
You may discuss these questions with your classmates, as it may be helpful to gain a good understanding of the topic. Nonetheless you should always submit your own work! Use a word processor to answer these questions, attach this questions page to your answers.

Question 1.

Depict the IP datagram format (Ipv4). Indicate each component and explain its purpose.

31	27	23	15	11	0
Version	IHL	Service Type	Total Length		
Sequence Number			Flags	Fragment Offset	
Hop Limit		Protocol	Header Checksum		
Source Address					
Destination Address					
Options and Padding					
Data Field (a multiple of bytes) Note: maximum total datagram length is 65,535 bytes.					

Version: The four-bit version of the IP. i.e. 4 for Ipv4.

IHL: It specifies the size of the header (this also coincides with the offset to the data)

Service Type: It specifies the service type to use for the current datagram, i.e. high priority, high reliability, normal delay, etc.

Total length: It defines the entire datagram size, including header and data, in bytes. The minimum-length datagram is 20 bytes and the maximum is 65,535, which is the maximum value of a 16-bit word.

Sequence number: It is used for identifying fragments of an original IP datagram with a unique sequence number. This field is also known as "Identification number".

Flags: Three bit-flags are used to control data fragmentation. This can be used when sending packets to a host that does not have sufficient resources to handle fragmentation.

Fragment offset: It is 13-bits long and specifies the offset of a particular fragment relative to the beginning of the original unfragmented IP datagram. It is measured in units of 8-byte blocks.

Hop limit: It indicates the amount of time the packet can "live" in the network. When the field hits zero, the packet is no longer forwarded by a packet switch and is discarded.

Protocol: It defines the protocol used in the data portion of the IP datagram.

Header checksum: It is used for error-checking of the header. At each hop, the checksum of the header must be compared to the value of this field. If a header checksum is found to be mismatched, then the packet is discarded.

Source address: This address is the address of the sender of the packet.

Destination address: This address is the address of the receiver of the packet.

Options: For additional options. In most cases this field is not used at all.

Data field: The contents of the data field are specified in the protocol header field and can be any one of the transport layer protocols.

Question 2.

Indicate the 5 classes of IP address formats in Ipv4. Explain the purpose of each of them.

Class A: Few networks, each with many hosts

0	Network	Host (24 bits)
---	---------	----------------

Class B: Medium number of hosts and networks

1 0	Network (14 bits)	Host (16 bits)
-----	-------------------	----------------

Class C: Many networks, each with few hosts

1 1 0	Network (21 bits)	Host (8 bits)
-------	-------------------	---------------

Class D: Intended for multicasting to all hosts in defined groups

1 1 1 0	Host Group Identifier (28 bits)
---------	---------------------------------

Class E: Reserved addresses

1 1 1 1	Address (28 bits)
---------	-------------------

Class A: Used when there are many hosts and few networks.

Class B: Used when there are relatively similar number of hosts and networks.

Class C: Used when there are many networks and fewer hosts.

Class D: Used when multicasting is used.

Class E: It is reserved for addresses only.

Question 3.

Depict the UDP segment format. Indicate each component and explain its purpose.

31		15	
Source Port		Destination Port	
Segment Length		Optional Segment Checksum	
Application Data			

Source port: It identifies the sending port when meaningful and should be assumed to be the port to reply to if needed.

Destination port: It identifies the destination port.

Segment length: It is a 16-bit field that specifies the length (in bytes) of the entire datagram including header and data. The minimum length is 8 bytes since that's the length of the header.

Option segment checksum: It is used for error-checking of the header and data.

Application data: It is the data being transmitted.

Question 4.

Within the context of the Hypertext Transfer Protocol (HTTP), describe the difference between safe and unsafe methods. Mention four safe methods. You may need to do some literature search.

Safe methods are intended only for information retrieval and should not change the state of the server. In other words, they should not modify the contents of the server. Unsafe methods should be displayed to the user in a special way, typically as buttons rather than links. For example deletion of a domain database record.

Some examples of safe methods are: HEAD, GET, OPTIONS, and TRACE.