

# IP V4 Header Format

The IP Version 4 header is 20 bytes long and contains information that helps route packets across networks. This header is critical for network communication and is used by routers and other network devices to process and forward IP packets.

## IPv4 Header Format

bits	4	8	16	20	32
version	H. length	TOS	total length		
identification			flags	fragment offset	
Time to Live		protocol	header checksum		
32-bit source address					
32-bit destination address					
options					

Total length: 20 bytes + options

modified

deleted

# Version and Header Length

## Version

The first four bits indicate the IP version, which is 4 for IPv4.

## Header Length

The next four bits specify the header length in 32-bit words. The minimum header length is 5 words (20 bytes).



# Type of Service (ToS)

## Precedence

The first 3 bits are used for precedence and are prioritized by network routers.

## Delay

The next bit indicates whether a delay is acceptable for the packet.

## Throughput

The following bit denotes whether the packet requires a high throughput rate.

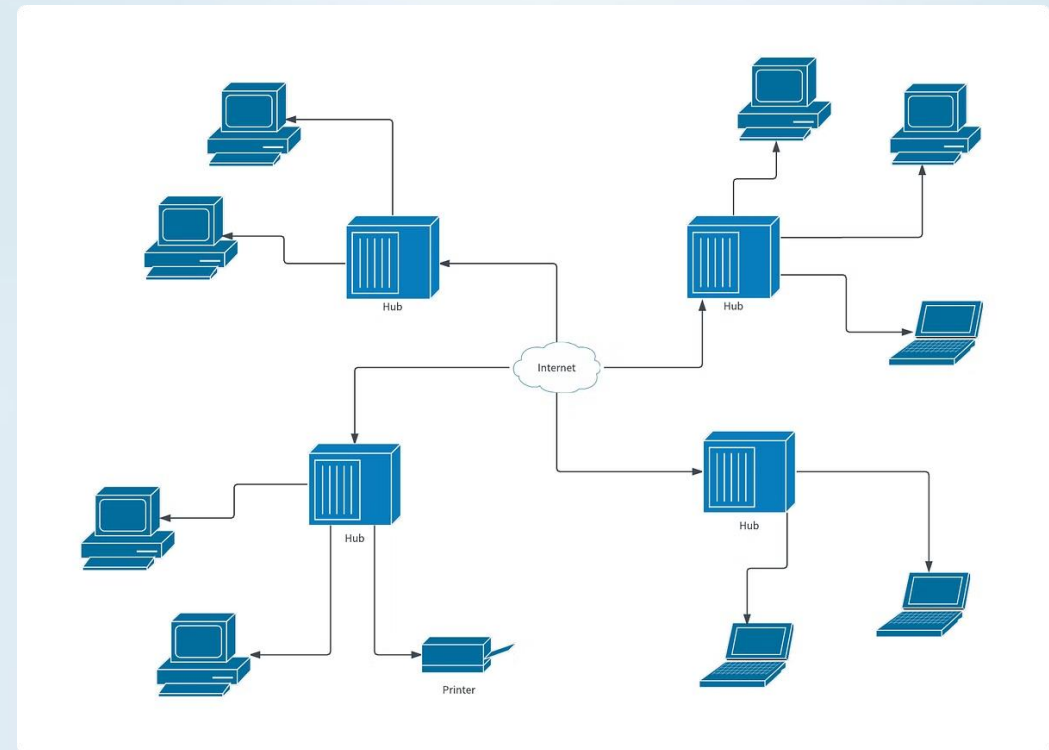
## Reliability

This bit determines whether the packet requires reliable delivery.

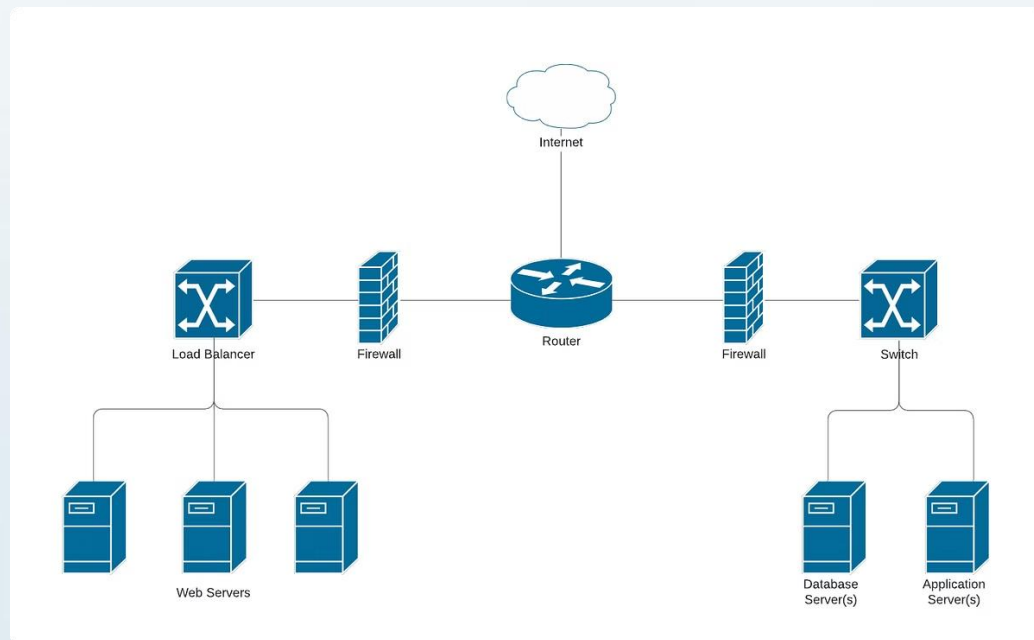
# Total Packet Length

## 1 Total Length

This 16-bit field indicates the total length of the IP packet, including both the header and the data.



# Identification, Flags, and Fragment Offset



1

## Identification

This field is used for fragmentation and reassembly.

2

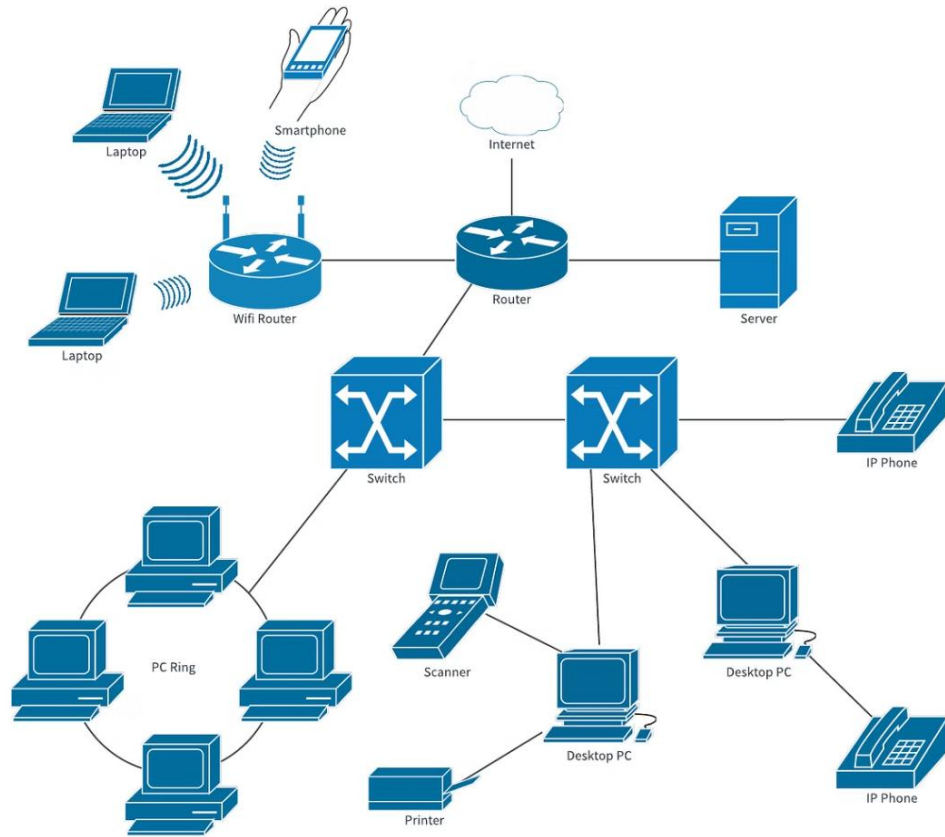
## Flags

The flags indicate whether the packet can be fragmented.

3

## Fragment Offset

This field indicates the position of the current fragment within the original packet.



# Time to Live (TTL) and Protocol

## Time to Live (TTL)

Specifies the maximum number of hops the packet can traverse before being discarded.

## Protocol

Identifies the upper layer protocol, such as TCP or UDP, that the data within the packet belongs to.

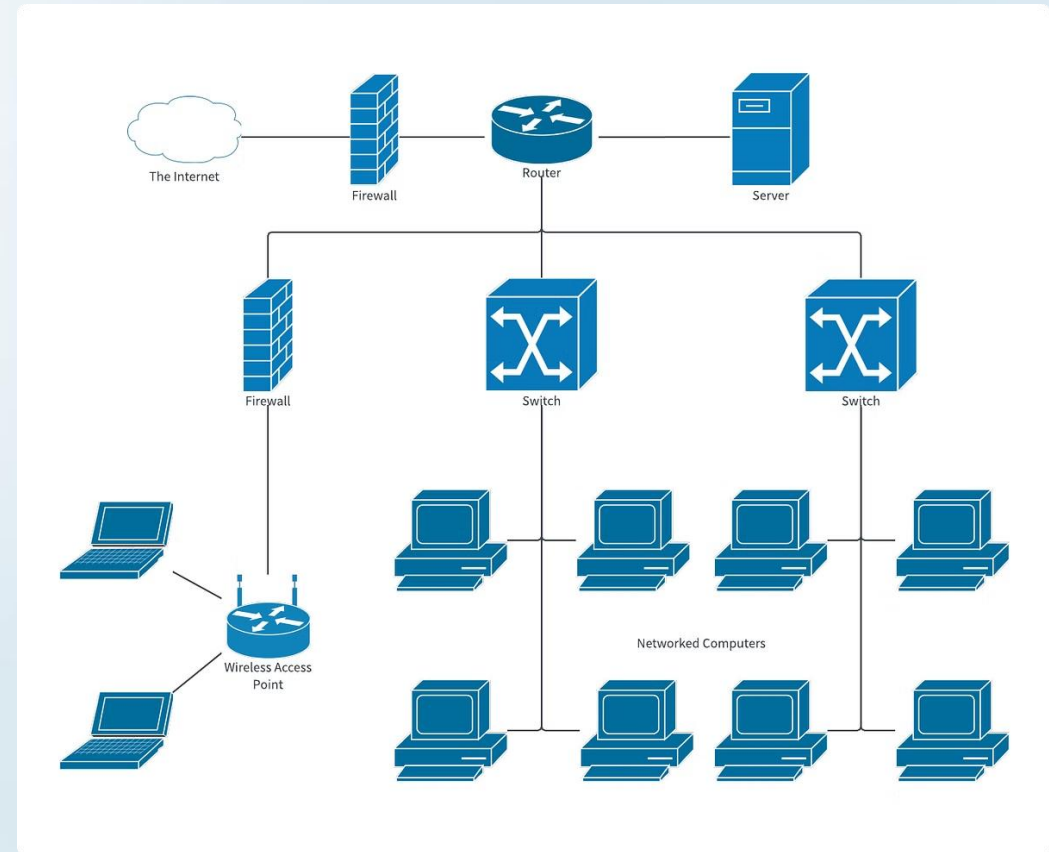
# Header Checksum

## 1 Checksum Calculation

The checksum is calculated across the header fields, ensuring data integrity during transmission.

## 2 Error Detection

Upon arrival, the checksum is recalculated to verify whether any data corruption has occurred during transit.



# Source and Destination IP Addresses



## Source IP Address

The IP address of the sending device, identifying the network interface from which the packet originated.



## Destination IP Address

The IP address of the receiving device, indicating the network interface where the packet is intended to arrive.

