

## UDP Header

|   |             |   |                  |   |
|---|-------------|---|------------------|---|
|   | 0           | 1 | 2                | 3 |
| 0 | Source Port |   | Destination Port |   |
|   |             |   |                  |   |
| 4 | Length      |   | Checksum         |   |
|   |             |   |                  |   |

### Common UDP Ports

|     |         |     |            |      |         |
|-----|---------|-----|------------|------|---------|
| 7   | echo    | 137 | netbios-ns | 546  | DHCPv6c |
| 19  | chargen | 138 | netbios    | 547  | DHCPv6s |
| 53  | domain  | 161 | snmp       | 1900 | SSDP    |
| 67  | DHCPs   | 162 | snmp-trap  | 5353 | mDNS    |
| 68  | DHCPc   | 500 | isakmp     |      |         |
| 69  | tftp    | 514 | syslog     |      |         |
| 123 | ntp     | 520 | Rip        |      |         |

Length: number of bytes including UDP header.

Minimum value is 8

Checksum includes pseudo-header (IPs, length, protocol), UDP header and payload.

## ARP

|    |                         |                |                   |   |
|----|-------------------------|----------------|-------------------|---|
|    | 0                       | 1              | 2                 | 3 |
| 0  | HW Addr. Type           |                | Prot. Addr. Type  |   |
| 4  | HW Addr Len.            | Prot. Addr Len | Opcode            |   |
| 8  | Source Hardware Addr.   |                |                   |   |
| 12 | Src HW Addr             |                | Src Protocol Addr |   |
| 16 | Src. Proto Addr         |                | Tgt HW Addr       |   |
| 20 | Tgt HW Address (cont.)  |                |                   |   |
| 24 | Target Protocol Address |                |                   |   |

Hardware Type: 1 - Ethernet

Protocol Type: 0x0800 - IPv4

Address Length: 4=IPv4, 6=Ethernet

Opcode: 1-request, 2-response



The best. Made better.

The SANS Technology Institute develops leaders to strengthen enterprise and global information security. STI educates managers and engineers in information security practices and techniques, attracts top scholar-practitioners as faculty, and engages both students and faculty in real-world applied research.

Learn more at <https://www.sans.edu>



A collaborative network security community. Learn about current issues, correlate your logs with others, free API and other resources to enhance your understanding of current threats. <https://isc.sans.edu>



## TCP/IP and tcpdump

Version January 2019

### POCKET REFERENCE GUIDE

Please submit comments and corrections to [jullrich@sans.edu](mailto:jullrich@sans.edu)  
<https://www.sans.org/security-resources/tcpip.pdf>

### COURSES & GIAC CERTIFICATIONS

**SEC503**  
Intrusion Detection In-Depth



SEC 401  
Security Essentials



SEC 573  
Automating with Python



SEC 560  
Network Penetration Testing



SEC 546  
IPv6 Security Essentials



FOR 572  
Network Forensics



MGT512  
Security Leadership Essentials



## tcpdump usage

```
tcpdump [-aAenStvxX] [-F filterfile] [-i int] [-c n]
[-r pcapfile] [-s snaplen] [-w pcapfile] ['bpf filter']
-A      display payload
-c n    display first n packets
-D      list interfaces
-e      display data link header
-F      read filter expression from file
-i      listen on specified interface
-n      do not resolve IP addresses / ports
-r      read packets from file
-s      set snap length in bytes
-S      display absolute TCP sequence numbers
-t      do not print timestamp
-tttt  print date and time
-v      verbose (multiple v: more verbose)
-w      write packets to file
-x      display in hex
-xx     display link layer in hex
-X      display in hex + ASCII
```

## Acronyms

|        |   |
|--------|---|
| AH     | Authentication Header (RFC 2402)                  |
| ARP    | Address Resolution Protocol (RFC 826)             |
| BGP    | Border Gateway Protocol (RFC 1771)                |
| CWR    | Congestion Window Reduced (RFC 2481)              |
| DF     | Do not fragment flag (RFC 791)                    |
| DHCP   | Dynamic Host Configuration Protocol (RFC 2131)    |
| DNS    | Domain Name System (RFC 1035)                     |
| ECN    | Explicit Congestion Notification (RFC 3168)       |
| ESP    | Encapsulating Security Payload (RFC 2406)         |
| FTP    | File Transfer Protocol (RFC 959)                  |
| GRE    | Generic Route Encapsulation (RFC 2784)            |
| HTTP   | Hypertext Transfer Protocol (RFC 1945)            |
| ICMP   | Internet Control Message Protocol (RFC 792)       |
| IGMP   | Internet Group Management Protocol (RFC 2236)     |
| IMAP   | Internet Message Access Protocol (RFC 2060)       |
| IP     | Internet Protocol (RFC 791)                       |
| ISAKMP | Internet Sec. Assoc. & Key Mngm Proto. (RFC 7296) |
| L2TP   | Layer 2 Tunneling Protocol (RFC 2661)             |
| OSPF   | Open Shortest Path First (RFC 1583)               |
| POP3   | Post Office Protocol v3 (RFC 1460)                |
| RFC    | Request for Comments                              |
| SMTP   | Simple Mail Transfer Protocol (RFC 821)           |
| SSH    | Secure Shell (RFC 4253)                           |
| SSL    | Secure Sockets Layer (RFC 6101)                   |
| TCP    | Transmission Control Protocol (RFC793)            |
| TLS    | Transport Layer Security (RFC 5246)               |
| TFTP   | Trivial File Transfer Protocol (RFC 1350)         |
| TOS    | Type of Service (RFC 2474)                        |
| UDP    | User Datagram Protocol (RFC 768)                  |

## DNS

|    |   |   |                   |   |
|----|---|---|-------------------|---|
|    | 0   | 1 | 2                 | 3 |
| 0  | Query ID  |   | Flags (see below) |   |
| 4  | Query Count   |   | Answer Count      |   |
| 8  | Authority Rec. #  |   | Addtl. Record #   |   |
| 12 | Questions...<br>Answers...<br>Authority Records...<br>Additional Records... |   |                   |   |

Flags:

| Byte Offset 2 |        |   |   | Byte Offset 3 |   |   |   |   |   |   |   |       |   |   |   |
|---------------|--------|---|---|---------------|---|---|---|---|---|---|---|-------|---|---|---|
| 0             | 1      | 2 | 3 | 4             | 5 | 6 | 7 | 0 | 1 | 2 | 3 | 4     | 5 | 6 | 7 |
| Q             | OPCODE |   |   | A             | T | R | R | Z | A | C | D | RCODE |   |   |   |
| R             |        |   |   | A             | C | D | A | Z | D | D |   |       |   |   |   |

QR: Query (0) or Response (1)  
 Opcode: 0 – Query, 1 Inverse Query, 2 Status, 4 Notify, 5 Update  
 AA: Authoritative Answer  
 TC: Truncated response  
 RD: Recursion Desired  
 RA: Recursion Available  
 Z: Zero (set to 0)  
 AD: Authentic Data (DNSSEC)  
 CD: Checking Disabled (DNSSEC)

RCODE:  
 0 – No error  
 1 – Format Error  
 2 – Server Failure  
 3 – Non-existent domain (NXDOMAIN)  
 4 – Query type not implemented  
 5 – Query refused

## ICMP

|   |   |      |          |   |
|---|---|------|----------|---|
|   | 0   | 1    | 2        | 3 |
| 0 | Type                                      | Code | Checksum |   |
| 4 | Addtl. information depending on type/code |      |          |   |

| Type | Code | Name  |
|------|------|---|
| 0    | 0    | Echo Reply                                  |
| 3    | 0    | Network Unreachable                         |
|      | 1    | Host Unreachable                            |
|      | 2    | Protocol Unreachable                        |
|      | 3    | Port Unreachable                            |
|      | 4    | Fragmentation Required                      |
|      | 5    | Source Route Failed                         |
|      | 6    | Dest. Network Unknown                       |
|      | 7    | Destination Host Unknown                    |
|      | 8    | Source Host Isolated                        |
|      | 9    | Net Administratively Prohibited             |
|      | 10   | Host Administratively Prohibited            |
|      | 11   | Network unreachable for TOS                 |
|      | 12   | Host unreachable for TOS                    |
|      | 13   | Communication Admin. Prohibited             |
| 4    | 0    | Source quench                               |
| 5    | 0    | Network Redirect                            |
|      | 1    | Host Redirect                               |
|      | 2    | ToS & Network Redirect                      |
|      | 3    | ToS & Host Redirect                         |
| 8    | 0    | Echo [Echo Request]                         |
| 9    | 0    | Router Advertisement                        |
|      | 1    | Fragment Reassembly time exceeded           |
| 12   | 0    | Parameter Prob. Pointer indicated the error |
|      | 1    | Missing a required option                   |
|      | 2    | Bad length                                  |
| 13   | 0    | Timestamp                                   |
| 14   | 0    | Timestamp Reply                             |
| 15   | 0    | Information Request                         |
| 16   | 0    | Information Reply                           |
| 17   | 0    | Address Mask Request                        |
| 18   | 0    | Address Mask Reply                          |
| 30   | 0    | Traceroute                                  |

### ICMP Echo Request/Reply (Ping)

|   |         |      |               |   |
|---|---------|------|---------------|---|
|   | 0       | 1    | 2             | 3 |
| 0 | Type    | Code | Checksum      |   |
| 4 | ICMP ID |      | ICMP Sequence |   |

## IPv4 Header

Offset: Add column+row. e.g. Protocol=9  
 ip[9] = "IP header offset 9" or the protocol field

|    |                     |          |          |              |
|----|---------------------|----------|----------|--------------|
|    | 0                   | 1        | 2        | 3            |
| 0  | Ver                 | IHL      | TOS      | Total Length |
| 4  | IP Identification   |          | Offset   |              |
| 8  | TTL                 | Protocol | Checksum |              |
| 12 | Source Address      |          |          |              |
| 16 | Destination Address |          |          |              |
| 20 | Options (optional)  |          |          |              |

Version: 4 ip[0]&0xf0  
 Header Length: IP header length in double-words (4 bytes). Minimum 5 (20 bytes)  
 ToS/Differentiated Services Byte ip[1]

|                       |   |   |   |   |   |     |   |
|-----------------------|---|---|---|---|---|-----|---|
| 0                     | 1 | 2 | 3 | 4 | 5 | 6   | 7 |
| Diff. Svc. Code Point |   |   |   |   |   | ECN |   |

Total Length: includes header ip[2:2]

Flags ip[6]

|   |   |   |   |   |   |   |   |
|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| X | D | M | O | O | O | O | O |

X: Reserved, D: Do Not Frag. M: More Fragments  
 O: Offset bits

Fragment Offset: position of this ip datagram's payload in original packet (multiply by 8)

Protocol ip[9]

|   |      |    |      |     |      |
|---|------|----|------|-----|------|
| 1 | ICMP | 17 | UDP  | 50  | ESP  |
| 2 | IGMP | 41 | IPv6 | 51  | AH   |
| 6 | TCP  | 47 | GRE  | 115 | L2TP |

Checksum: IP Header Only

Options: up to 40 bytes, 4 byte padded ip[20..]

|   |                     |     |                     |
|---|---------------------|-----|---------------------|
| 0 | End of Options List | 68  | Timestamp           |
| 1 | No Operation        | 131 | Loose source route  |
| 7 | Record Route        | 137 | Strict Source Route |

## TCP

|    |                          |   |                |             |
|----|--------------------------|---|----------------|-------------|
|    | 0                        | 1 | 2              | 3           |
| 0  | Source Port              |   | Dest. Port     |             |
| 4  | Sequence Number          |   |                |             |
| 8  | Acknowledgement Number   |   |                |             |
| 12 | HL                       | R | Flags          | Window Size |
| 16 | Checksum                 |   | Urgent Pointer |             |
| 20 | Options (up to 40 bytes) |   |                |             |

Common TCP Ports

|    |          |     |          |      |          |
|----|----------|-----|----------|------|----------|
| 20 | ftp-data | 80  | http     | 443  | https    |
| 21 | ftp      | 88  | kerberos | 445  | MS SMB   |
| 22 | ssh      | 110 | pop3     | 465  | SMTSPS   |
| 23 | telnet   | 113 | authd    | 1433 | MS SQL   |
| 25 | smtp     | 119 | nntp     | 3128 | Squid    |
| 43 | whois    | 143 | imap     | 3306 | Mysql    |
| 53 | dns      | 179 | bgp      | 3389 | MS Term. |

Advanced

- Sequence Number tcp[4:4]: increments with each byte
- Ack. Number tcp[8:4]: next expected sequence number
- Header Length tcp[12]>>4: TCP Header Length / Offset; minimum 5. Number of 32 bit dwords (4 bytes)
- Reserved tcp[12]&0x0f: Set to 0
- Flags tcp[13]

|     |     |     |     |      |     |     |     |
|-----|-----|-----|-----|------|-----|-----|-----|
| 8   | 4   | 2   | 1   | 8    | 4   | 2   | 1   |
| CWR | ECE | URG | ACK | PUSH | RES | SYN | FIN |

Window Size tcp[14:2]: recv. Window size

Checksum tcp[16:2]: Covers pseudo-header + TCP Header + TCP Payload

Urgent Point tcp[18:2]: Offset pointer to urgent data

Options tcp[20:..]

|    |                   |    |                  |
|----|-------------------|----|------------------|
| 0  | End of List       | 3  | Window Scale     |
| 1  | No Operation      | 4  | Selective Ack OK |
| 2  | Max. Segment Size | 8  | Timestamp        |
| 29 | TCP Auth Option   | 30 | Multipath TCP    |