APPENDIX C

Packet Header Formats

Snort rules use the protocol type field to distinguish among different protocols. Different header parts in packets are used to determine the type of protocol used in a packet. In addition, rule options can test many of the header fields. This appendix explains headers of different protocols. These packet headers are explained in detail in RFCs. Understanding different parts of these packet headers is very important for writing effective Snort rules.

IP Packet Header

The basic IPv4 header consists of 20 bytes. An options part may be present after these 20 bytes. This optional part may be up to forty bytes long. Structure of IP header is present in Figure C-1.

<table>
<tr><td>V</td><td>IHL</td><td>TOS</td><td colspan="2">Total Length</td></tr>
<tr><td colspan="3">ID</td><td>F</td><td>Frag Offset</td></tr>
<tr><td colspan="2">TTL</td><td>Protocol</td><td colspan="2">Header Checksum</td></tr>
<tr><td colspan="5">Source Address</td></tr>
<tr><td colspan="5">Destination Address</td></tr>
</table>

Figure C-1 IP header

Detailed information about the IP packet header can be found in RFC 791 which is available from ftp://ftp.isi.edu/in-notes/rfc791.txt and many other places including the RFC editor web site. A brief explanation of different fields in the IP packet header is found in Table C-1.

Table C-1 IP Packet Header Fields

Field	Explanation
V	Version number. The value is 4 for IPv4. Four bits are used for this part.
IHL	This field shows length of IP packet header. This is used to find out if the options part is present after the basic header. Four bits are used for IHL and it shows length in 32-bit word length. The value of this field for a basic 20-bytes header is 5.
TOS	This field shows type of service used for this packet. It is 8 bits in length.
Total Length	This field shows the length of the IP packet, including the data part. It is 16 bits long.
ID	This field packet identification number. This part is 16 bits long.
F	This part is three bits long and it shows different flags used in the IP header.
Frag Offset	This part is thirteen bits long and it shows fragment offset in case an IP packet is fragmented.
TTL	This is time to live value. It is eight bits long.
Protocol	This part shows transport layer protocol number. It is eight bits long.
Header Checksum	This part shows header checksum, which is used to detect any error in the IP header. This part is sixteen bits long.
Source Address	This is the 32 bit long source IP address.
Destination Address	This is the 32 bit long destination IP address.

ICMP Packet Header

ICMP header is completely explained in RFC 792, which is available from ftp://ftp.isi.edu/in-notes/rfc792.txt for download. Figure C-2 shows basic structure of ICMP header. Note that depending upon type of ICMP packet, this basic header is followed by different parts.

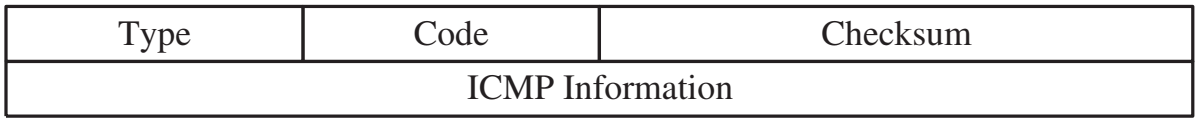

Figure C-2 Basic ICMP header

An explanation of the fields in a basic ICMP header is provided in Table C-2.

Table C-2 ICMP Packet Header Fields

Field	Explanation
Type	This part is 8 bits long and shows the type of ICMP packet.
Code	This part is also 8 bits long and shows the sub-type or code number used for the packet.
Checksum	This part is 16 bits long and is used to detect any errors in the ICMP packet.

The ICMP information part is variable depending upon the value of the type field. For example, the ping command uses ICMP ECHO REQUEST type packet. This packet header is shown in Figure C-3.

Figure C-3 ICMP packet used in ping command.

For a complete list of ICMP packet types, refer to RFC 792.

TCP Packet Header

TCP packet header is discussed in detail in RFC 793 which is available at ftp://ftp.isi.edu/in-notes/rfc793.txt for download. Figure C-4 shows structure of TCP header.

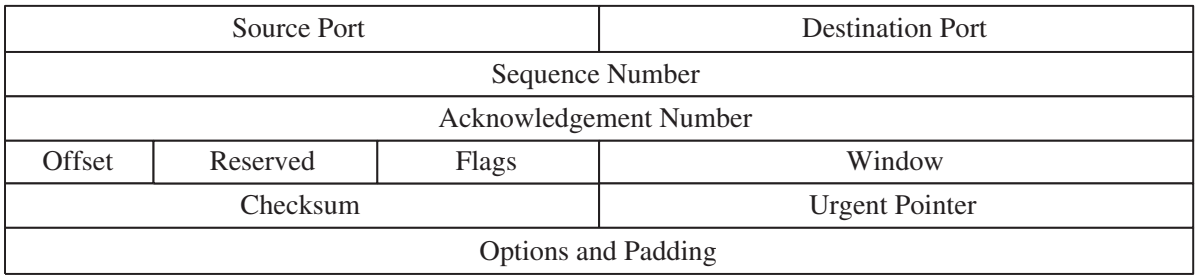

Figure C-4 TCP header

Different parts of TCP header are explained in Table C-3. Again for a detailed explanation of TCP, refer to the RFC 793.

Table C-3 TCP Packet Header Fields

Field	Explanation
Source Port	This part is 16 bits long and shows source port number.
Destination Port	This is a 16-bit long field and shows the destination port number.
Sequence Number	This is the sequence number for the TCP packet. It is 32 bits long. It shows the sequence number of the first data octet in the packet. However if SYN bit is set, this number shows the initial sequence number.
Acknowledgement Number	This number is used for acknowledging packets. It is 32 bits long. This number shows the sequence number of the octet that the sender is expecting.
Offset	This is a 4- bit field and shows the length of the TCP header. Length is measured in 32-bit numbers.
Reserved	Six bits are reserved.
Flags or Control bits	The flags are six bits in length and are used for control purposes. These bits are URG, ACK, PSH, RST, SYN and FIN. A value of 1 in any bit place indicates the flag is set.
Window	This is 16 bits long and is used to tell the other side about the length of TCP window size.

Table C-3 TCP Packet Header Fields (continued)

Field	Explanation
Checksum	This is a checksum for TCP header and data. It is 16 bits long.
Urgent Pointer	This field is used only when the URG flag is set. It is 16 bits long.
Options	This part is of variable length.

UDP Packet Header

The UDP packet header is simple and is described in RFC 768. It has four fields as shown in Figure C-5. Each field is 16 bits long. Names of all fields are self-explanatory.

Source Port	Destination Port
Length	Checksum

Figure C-5 UDP packet header

ARP Packet Header

ARP packets are used to discover the hardware or MAC addresses when the IP address is known. In any LAN, you will see a lot of ARP packets being transmitted. This is because each host has to find out the MAC address of the destination host before sending data. The ARP is a broadcast protocol and its packet header is shown in Figure C-6.

<table>
<tr><td colspan="2">HW Address Type</td><td>Protocol Address Type</td></tr>
<tr><td>HW Addr Len</td><td>Proto Addr Len</td><td>Operation</td></tr>
<tr><td colspan="3">Source Hardware Address</td></tr>
<tr><td colspan="2">Source Hardware Address (Continued)</td><td>Source Protocol Address</td></tr>
<tr><td colspan="2">Source Protocol Address (Continued)</td><td>Target Hardware Address</td></tr>
<tr><td colspan="3">Target Hardware Address (Continued)</td></tr>
<tr><td colspan="3">Target Protocol Address</td></tr>
</table>

Figure C-6 ARP header

Different fields in the ARP packet header are described in Table C-4.

Table C-4 ARP Packet Header Fields

Field	Explanation
HW Address Type	The HW Address type is a 16 bit long field and it shows the type of hardware. Since most of LANs are Ethernet-based, its value is 1. For IEEE 802 networks, its value is 6. For IPSec tunnel, the value is 31.
Protocol Address Type	The protocol address type shows the protocol used in the network layer. The value of this field is 0x800 for IP.
HW Addr Len	This field shows the length of the hardware address in number of bytes. This field is 8 bits long.
Proto Addr Length	This field shows the length of the protocol address. This field is also 8 bits long.
Operation or Opcode	This field is 16 bits long and is used for the type of ARP packet. A value of 1 indicates a request packet and a value of 2 indicates a reply packet.
Source hardware address	This is a 48 bit long field in the case of Ethernet. However its length is variable.
Source protocol address	This is a 32 bit field in the case of IPv4 packets. However its length is variable.
Target hardware address	This is 48 bits long in Ethernet and its length is variable.
Target protocol address	This is 32 bits in the case of IPv4 and its length is variable.