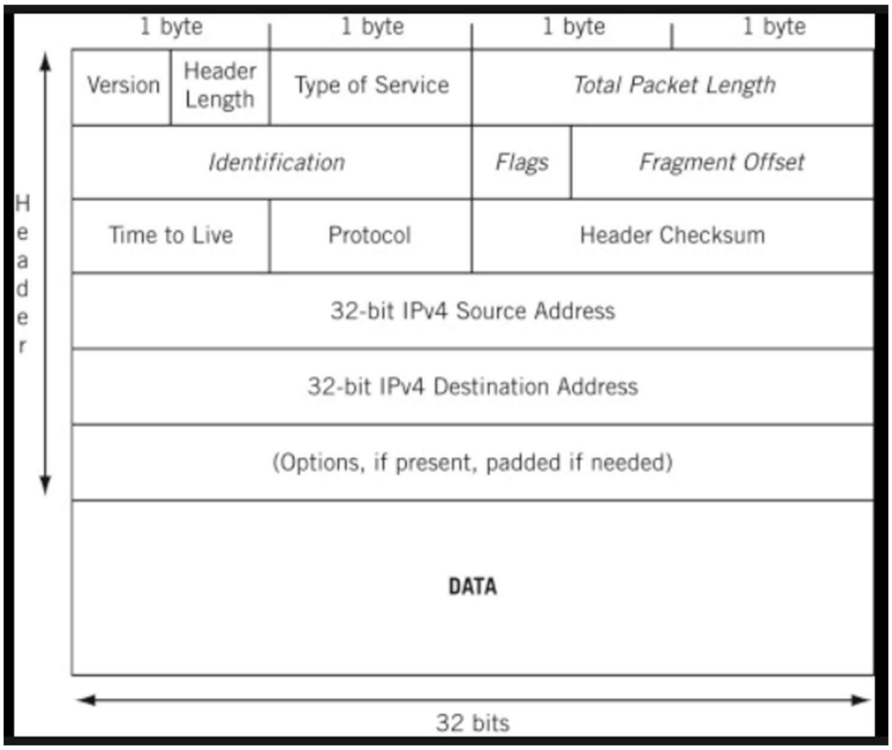
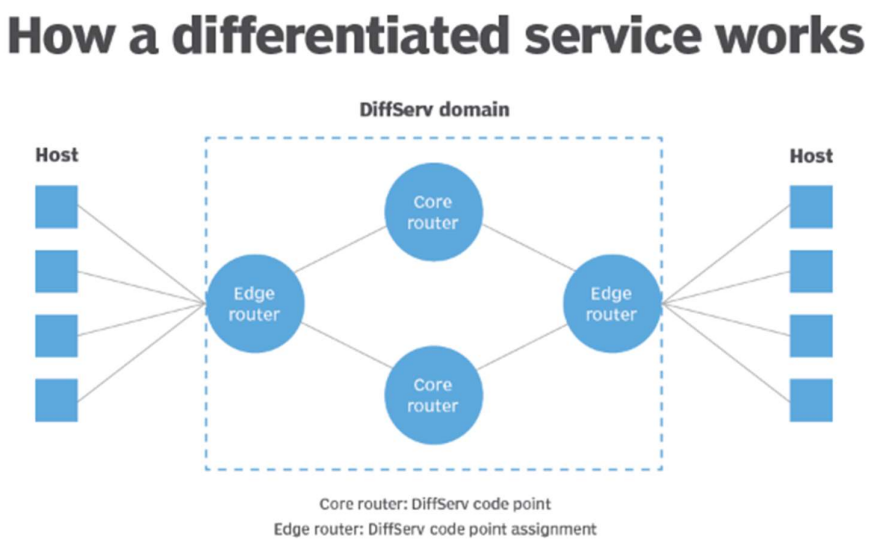
Header length-

Header Length—Technically, this is the Internet header length (IHL). It is the length of the IP header in 4-byte (32-bit) units known as “words,” and includes any option fields present and padding needed to align the header on a 32-bit boundary.



Differentiated Services Field

Differentiated services or DiffServ is a computer networking architecture that specifies a mechanism for classifying and managing network traffic and providing quality of service on modern IP networks.



Differentiated Services Codepoint

DSCP is a mechanism used for classifying network traffic on IP networks. It uses the 6-bit Differentiated Services Field (DS or DSCP field) in the IP header for packet classification purposes. Using Layer 3 classification enables you to maintain the same classification semantics beyond local network, across routers.

Explicit Congestion Notification

Explicit Congestion Notification (ECN) is a mechanism used in computer networks to manage congestion and prevent network congestion collapse. It is designed to improve the performance and efficiency of network traffic by providing explicit feedback about network congestion to the endpoints. ECN allows end-to-end notification of network congestion without dropping packets. ECN is an optional feature that may be used between two ECN-enabled endpoints when the underlying network infrastructure also supports it.

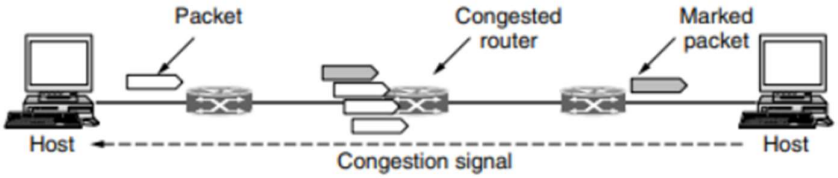


Figure 5-25. Explicit congestion notification

What does don't fragment mean?

If the Don't Fragment flag (DF) bit is set, then internet fragmentation of this datagram is NOT permitted, although it may be discarded. This can be used to prohibit fragmentation in cases where the receiving host does not have sufficient resources to reassemble internet fragments.

IP fragmentation is an Internet Protocol (IP) process that breaks packets into smaller pieces (fragments), so that the resulting pieces can pass through a link with a smaller maximum transmission unit (MTU) than the original packet size.

What is a fragment offset?

Fragment offset (13 bits) – use to identify the sequence of fragments in the frame. It generally indicates a number of data bytes preceding or ahead of the fragment.

MF	Fragment Offset	
1	0	→ 1st packet
1	!=0	→ Intermediate packet
0	!=0	→ Last packet
0	0	→ Invalid

Time-to-live (TTL)

is a value for the period of time that a packet, or data, should exist on a computer or network before being discarded.

How does header checksum work?

The checksum is calculated by the sender using a specific algorithm. It is then stored in the header and sent as part of the datastream. The receiving side calculates the checksum on the data that is received using the same algorithm as the sender and compares its value to the checksum passed in the header.

If the calculated checksum matches the one in the header, it indicates that the header has not been corrupted during transmission.

A checksum is a value that represents the number of bits in a transmission message and is used by IT professionals to detect high-level errors within data transmissions.

Source IP address - the IP packet field containing the IP address of the workstation from which it came.

Destination IP address - the IP packet field containing the IP address of the workstation to which it is addressed.