Home address		
Home agent address		
Identification		
Extensions ...		

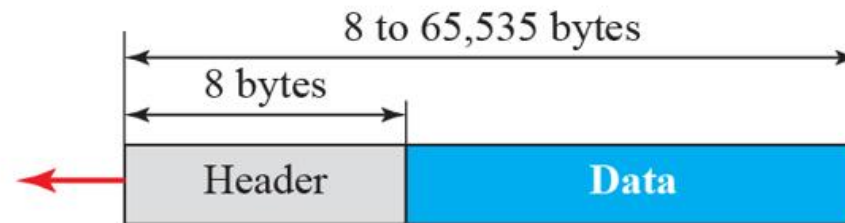
Activate Windows
Go to Settings to activate Windows.

Figure 22.6: IPv6 datagram

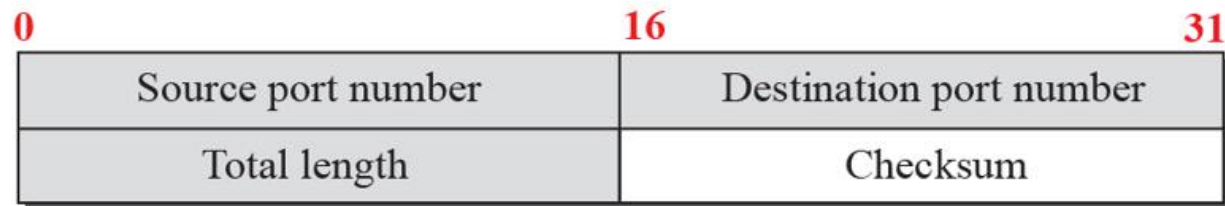


Activate Windows
Go to Settings to activate Windows.

Figure 24.2: *User datagram packet format*

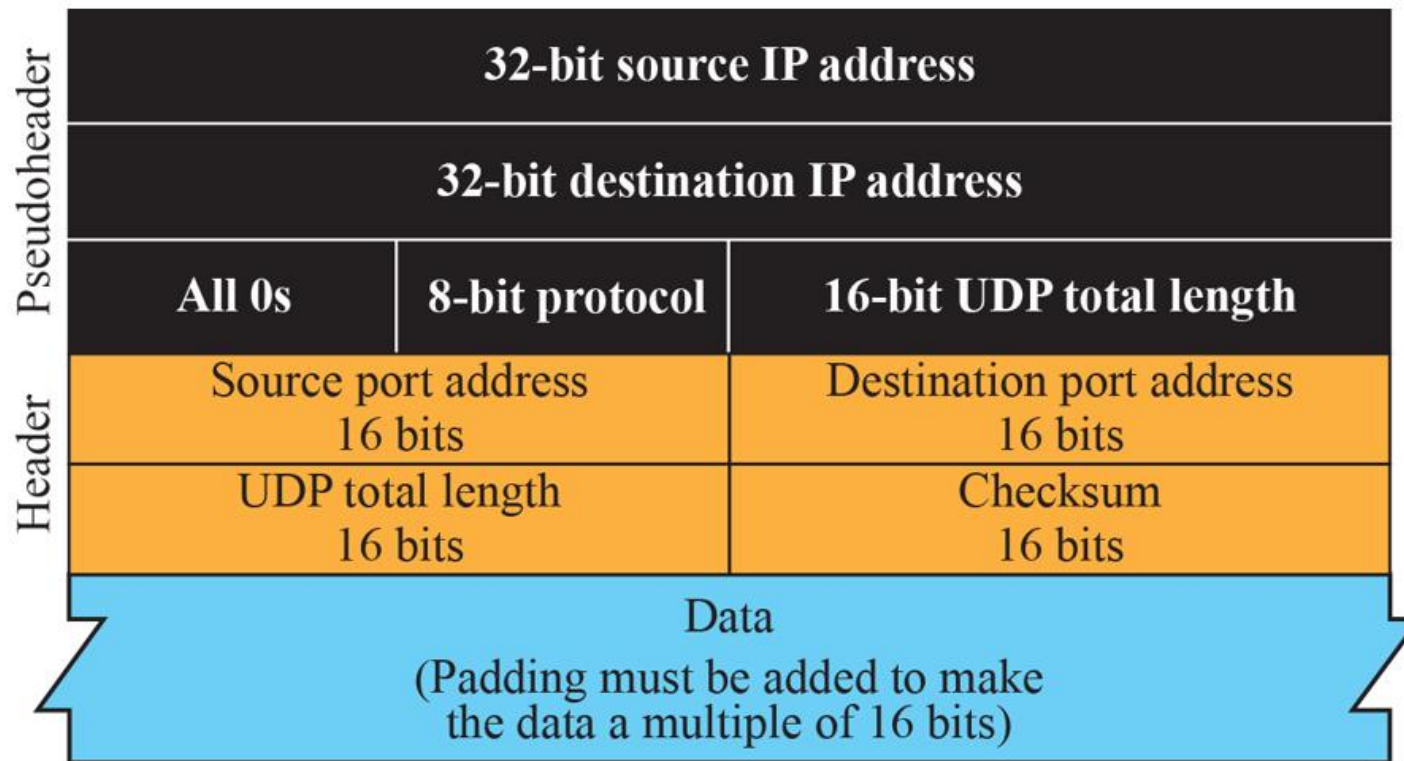


a. UDP user datagram



b. Header format

Figure 24.3: *Pseudoheader for checksum calculation*



Activate Windows
Go to Settings to activate Windows.

Figure 24.7: TCP segment format

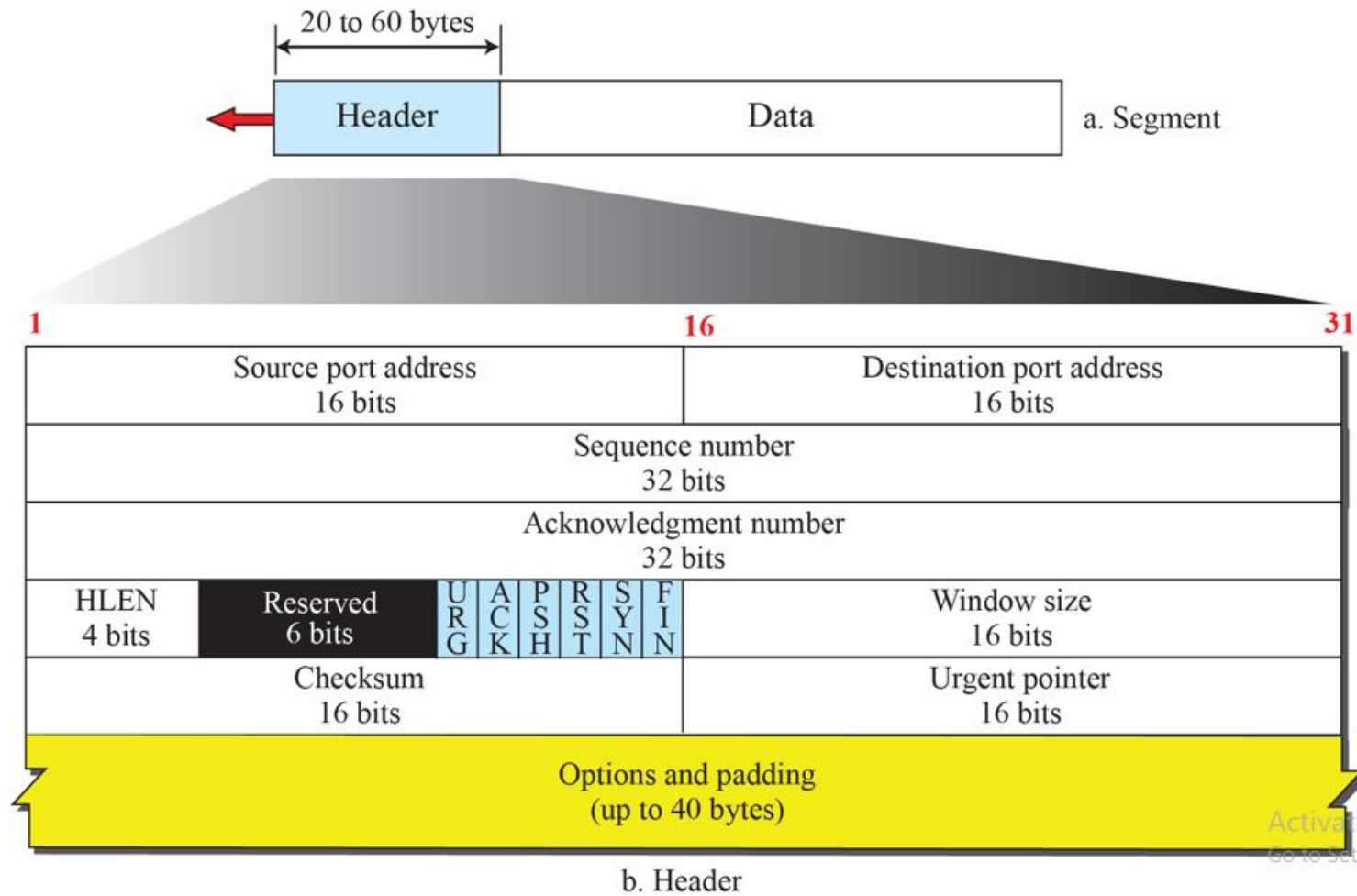
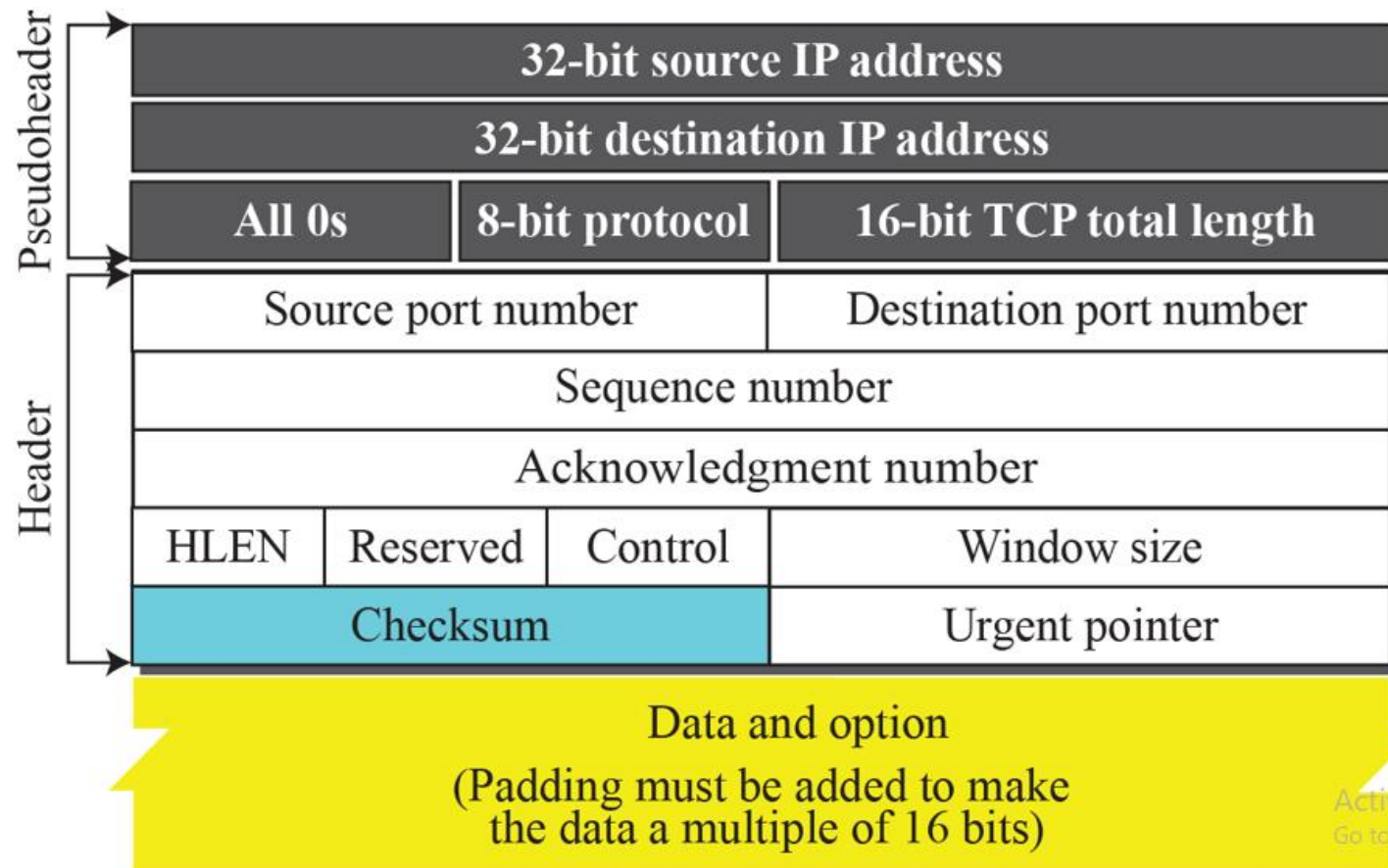
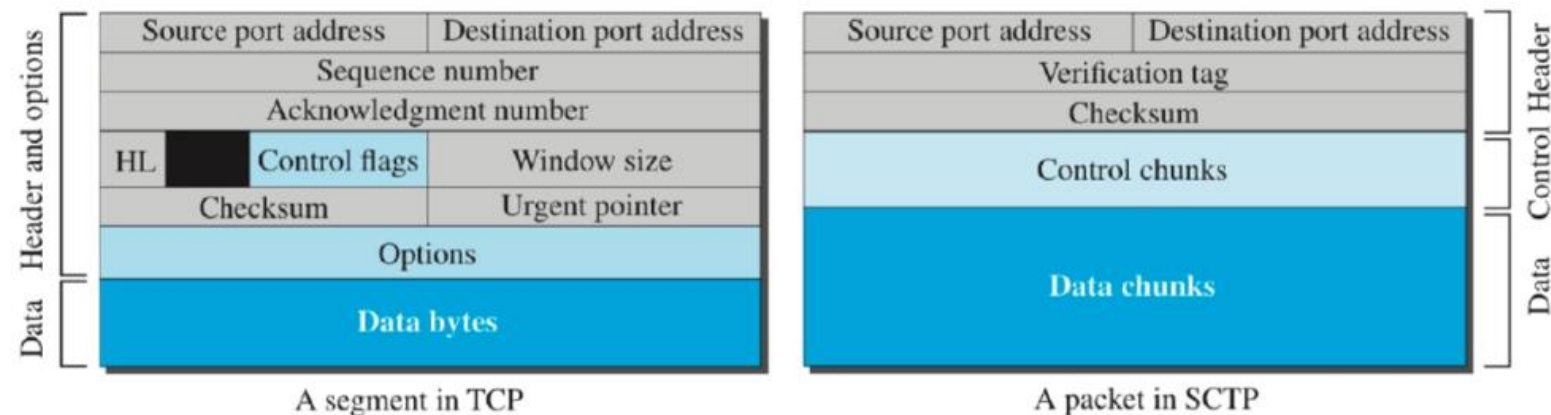


Figure 24.9: *Pseudoheader added to the TCP datagram*



In TCP, a segment carries data and control information. Data are carried as a collection of bytes; control information is defined by six control flags in the header. The design of SCTP is totally different: data are carried as data chunks, control information as control chunks. Several control chunks and data chunks can be packed together in a packet. A packet in SCTP plays the same role as a segment in TCP. Figure 24.40 compares a

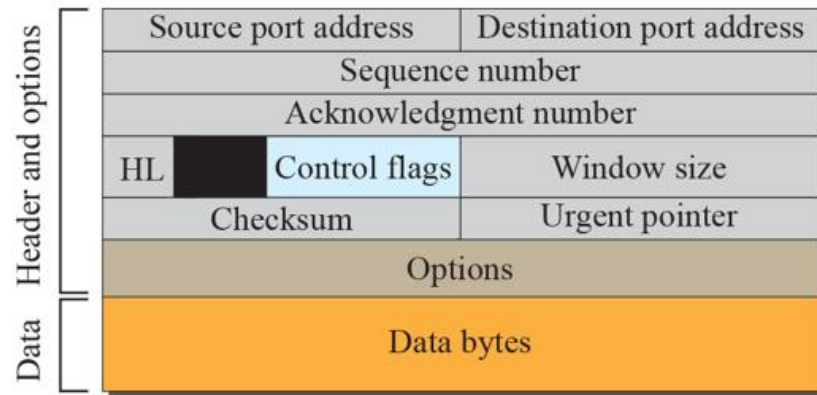
Figure 24.40 *Comparison between a TCP segment and an SCTP packet*



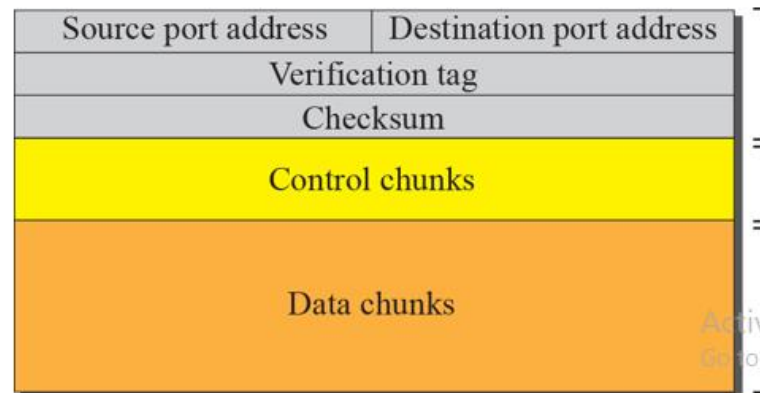
segment in TCP and a packet in SCTP. We will discuss the format of the SCTP packet in the next section.

In SCTP, we have data chunks, streams, and packets. An association may send many packets, a packet may contain several chunks, and chunks may belong to differ-

Figure 24.40 : *Comparison between a TCP segment and an SCTP packet*



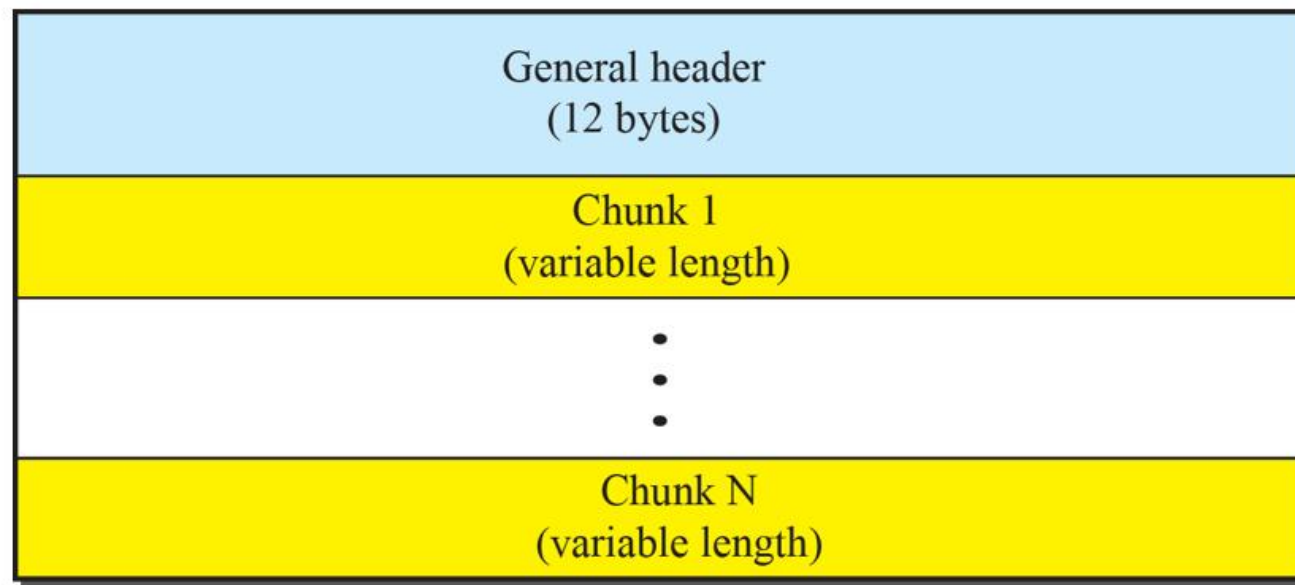
A segment in TCP



A packet in SCTP

Activate Windows
Go to Settings to activate Windows.

Figure 24.43 : SCTP packet format



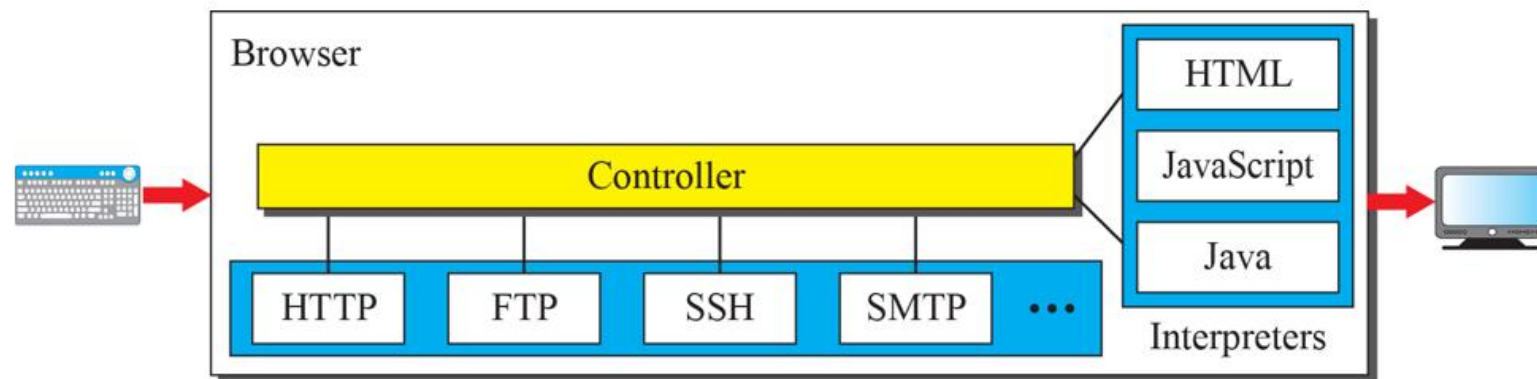
Activate Windows
Go to Settings to activate Windows.

Figure 8.50 : General header

Source port address 16 bits	Destination port address 16 bits
Verification tag 32 bits	
Checksum 32 bits	

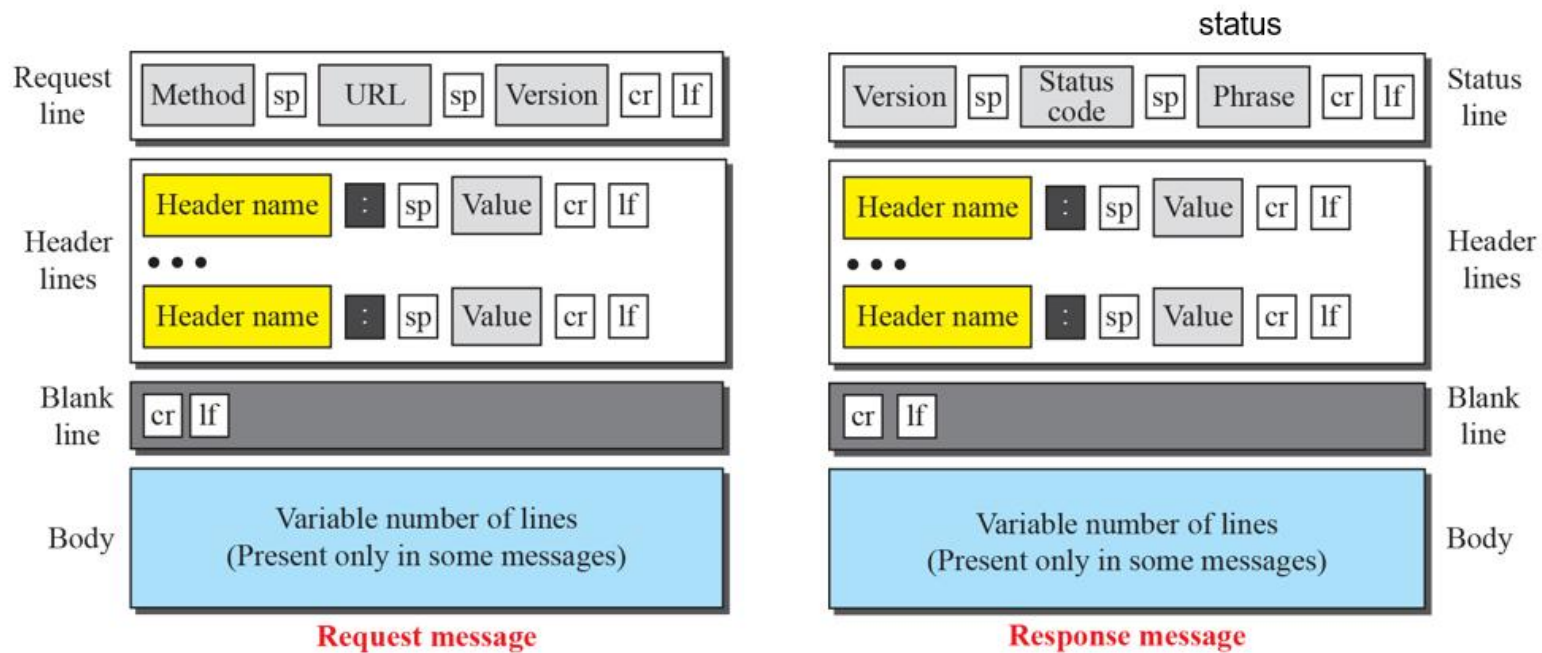
Activate Windows
Go to Settings to activate Windows.

Figure 26.2: Browser



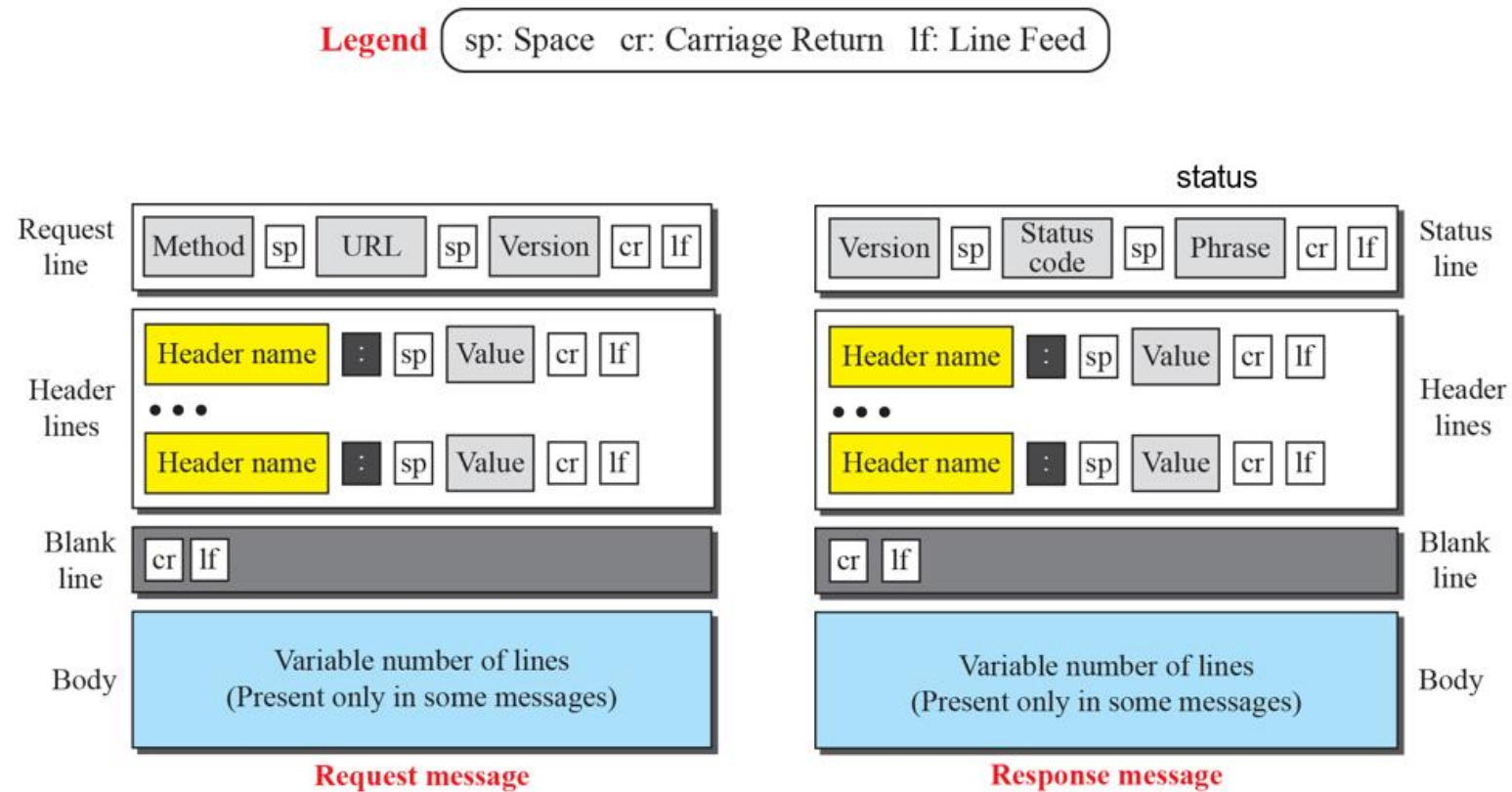
Activate Windows
Go to Settings to activate Windows.

Figure 26.5: *Formats of the request and response messages*



Activate Windows
Go to Settings to activate Windows.

Figure 26.5: *Formats of the request and response messages*



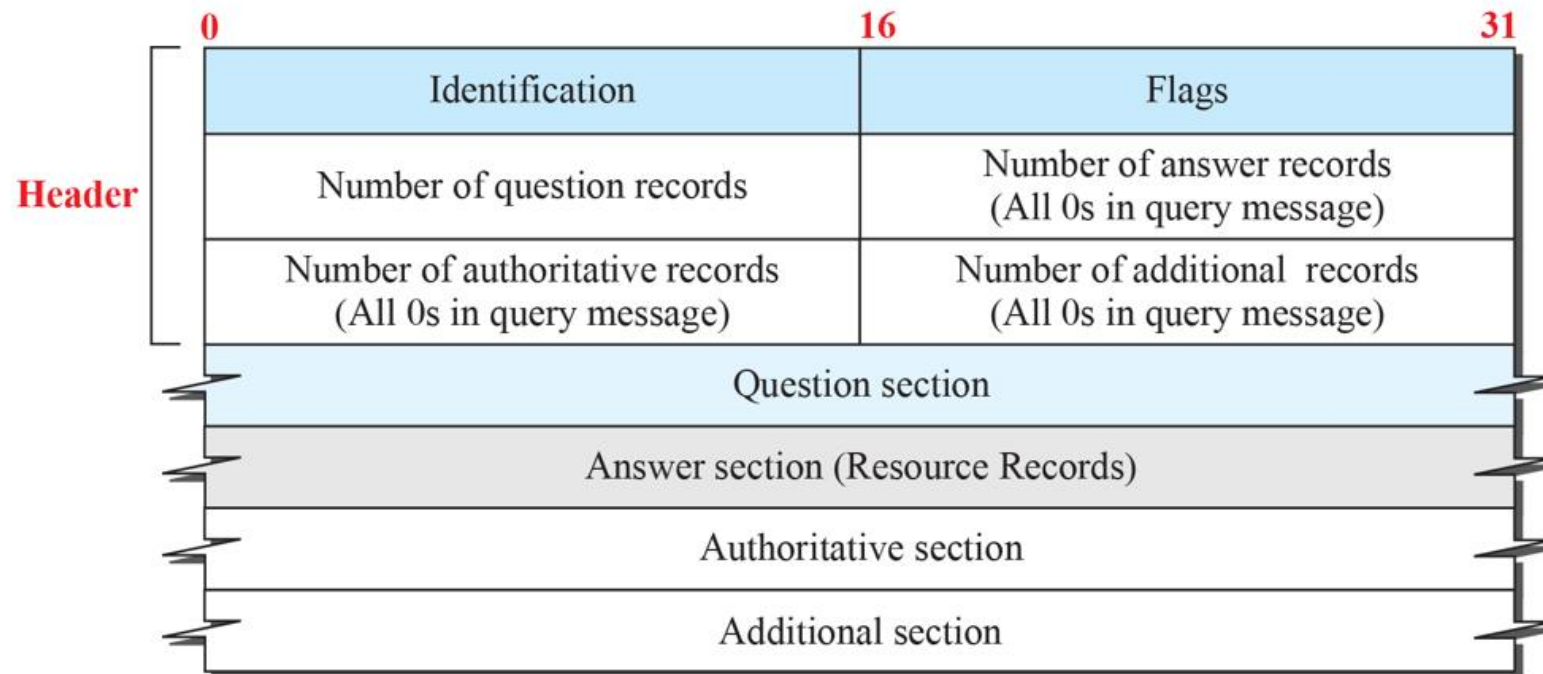
Activate Windows
Go to Settings to activate Windows.

Figure 26.27: SSH Packet Format



Activate Windows
Go to Settings to activate Windows.

Figure 26.38: DNS message



Note:

The query message contains only the question section. The response message includes the question section, the answer section, and possibly two other sections.

Activate Windows
Go to Settings to activate Windows.