# TCP/IP and tcpdump
# Pocket Reference Guide

tcpdump Usage
tcpdump [-aenStvx] [-F file] [-I int] [-r file] [-s snaplen] [-w file] ['filter_ expression']

-a Display in ASCIII.
-e Display data link header.
-F Filter expression in file.
-I Lisen on int interface.
-n Don't resolve IP addresses.
-r Read packets from file.
-s Get snaplen bytes from each packet.
-S Use absolute TCP sequence numbers.
-t Don't print timestamp.
-v Verbose mode.
-w Write packets to file
-x Display in hex.

**Acronyms**

| | | | |
|---|---|---|---|
| AH | Authentication Header | ISAMKP | Internet Security Association & Key Management |
| ARP | Address Resolution Protocol | | |
| BGP | Border Gateway Protocol | L2T | Layer2 Tunneling Protocol |
| CWR | Congestion Window Reduced | NTP | Network News Transfer Protocol |
| DF | Don't fragment bit (IP) | OSPF | Open Shortest Path First |
| DHCP | Dynamic Host Configuration Protocol | POP3 | Post Office Protocol |
| DNS | Domain Name System | RFC | Request for Comments |
| ECN | Explicit Congestion Notification | RIP | Routing Information Protocol |
| EIGRP | Extended IGRP (Cisco) | LDAP | Lightweight Directory Access Protocol |
| ESP | Encapsulating Security Payload | SMTP | Simple Mail Transfer Protocol |
| FTP | File Transfer Protocol | SNMP | Simple Network Management Protocol |
| GRE | Generic Routing Encapsulation | SSH | Secure Shell |
| HTTP | Hypertext Transfer Protocol (Netscape) | SSL | Secure Sockets Layer |
| ICMP | Internet Control Message Protocol | TCP | Transmission Control Protocol |
| IGMP | Internet Group Management Protocol | TFTP | Trivial File Transfer Protocol |
| IGRP | Interior Gateway Routing Protocol | TOS | Type of Service |
| IMAP | Internet Message Access Protocol | UDP | User Datagram Protocol |
| IP | Internet Protocol | | |

## UDP HEADER

8 bytes
16 bits.

Bit Number

| | |
|---|---|
| Source Port (16b) | Destination Port (16b) |
| Length (16b) | Checksum (16b) |

**UDP Header Information**
Common UDP Well known Server Ports

| | | | |
|---|---|---|---|
| 7 | echo | 138 | netbios-dgm |
| 19 | chargen | 161 | snmp |
| 37 | time | 162 | snmp-trap |
| 53 | domain | 500 | isakmp |
| 67 | bootps (DHCP) | 514 | syslog |
| 68 | bootpc (DHCP) | 520 | rip |
| 69 | tftp | 33434 | tracerote |
| 137 | netbios-ns | | |

**Length**
(Number of bytes in entire datagram including header; minimum value=8)

**Checksum**
(Covers pseudo-header and entire UDO datagram)

## ARP
Bit Number

| | | |
|---|---|---|
| Hardware Address Type (16b) | | Protocol Address Type (16b) |
| H/W Addr.Length (8b) | Protocol Address Length (8b) | Operation (16b) |
| Source Hardware Address (48b) | | |
| Source Hardware Addr. (cont.) | | Source Protocol Addr. (32b) |
| Source Protocol Addr. (cont.) | | Target Hardware Addr. (48b) |
| Target Hardware Address (cont.) | | |
| Target Protocol Address (32b) | | |

**ARP Parameters( for Ethernet and IPv4)**
**Hardware Address Type**
1 Ethernet
6 IEEE 802 LAN

**Protocol Address Type**
2048 Ipv4 (0x800)

**Hardware Address Length**
6 for Ethernet / IEEE 802

**Protocol Address Length**
4 for Ipv4
**Operation**
1 Request
2 Reply

## DNS
Bit Number

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **ID** | | | | | | | |
| **QR** | **Opcode** | **AA** | **TC** | **RD** | **RA** | **Z** | **RCODE** |
| **QDCOUNT** | | | | | | | |
| **ANCOUNT** | | | | | | | |
| **NSCOUNT** | | | | | | | |
| **ARCOUNT** | | | | | | | |
| **Question Section** | | | | | | | |
| **Answer Section** | | | | | | | |
| **Authority Section** | | | | | | | |
| **Additional Information Section** | | | | | | | |

**DNS Parameters**

**Query /Response**
0 Query
1 Response
**Opcode**
0 Standard query ( QUERY)
1 Inverse query ( IQUERY)
2 Server status request ( STATUS)
**AA**
(1 = Authoritative Answer)
**TC**
(1 = TrunCation)
**RD**
(1 = Recursion Desired)
**RA**
(1 = Recursion Available)
**z**
(Reserved; set to 0)
**Response Code**

| | |
|---|---|
| 0 | No error |
| 1 | Format Error |
| 2 | Server Failure |
| 3 | Non-existent domain (NXDOMAIN) |
| 4 | Query type not implemented |
| 5 | Query Refused |

**QDCOUNT:** No. of entries in Question Section
**ANCOUNT:** No. of resource records in Answer Section
**NSCOUNT:** No. of name server resource records in Authority Section
**QDCOUNT:** No. of resource records in Additional Information Section

## ICMP
Bit Number

| | | |
|---|---|---|
| Type (8b) | Code (8b) | Checksum (16b) |
| Other message specific information… | | |

**Type Name/Codes (code =0 unless otherwise specified)**

0 Echo Reply
3 Destination Unreachable
  0 Net Unreachable
  1 Host Unreachable
  2 Protocol Unreachable
  3 Port Unreachable
  4 Fragmentation needed & DF Set
  5 Source Route Failed
  6 Destination Network Unknown
  7 Destination Host Unknown
  8 Source Host Isolated
  9 Network Administratively Prohibited
  10 Host Administratively Prohibited
  11 Network Unreachable for TOS
  12 Host Unreachable for TOS
  13 Communications Administratively Prohibited
4 Source Quench
5 Redirect
  0 Redirect Datagram for the Network
  1 Redirect Datagram for the Host
  2 Redirect Datagram for the TOS & Network
  3 Redirect Datagram for the TOS & Host
8 Echo
9 Router Advertisement
10 Router Selection
11 Time Exceeded
  0 Time to live exceeded in transit
  1 Fragment Reassembly Time Exceeded
12 Parameter Problem
  0 Pointer indicates
  1 Missing a Required Option
  2 Bad length
13 Timestamp
14 Timestamp Reply
15 Information Request
16 Information Reply
17 Address Mask Request
18 Address Mask Reply
30 Traceroute

### PING (Echo / Echo Reply)
Bit Number

| | | |
|---|---|---|
| Type ( 8 or 0) | Code (0) | Checksum |
| Identifier | | Sequence Number |
| Data… | | |

## IP HEADER 20bytes
Bit Number 160 bits

| | | | |
|---|---|---|---|
| Version (4b) | IHL (4b) | Type of Service (8b) | Total Length (16b) |
| Identification (16b) | | Flags (3b) | Fragment Offset (13b) |
| Time To Live (8b) | | Protocol (8b) | Header Checksum (16b) |
| Source Address (32b) | | | |
| Destination Address (32b) | | | |
| Options (optional) | | | |

**IP Header Contents**

**Version**
4 IP Version 4

**Internet Header Length**
Number of 32-bit words in IP header; minimum Value=5 (20 bytes) & maximum value=15 (60 bytes)

| **Type of Service (PreDTRCx)** → | **Differentiated Services** |
|---|---|
| Precedence (000-111) | 000 |
| D (1 = minimize delay) | 0 |
| T (1 = maximize throughout) | 0 |
| R (1 = maximize reliability) | 0 |
| C (1 = minimize cost) | 1 =ECN capable |
| X (reserved and set to 0) | 1 =congestion experienced |

**Total Length**
Number of bytes in packet; maximum lenth=65,535

**Flags (xDM)**
x (reserved and set to 0)
D (1 = Don't Fragment)
M (1 = More Fragments)

**Fragment Offset**
Position of this fragment in the original datagram, in units of 8 bytes.

**Protocol**

| | | |
|---|---|---|
| 1 ICMP | 17 UDP | 88 EIGRP |
| 2 IGMP | 47 GRE | 89 OSPF |
| 6 TCP | 50 ESP | 115 L2TP |
| 9 IGRP | 51 AH | |

**Header Checksum**
Covers IP header only

**Addressing**

| NET_ID | | RFC 1918 PRIVATE ADDRESSES |
|---|---|---|
| 0-127 | Class A | 10.0.0.0-10.255.255.255 |
| 128-191 | Class B | 172.16.0.0-172.31.255.255 |
| 192-223 | Class C | 192.168.0.0-192.168.255.255 |
| 224-239 | Class D | (multicast) |
| 240-255 | Class E | (experimental) |

HOST_ID
0 Network value; broadcast (old)
255 Broadcast

**Options (0-40 bytes; padded to 4-byte boundary)**

| | |
|---|---|
| 0 End of Options list | 68 Timestamp |
| 1 No operation (pad) | 131 Loose source route |
| 7 Record route | 137 Strict source route |

## TCP HEADER 20 bytes
Bit Number 160 bits.

| | | | |
|---|---|---|---|
| Source Port (16b) | | Destination Port (16b) | |
| Sequence Number (32b) | | | |
| Acknowledgement Number (32b) | | | |
| Offset (4b) | Reserved (6b) | Flags (6b) | Window (16b) |
| Checksum (16b) | | Urgent Pointer (16b) | |
| Options (Optional) | | | |

**TCP Header Contents**

Common TCP Well Known Server Ports

| | |
|---|---|
| 7 echo | 110 pop3 |
| 19 chargen | 111 sunrpc |
| 20 ftp-data | 119 nntp |
| 21 ftp-control | 139 netbios-ssn |
| 22 ssh | 143 imap |
| 23 telnet | 179 bgp |
| 25 smtp | 389 ldap |
| 53 domain | 443 https (ssl) |
| 79 finger | 445 microsoft-ds |
| 80 http | 1080 socks |

**Offset**
Number of 32-bit words in TCP header; minimum value =5

**Reserved**
4 bits; set to 0
ECN bits (used when ECN employed; else 00)
CWR ( 1= sender has cut congestion window in half)
ECN-Echo 9 1- receiver cuts congestion window in half)

**Flags (UAPRSF)**
U (1=Urgent pointer valid)
A (1= Acknowledgement field value valid)
P (1=Push data)
R (1=Reset connection)
S (1= Synchronize sequence numbers)
F (1=no more data; Finish connection)

**Checksum**
Covers pseudoheader and entire TCP segment

**Urgent Pointer**
Points to the sequence number of the byte following urgent data.

**Options**

| | |
|---|---|
| 0 End of Options list | 3 Window scale |
| 1 No operation (pad) | 4 Selective ACK ok |
| 2 Maximum segment size | 8 Timestamp |