UDP Header

Bit Number

```
                    1 1 1 1 1 1 1 1 1 1 2 2 2 2 2 2 2 2 2 2 3 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
```

Source Port	**Destination Port**
Length	**Checksum**

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	traceroute
137	netbios-ns		

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

Checksum
(Covers pseudo-header and entire UDP datagram)

ARP

Bit Number

```
                    1 1 1 1 1 1 1 1 1 1 2 2 2 2 2 2 2 2 2 2 3 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
```

<table>
<tr><td colspan="2"><b>Hardware Address Type</b></td><td colspan="2"><b>Protocol Address Type</b></td></tr>
<tr><td><b>H/w Addr Len</b></td><td><b>Prot. Addr Len</b></td><td colspan="2"><b>Operation</b></td></tr>
<tr><td colspan="4"><b>Source Hardware Address</b></td></tr>
<tr><td colspan="2"><b>Source Hardware Addr (cont.)</b></td><td colspan="2"><b>Source Protocol Address</b></td></tr>
<tr><td colspan="2"><b>Source Protocol Addr (cont.)</b></td><td colspan="2"><b>Target Hardware Address</b></td></tr>
<tr><td colspan="4"><b>Target Hardware Address (cont.)</b></td></tr>
<tr><td colspan="4"><b>Target Protocol Address</b></td></tr>
</table>

ARP Parameters (for Ethernet and IPv4)

Hardware Address Type
1 Ethernet
6 IEEE 802 LAN

Protocol Address Type
2048 IPv4 (0x0800)

Hardware Address Length
6 for Ethernet/IEEE 802

Protocol Address Length
4 for IPv4

Operation
1 Request
2 Reply

DNS

Bit Number

```
                    1   1   1   1   1   1
0 1 2 3 4 5 6 7 8 9 0   1   2   3   4   5
```

<table>
<tr><td colspan="8"><b>ID.</b></td></tr>
<tr><td><b>QR</b></td><td><b>Opcode</b></td><td><b>AA</b></td><td><b>TC</b></td><td><b>RD</b></td><td><b>RA</b></td><td><b>Z</b></td><td><b>RCODE</b></td></tr>
<tr><td colspan="8"><b>QDCOUNT</b></td></tr>
<tr><td colspan="8"><b>ANCOUNT</b></td></tr>
<tr><td colspan="8"><b>NSCOUNT</b></td></tr>
<tr><td colspan="8"><b>ARCOUNT</b></td></tr>
<tr><td colspan="8"><b>Question Section</b></td></tr>
<tr><td colspan="8"><b>Answer Section</b></td></tr>
<tr><td colspan="8"><b>Authority Section</b></td></tr>
<tr><td colspan="8"><b>Additional Information Section</b></td></tr>
</table>

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-existant 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)
ARCOUNT
(No. of resource records in Additional Information section.

SANS EMERGENCY
www.incidents.org
INCIDENT HANDLER

TCP/IP and tcpdump

Pocket Reference Guide

SANS Institute
incidents@sans.org
+1 317.580.9756
http://www.sans.org
http://www.incidents.org

tcpdump Usage

```
tcpdump  [-aenStvx]  [-F file]
[-i int]  [-r file]  [-s snaplen]
[-w file]  ['filter_expression']

-e  Display data link header.
-F  Filter expression in file.
-i  Listen 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.
-X  Display in hex and ASCII.
```

Acronyms

AH	Authentication Header (RFC 2402)	ISAKMP	Internet Security Association & Key Management Protocol (RFC 2408)
ARP	Address Resolution Protocol (RFC 826)	L2TP	Layer 2 Tunneling Protocol (RFC 2661)
BGP	Border Gateway Protocol (RFC 1771)	NNTP	Network News Transfer Protocol (RFC 977)
CWR	Congestion Window Reduced (RFC 2481)	OSPF	Open Shortest Path First (RFC 1583)
DF	Don't Fragment bit (IP)	POP3	Post Office Protocol v3 (RFC 1460)
DHCP	Dynamic Host Configuration Protocol (RFC 2131)	RFC	Request for Comments
DNS	Domain Name System (RFC 1035)	RIP	Routing Information Protocol (RFC 2453)
ECN	Explicit Congestion Notification (RFC 3168)	LDAP	Lightweight Directory Access Protocol (RFC 2251)
EIGRP	Extended IGRP (Cisco)	SKIP	Simple Key-Management for Internet Protocols
ESP	Encapsulating Security Payload (RFC 2406)	SMTP	Simple Mail Transfer Protocol (RFC 821)
FTP	File Transfer Protocol (RFC 959)	SNMP	Simple Network Management Protocol (RFC 1157)
GRE	Generic Routing Encapsulation (RFC 2784)	SSH	Secure Shell
HTTP	Hypertext Transfer Protocol (RFC 1945)	SSL	Secure Sockets Layer (Netscape)
ICMP	Internet Control Message Protocol (RFC 792)	TCP	Transmission Control Protocol (RFC 793)
IGMP	Internet Group Management Protocol (RFC 2236)	TFTP	Trivial File Transfer Protocol (RFC 1350)
IGRP	Interior Gateway Routing Protocol (Cisco)	TOS	Type of Service field (IP)
IMAP	Internet Message Access Protocol (RFC 2060)	UDP	User Datagram Protocol (RFC 768)
IP	Internet Protocol (RFC 791)		

All RFCs can be found at http://www.rfc-editor.org

ICMP

Bit Number

```
                    1 1 1 1 1 1 1 1 1 1 2 2 2 2 2 2 2 2 2 2 3 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
```

<table>
<tr><td>Type</td><td>Code</td><td>Checksum</td></tr>
<tr><td colspan="3">Other message-specific information...</td></tr>
</table>

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	Communication 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 the error
	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

```
                    1 1 1 1 1 1 1 1 1 1 2 2 2 2 2 2 2 2 2 2 3 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
```

<table>
<tr><td>Type (8 or 0)</td><td>Code (0)</td><td>Checksum</td></tr>
<tr><td colspan="2">Identifier</td><td>Sequence Number</td></tr>
<tr><td colspan="3">Data...</td></tr>
</table>

IP Header

Bit Number

```
                    1 1 1 1 1 1 1 1 1 1 2 2 2 2 2 2 2 2 2 2 3 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
```

<table>
<tr><td>Version</td><td>IHL</td><td>Type of Service</td><td colspan="2">Total Length</td></tr>
<tr><td colspan="3">Identification</td><td>Flags</td><td>Fragment Offset</td></tr>
<tr><td colspan="2">Time to Live</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>
<tr><td colspan="5">Options (optional)</td></tr>
</table>

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 throughput)	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 length = 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	57	SKIP
2	IGMP	47	GRE	88	EIGRP
6	TCP	50	ESP	89	OSPF
9	IGRP	51	AH	115	L2TP

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

Bit Number

```
                    1 1 1 1 1 1 1 1 1 1 2 2 2 2 2 2 2 2 2 2 3 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
```

<table>
<tr><td colspan="3">Source Port</td><td>Destination Port</td></tr>
<tr><td colspan="4">Sequence Number</td></tr>
<tr><td colspan="4">Acknowledgment Number</td></tr>
<tr><td>Offset
(Header Length)</td><td>Reserved</td><td>Flags</td><td>Window</td></tr>
<tr><td colspan="3">Checksum</td><td>Urgent Pointer</td></tr>
<tr><td colspan="4">Options (optional)</td></tr>
</table>

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 (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