IPv4 Packet

8.2.1

IPv4 Packet Header

IPv4 is one of the primary network layer communication protocols. The IPv4 packet header is used to ensure that this packet is delivered to its next stop on the way to its destination end device.

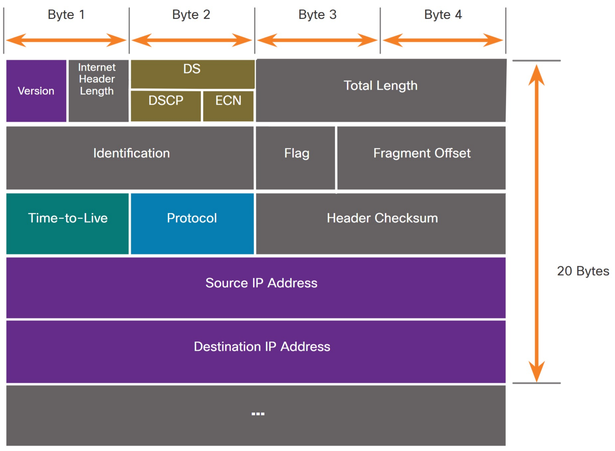
An IPv4 packet header consists of fields containing important information about the packet. These fields contain binary numbers which are examined by the Layer 3 process.

8.2.2

IPv4 Packet Header Fields

The binary values of each field identify various settings of the IP packet. Protocol header diagrams, which are read left to right, and top down, provide a visual to refer to when discussing protocol fields. The IP protocol header diagram in the figure identifies the fields of an IPv4 packet.

Fields in the IPv4 Packet Header



Significant fields in the IPv4 header include the following:

- **Version –** Contains a 4-bit binary value set to 0100 that identifies this as an IPv4 packet.
- **Differentiated Services or DiffServ (DS) –** Formerly called the type of service (ToS) field, the DS field is an 8-bit field used to determine the priority of each packet. The six most significant bits of the DiffServ field are the differentiated services code point (DSCP) bits and the last two bits are the explicit congestion notification (ECN) bits.
- **Time to Live (TTL) –** TTL contains an 8-bit binary value that is used to limit the lifetime of a packet. The source device of the IPv4 packet sets the initial TTL value. It is decreased by one each time the packet is processed by a router. If the TTL field decrements to zero, the router discards the packet and sends an Internet Control Message Protocol (ICMP) Time Exceeded message to the source IP address. Because the router decrements the TTL of each packet, the router must also recalculate the Header Checksum.
- **Protocol –** This field is used to identify the next level protocol. This 8-bit binary value indicates the data payload type that the packet is carrying, which enables the network layer to pass the data to the appropriate upper-layer protocol. Common values include ICMP (1), TCP (6), and UDP (17).
- **Header Checksum –** This is used to detect corruption in the IPv4 header.
- **Source IPv4 Address –** This contains a 32-bit binary value that represents the source IPv4 address of the packet. The source IPv4 address is always a unicast address.
- **Destination IPv4 Address –** This contains a 32-bit binary value that represents the destination IPv4 address of the packet. The destination IPv4 address is a unicast, multicast, or broadcast address.

The two most commonly referenced fields are the source and destination IP addresses. These fields identify where the packet is coming from and where it is going. Typically, these addresses do not change while travelling from the source to the destination.

The Internet Header Length (IHL), Total Length, and Header Checksum fields are used to identify and validate the packet.

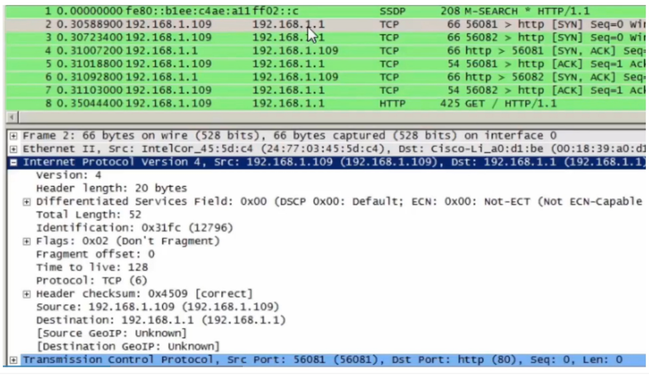
Other fields are used to reorder a fragmented packet. Specifically, the IPv4 packet uses Identification, Flags, and Fragment Offset fields to keep track of the fragments. A router may have to fragment an IPv4 packet when forwarding it from one medium to another with a smaller MTU.

The Options and Padding fields are rarely used and are beyond the scope of this module.

8.2.3

Video - Sample IPv4 Headers in Wireshark

Click Play in the figure to view a demonstration of examining IPv4 headers in a Wireshark capture.



8.2.4

Check Your Understanding - IPv4 Packet

Check your understanding of the IPv4 packet by choosing the correct answer to the following questions.

1. What are the two most commonly referenced fields in an IPv4 packet header that indicate where the packet is coming from and where it is going? (Choose two.)

- [x] destination IP address
- [ ] protocol
- [ ] Time to Live
- [x] source IP address
- [ ] Differentiated Services (DS)

2. Which statement is correct about IPv4 packet header fields?

- (•) The source and destination IPv4 addresses remain the same while travelling from source to destination.
- ( ) The Time to Live field is used to determine the priority of each packet.
- ( ) The Total Length and Header Checksum fields are used to reorder a fragmented packet.
- ( ) The Version field identifies the next level protocol.

3. Which field is used to detect corruption in the IPv4 header?

- (•) Header Checksum
- ( ) Time to Live
- ( ) Protocol
- ( ) Differentiated Services (DS)

4. Which field includes common values such as ICMP (1), TCP (6), and UDP (17)?

- ( ) Header Checksum
- ( ) Time to Live
- (•) Protocol
- ( ) Differentiated Services (DS)

Check

Show Me

Reset