INTERNET PROTOCOL (IP)

Packet-Level Functionality and Fields of the Internet Protocol

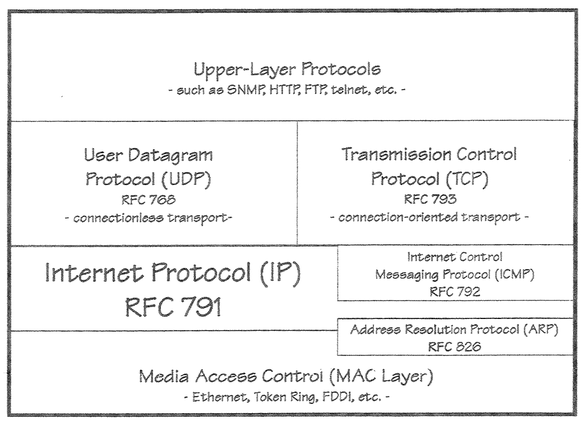
IP Functionality:

IP offers end-to-end connectivity between devices on separate networks. An IP header enables a packet to be routed through an internetwork using a software address that includes a network address portion and a host address portion. Routers along a path examine the destination IP address found in the IP header to determine if they can forward the packet.

The IP header also includes fields to ensure the packet does not circulate endlessly in case of an internetwork loop and fields to enable a packet to be broken down (fragmented) into smaller pieces when the network path does not support a single MTU (maximum transmission unit) size from end-to-end.

The currently widely-implemented version of IP is IPv4. IPv6 is in development. (See www.packet-level.com for more information.)

Basic TCP/IP Stack Elements



UDP-over-IP Communication (DNS Query)

```
DLC:  Destination = Station 00104B30C44A
DLC:  Source      = Station 00A0CC30C8DB
DLC:  Ethertype   = 0800 (IP)
IP:  Vers. = 4, header length = 20 bytes
IP:  Type of service = 00
IP:  Total length    = 58 bytes
IP:  Identification  = 45568
IP:  Flags           = 0X may/last fragment
IP:  Fragment offset = 0 bytes
IP:  Time to live    = 128 seconds/hops
IP:  Protocol        = 17 (UDP)
IP:  Header checksum = 744F (correct)
IP:  Source address      = [10.0.0.99]
IP:  Destination address = [10.0.0.1]
IP:  No options
UDP:  Source port      = 1031
UDP:  Destination port = 53 (Domain)
UDP:  Length           = 38
UDP:  Checksum         = CB03 (correct)
UDP:  [30 byte(s) of data]
DNS:  DNS: ID = 1
DNS:  Flags = 01 Query; Recursion desired
DNS:  Flags = 0X; verified data only
DNS:  Question count = 1, Answer count = 0
DNS:  Authority count = 0, Addl. record= 0
DNS:     ZONE Section
DNS:     Name = ftpcorp1.NAI
DNS:     Type = Host address (A,1)
DNS:     Class = Internet (IN,1)
```

TCP-over-IP Communication (TCP Handshake)

```
DLC:  Destination = Station Trndnt3C3D8B
DLC:  Source      = Station Eagle 005FC1
DLC:  Ethertype   = 0800 (IP)
IP:  Version = 4, header length = 20 bytes
IP:  Type of service = 00
IP:  Total length    = 44 bytes
IP:  Identification  = 1536
IP:  Flags           = 4X; don't/last fragment
IP:  Fragment offset = 0 bytes
IP:  Time to live    = 32 seconds/hops
IP:  Protocol        = 6 (TCP)
IP:  Header checksum = 284F (correct)
IP:  Source address      = [130.57.20.10]
IP:  Destination address = [130.57.20.1]
IP:  No options
TCP:  Source port             = 1026
TCP:  Destination port        = 524
TCP:  Initial sequence number = 12952
TCP:  Next expected Seq number= 12953
TCP:  Data offset             = 24 bytes
TCP:  Flags                   = 02
                      ..0. .... = (No urgent pointer)
                      ...0 .... = (No acknowledgment)
                      .... 0... = (No push)
                      .... .0.. = (No reset)
                      .... ..1. = SYN
                      .... ...0 = (No FIN)
TCP:  Window                  = 8192
TCP:  Checksum                = 1303 (correct)
TCP:  Options follow
TCP:  Maximum segment size = 1460
```

NOTES:

Note #1 **Version field:** This 4-bit field indicates the version of IP in use. The following lists the version numbers assigned:

v0 Reserved	v7 TP/IX: The Next Internet
v4 Internet Protocol (RFC 791)	v8 PIP: The P Internet Protocol
v5 ST (Stream) Datagram Mode (RFC 1190)	v9 TUBA
v6 Internet Protocol Version 6 (RFC 1752)	v15 Reserved

Versions 1-3 and 10-14 are unassigned.

Note #2 **Internet Header Length (IHL) field:** This field denotes the length of the IP header in 4-byte increments. For example, the value 5 in this field defines a 20-byte IP header. Subtract this value from the Total Length field to obtain the length of transport layer and data in the packet.

Note #3 **Precedence/Type of Service field:** This field identifies the quality of service that a packet should receive (if possible). Bits 0-2 are used for Precedence; bits 3-6 are used for Type of Service; bit 7 is reserved.

Precedence Value	Precedence Description
111	Network Control
110	Internetwork Control
101	CRITIC/ECP
100	Flash Override
011	Flash
010	Immediate
001	Priority

TOS Value	Service Description
0000	Default (no specific service type)
0001	Minimize Monetary Cost
0010	Maximize Reliability
0100	Maximize Throughput
1000	Minimize Delay
1111	Maximize Security

Note #4 **Total Length field:** This field defines the total number of bytes in the IP packet from the start of the IP header through the end of valid data. This field does not include any bytes inserted as padding at the end of the packet.

Note #5 **Flags field:** This field actually consists of three separate single-bit fields. The fields are:

Bit 0: Reserved (set to 0)
Bit 1: May/Don't Fragment bit (0=May Fragment; 1=Don't Fragment)
Bit 2: More/Last Fragment bit (0=Last Fragment; 1=More Fragments to Come)

The following figure denotes the bit placement/values as well.

Bit 0	Bit 1	Bit 2
0	D F	M F

DF = Don't Fragment bit
MF = More Fragment bit

Note #6 **Time to Live field:** This field defines the remaining lifetime of the packet. Although originally defined as a measurement of 'seconds,' it is often referred to as the 'remaining hop count' value since routing devices will decrement this field value by 1 even if it didn't take one second for the routing process to transpire. Typical TTL starting values are 32, 64 and 128.

A packet with a TTL value of 1 arriving at a router cannot be routed (the router may not decrement the TTL value to 0 and forward the packet). A packet with a TTL value of 1 arriving at the destination can be processed, however.

In the case of a fragmented packet, all fragments are given the TTL value at the time of fragmentation. The fragments may take different paths to the destination and may end up with different TTL values upon arrival. All fragments must arrive at the destination within the TTL value of the first-received fragment, however.

Note #7 **Header Checksum field:** This field contains a checksum value for the IP header only and includes all fields except the Header Checksum field itself.

IP Header Structure

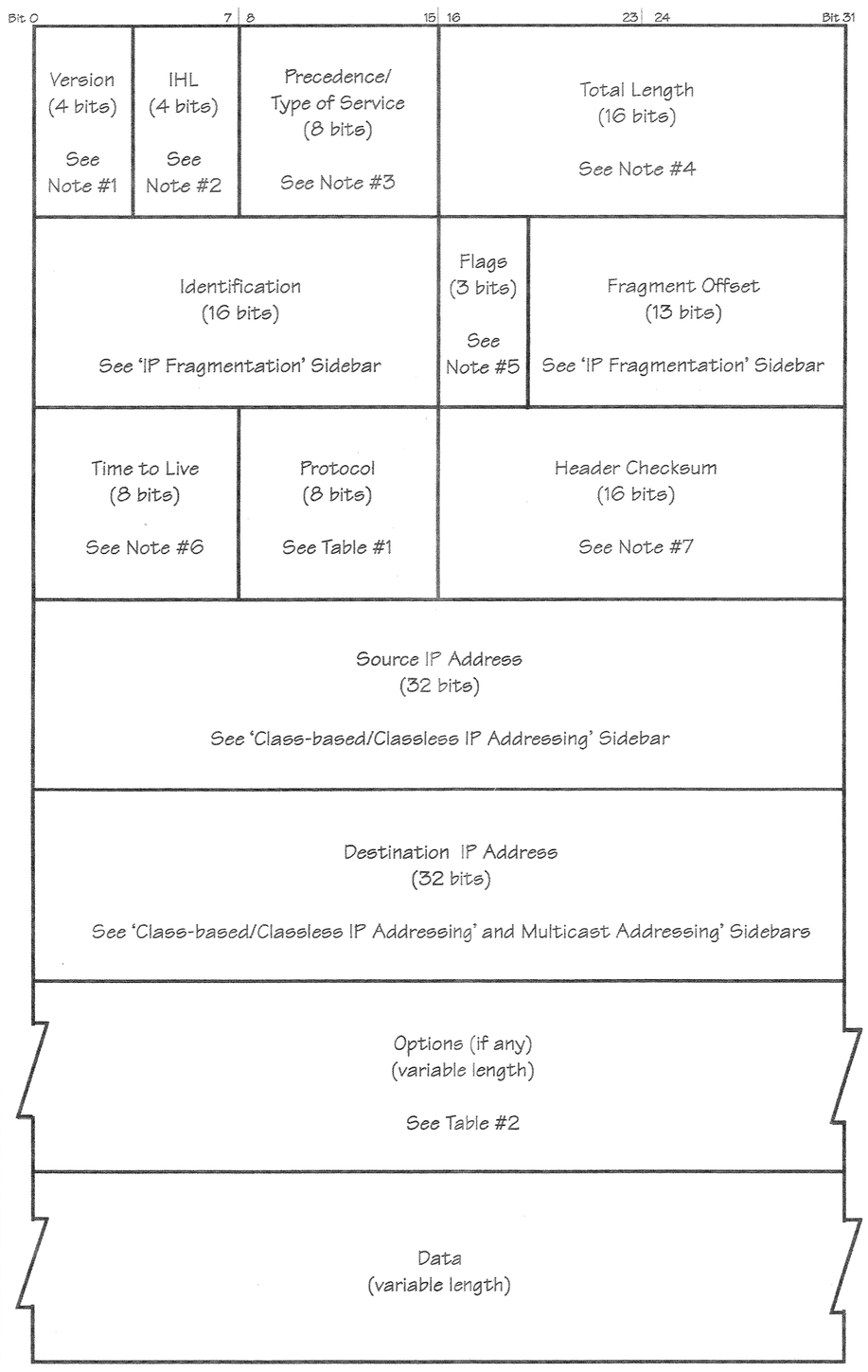


Table #1: Protocol Field

Decimal	Protocol
0	IPv6 Hop-by-Hop Option
1	Internet Control Message Protocol
2	Internet Group Management Protocol
3	Gateway-to-Gateway
4	IP in IP (encapsulation)
5	Stream
6	Transmission Control Protocol
7	CBT
8	Exterior Gateway Protocol
9	Any private interior gateway (i.e. IGRP)
10	BBN RCC Monitoring
11	Network Voice Protocol
12	PUP
13	ARGUS
14	EMCON
15	Cross Net Debugger
16	Chaos
17	User Datagram Protocol
18	Multiplexing
19	DCN Measurement Subsystems
20	Host Monitoring
21	Packet Radio Measurement
22	XEROX NS IDP
23	Trunk-1
24	Trunk-2
25	Leaf-1
26	Leaf-2
27	Reliable Data Protocol
28	Internet Reliable Transaction
29	ISO Transport Protocol Class 4
30	Bulk Data Transfer Protocol
31	MFE Network Services Protocol
32	MERIT Internodal Protocol
33	Sequential Exchange Protocol
34	Third Party Connect Protocol
35	Inter-Domain Policy Routing Protocol
36	XTP

Decimal	Protocol (continued)
36	XTP
37	Datagram Delivery Protocol
38	IDPR Control Message Transport
39	TP++ Transport Protocol
40	IL Transport Protocol
41	IPv6
42	Source Demand Routing Protocol
43	IPv6-Route Routing Header for IPv6
44	Fragment Header for IPv6
45	Inter-Domain Routing Protocol
46	Reservation Protocol
47	General Routing Encapsulation
48	Mobile Host Routing Protocol
49	BNA
50	Encap Security Payload for IPv6
51	Authentication Header for IPv6
52	Integrated Net Layer Security
53	IP with Encryption
54	NBMA Address Resolution Protocol
55	IP Mobility
56	Transport Layer Security Protocol
57	SKIP
58	ICMP for IPv6
59	No Next Header for IPv6
60	Destination Options for IPv6
61	Any host internal protocol
62	CFTP
63	Any local network
64	SATNET and Backroom EXPAK
65	Kryptolan
66	MIT Remote Virtual Disk Protocol
67	Internet Pluribus Packet Core
68	Any distributed file system
69	SATNET Monitoring
70	VISA Protocol

[see www.iana.org for remaining assigned values]

Table #2: IP Header Options

#	Value	Reference
0	0	End of Options List
1	1	No Operation
2	130	Security
3	131	Loose Source Route
4	68	Time Stamp
5	133	Extended Security
6	134	Commercial Security
7	7	Record Route
8	136	Stream ID
9	137	Strict Source Route
10	10	Experimental Measurement
11	11	MTU Probe
12	12	MTU Reply

#	Value	Reference (continued)
13	205	Experimental Flow Control
14	142	Experimental Access Control
15	15	Encode
16	144	IMI Traffic Descriptor
17	145	Extended Internet Protocol
18	82	Traceroute
19	147	Address Extension
20	148	Router Alert
21	149	Selective Directed Broadcast
22	150	NSAP Addresses
23	151	Dynamic Packet State
24	152	Upstream Multicast Pkt.

[Options list assigned/maintained at www.iana.org.]

IP Fragmentation

Fragmentation is necessary when a packet is too large to fit on the media. The packet must be fragmented into multiple pieces at the point where the media size changes (typically a router) and reassembled at the destination.

For example, consider a device that sends a 4096-byte packet from a Token Ring network to a device located one router on an Ethernet network. The Ethernet network can only support 1518 byte packets. The router that connects the Token Ring network to the Ethernet network must fragment a single packet into three separate packets.

The process of fragmentation uses three fields of the IP header: the Identification field, Flags field, and the Fragment Offset field.

Identification field: All IP packets contain a unique ID number. When a packet must be fragmented into several pieces, the same ID number is placed in each fragment to identify them as a set.

Flags field: This field consists of three bits - only two are used. Bits 1 and 2 of this field (see Note #5) are used to indicate if fragmentation is allowed (Don't Fragment bit) and if a packet is part of a fragment set (More Fragments).

Fragmentation Offset field: This field indicates where the fragment's data should be placed in relation to the other fragment data. The field indicates the offset in a units of 8 octets (64 bits).

Fragment 1 of 3

```
IP:  ----- IP Header -----
IP:  Total length    = 1500 bytes
IP:  Identification  = 19485
IP:  Flags           = 2X
IP:        .0.. .... = may fragment
IP:        ..1. .... = more fragments
IP:  Fragment offset = 0 bytes
IP:  Time to live    = 32 seconds/hops
IP:  Protocol        = 1 (ICMP)
IP:  Multi-Frame IP data, Frames:  1, 2, 3
```

Fragment 2 of 3

```
IP:  ----- IP Header -----
IP:  Total length    = 1500 bytes
IP:  Identification  = 19485
IP:  Flags           = 2X
IP:        .0.. .... = may fragment
IP:        ..1. .... = more fragments
IP:  Fragment offset = 1480 bytes
IP:  Time to live    = 32 seconds/hops
IP:  1480 bytes of data continuation of IP ident=19485
```

Fragment 3 of 3

```
IP:  ----- IP Header -----
IP:  Total length    = 1164 bytes
IP:  Identification  = 19485
IP:  Flags           = 0X
IP:        .0.. .... = may fragment
IP:        ..0. .... = last fragment
IP:  Fragment offset = 2960 bytes
IP:  Time to live    = 32 seconds/hops
IP:  [1144 bytes of data continuation of IP ident=19485]
```

Class-based IP Addressing

Class-based addressing offers an IP address system that separates address into several basic classes with predefined field lengths for the network portion of the address and the host ID portion of the address as shown below.

Class	Net/Host	Network Mask	First Byte in Binary	First Byte in Decimal
Class A	N.H.H.H	255.0.0.0	0xxxxxxx	0 - 127*
Class B	N.N.H.H	255.255.0.0	10xxxxxx	128 - 191
Class C	N.N.N.H	255.255.255.0	110xxxxx	192 - 223
Class D	Multicast	n/a	1110xxxx	224 - 239
Class E	Reserved	n/a	11111xxx	240 - 255

* A network address starting with 0 is invalid. The network address 127 is reserved for the loopback address.

When a single network address is required to support two or more physical networks, the address can be subnetted. Subnetting is covered in detail in RFC 1918.

The "Network Address"
Placing the value 0 (binary) in all positions of the host ID portion indicate the network's address. For example, 9.0.0.0 can be used to refer to the entire 9.x.x.x network. It is not allowable to assign a host the host ID of all 0s.

All-Network Broadcast
Placing the value 1 (binary) in all positions of the network and host ID portion of an address is a network broadcast. The decimal value is 255.255.255.255. Broadcasts are typically not be forwarded by routers (even though the broadcast is directed to 'all networks.')..

Subnet Broadcast
Placing the value 1 (binary) in all positions of the host ID portion of an address is a broadcast for a specific subnetwork. For example, 9.255.255.255 is a broadcast onto network 9.0.0.0.

Classless IP Addressing

Classless Interdomain Routing (CIDR) defines a method for addressing without Class A, B, or C network delineations. Instead of using such rigid delimiters and making assumptions on the bytes used for network and host portion of the address, classless addresses consist of an address and the prefix. The prefix indicates the number of bits to be masked off for the network portion. The following table illustrates the classless addressing prefixes and masks.

CIDR Prefix	Dotted Decimal Mask	Binary
/1	128.0.0.0	10000000 00000000 00000000 00000000
/2	192.0.0.0	11000000 00000000 00000000 00000000
/3	224.0.0.0	11100000 00000000 00000000 00000000
/4	240.0.0.0	11110000 00000000 00000000 00000000
/5	248.0.0.0	11111000 00000000 00000000 00000000
/6	252.0.0.0	11111100 00000000 00000000 00000000
/7	254.0.0.0	11111110 00000000 00000000 00000000
/8	255.0.0.0	11111111 00000000 00000000 00000000
/9	255.128.0.0	11111111 10000000 00000000 00000000
/10	255.192.0.0	11111111 11000000 00000000 00000000
/11	255.224.0.0	11111111 11100000 00000000 00000000

(and so on...)

Private Addresses
The Internet Assigned Numbers Authority (IANA) has reserved the following addresses for private internets.

10.0.0.0 - 10.255.255.255 (10/8 prefix)
172.16.0.0 - 172.31.255.255 (172.16/12 prefix)
192.168.0.0 - 192.168.255.255 (192.168/16 prefix)

These numbers cannot be advertised on the Internet. Network Address Translation (NAT) systems may be used to allow connectivity between private from public addressing systems.

Multicast Addressing

Multicasting is used to address a group of IP devices. The multicast address can only be used in the destination IP address field (never in the source IP address field). Routing Information Protocol (RIP) version 2, Open Shortest Path First (OSPF), Service Location Protocol (SLP) and Internet Group Management Protocol (IGMP) use multicast addresses. See RFC 1112, Host Extensions for IP Multicasting" for more information.

All IP multicast addresses are assigned between 224.0.0.0 and 239.255.255.255. The range 224.0.0.0 through 224.0.0.255, inclusively, are reserved for the use of routing protocols and other topology and maintenance discovery protocols. These multicast packets should not be forwarded by multicast routers.

Multicast MAC Headers
The IP multicast address provides the 'seed' for the creation of a multicast MAC address by translating the last three bytes of the IP multicast address into hexadecimal and placed in the last three bytes of the MAC address.

For example, in the packet shown at right, an IGMP packet addressed to IP address 224.0.1.22 (Service Location Protocol multicast address) uses the MAC header destination address 0x01005E000116 (where '16' is the hexadecimal equivalent of '22' decimal). The leading three bytes use an IANA-assigned MAC identifier (0x00005E with the first byte changed to an odd number - 0x01 - to denote a multicast MAC packet).

Partial List of Assigned Multicast Addresses
The following list includes the basic set of multicast addresses (from 224.0.0.0 to 224.0.0.255). Refer to www.iana.org for a complete list of assigned multicast addresses.

Address	Description
224.0.0.0	Base Address (Reserved)
224.0.0.1	All Systems on this Subnet
224.0.0.2	All Routers on this Subnet
224.0.0.3	Unassigned
224.0.0.4	DVMRP Routers
224.0.0.5	OSPFIGP All Routers
224.0.0.6	OSPFIGP Designated Rtrs.
224.0.0.7	ST Routers
224.0.0.8	ST Hosts
224.0.0.9	RIP2 Routers
224.0.0.10	IGRP Routers
224.0.0.11	Mobile-Agents

Address	Description (continued)
224.0.0.12	DHCP Server/Relay Agent
224.0.0.13	All PIM Routers
224.0.0.14	RSVP-ENCAPSULATION
224.0.0.15	all-cbt-routers
224.0.0.16	designated-sbm
224.0.0.17	all-sbms
224.0.0.18	VRRP
224.0.0.19	IPAIL1ISs
224.0.0.20	IPAIL2ISs
224.0.0.21	IPAll Intermediate Systems
224.0.0.22	IGMP
224.0.0.23 to 224.0.0.255	unassigned

Multicast Packet (Joining SLP Group)

```
DLC:  Destination = Multicast 01005E000116
DLC:  Source      = Station 00A0CC30C8DB
DLC:  Ethertype   = 0800 (IP)
DLC:  IP: ----- IP Header -----
      IP: Vers = 4, header length = 24 bytes
IP:   Type of service = 00
IP:   Total length    = 32 bytes
IP:   Identification  = 768
IP:   Flags           = 0X
IP:         .0.. .... = may fragment
IP:         ..0. .... = last fragment
IP:   Fragment offset = 0 bytes
IP:   Time to live    = 1 seconds/hops
IP:   Protocol        = 2 (IGMP)
IP:   Header checksum = 365F (correct)
IP:   Source address      = [10.0.0.99]
IP:   Destination address = [224.0.1.22]
IP:   Options follow
IP:   Option 148
IP:   [3 byte(s) of header padding]
IP:   IGMP: ----- IGMP header -----
IGMP:  IGMP: Version       = 1
IGMP:  Type = 6 (Ver2 Membership Report)
IGMP:  Unused        = 0x00
IGMP:  Checksum      = 08E9 (correct)
IGMP:  Group Address = [224.0.1.22]
```

DEVELOPER
PROTOCOL ANALYSIS INSTITUTE, LLC

Reach us at
www.packet-level.com

TITLE
INTERNET PROTOCOL (IP) AT PACKET-LEVEL

SIZE	DRAWING INFORMATION	REVISION
D	IPPKT.DWG	A

Packet-Level Courses: www.podbooks.com
Phone orders - 408/378-7841. Fax orders - 408/378-7891