DNS

Bit Number

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

LENGTH (TCP ONLY)							
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-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.

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

Type	Code	Checksum
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 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

Type (8 or 0)	Code (0)	Checksum
Identifier		Sequence Number
Data...		

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

Version	IHL	Type of Service	Total Length
Identification		Flags	Fragment Offset
Time to Live	Protocol	Header Checksum	
Source Address			
Destination Address			
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 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

Source Port			Destination Port
Sequence Number			
Acknowledgment Number			
Offset (Header Length)	Reserved	Flags	Window
Checksum			Urgent Pointer
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

Flags (CEUAPRSF)

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)

U (1 = Consult urgent pointer, notify server application of urgent data)
A (1 = Consult acknowledgement field)
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
Offset pointer to 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