

Internet Protocol (IP) v4 Reference

Benoît H. Dicaire <Benoit.Dicaire@INFRAX.com>

Version: July, 2006

This is a snapshot of an on-line document. Paper copies are valid only on the day they are printed.

Please refer to the author if you are in any doubt about the currency of this document.

While every effort has been taken to verify the accuracy of this information, neither INFRAX incorporated nor the author of this publication can accept any responsibility or liability for errors, omissions, or damages resulting from the use of the information herein.

The current electronic of the document will be found at : www.INFRAX.com/Publications

Internet Protocol (IP) v4 Reference

Publication's Information

Version: July, 2006

This document was created on 12 June 2001 and is based on the best information available at revision time.

The copyright in this work belong to INFRAX Incorporated. Please direct permission questions to Info@INFRAX.com and content feedback to the author: Benoit.Dicaire@INFRAX.com.

Products or corporate names may be trademarks or registered trademarks of other companies and are used only for the explanation and to the owner's benefit, without intent to infringe.

Reproduction Guideline

You may print this document and distribute it electronically. If you quote or reference this document, you must appropriately attribute the contents and authorship. You may not alter this document in any way nor charge for it.

About the Author

Benoît H. Dicaire is the founder and Information Security Strategist for INFRAX.

With nearly two decades of experience providing key strategies and technology solutions for managing information security risks, Dicaire now focuses his work on Security Posture Assessment and Enterprise Architecture for organizations in Canada and around the world.

A trusted advisor, Dicaire is frequently consulted by leaders of private and government organizations.

About INFRAX

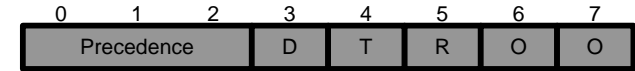
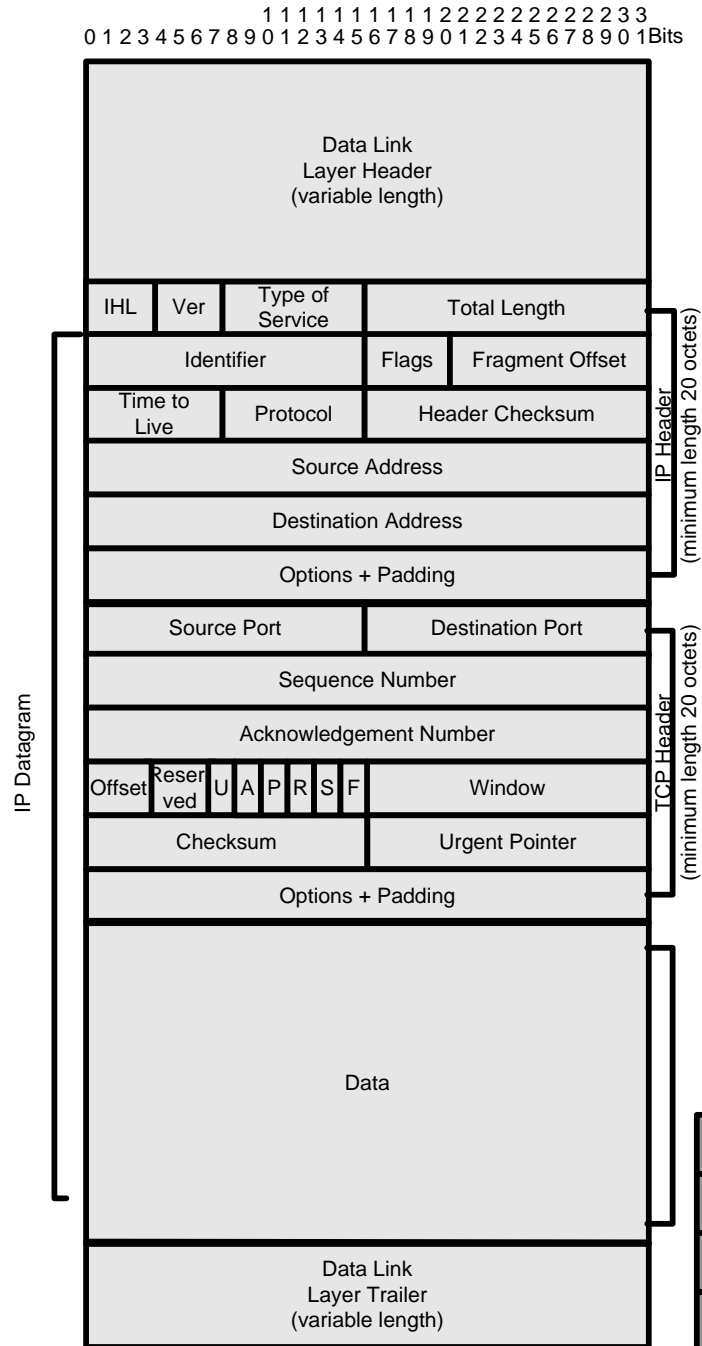
INFRAX is an independent Information Security consulting firm dedicated to providing our clients with top-level security solutions, advice and protection. Furthermore, unbiased in-depth INFRAX structure analysis helps organizations make smarter enterprise architecture decisions adapted to today's increasingly complex environments.

Adress Resolution Protocol (ARP)
Reverse Address Resolution Protocol (RARP)
 1 1 1 1 1 1 1 1 1 1 2 2 2 2 2 2 2 2 2 2 3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 Bits

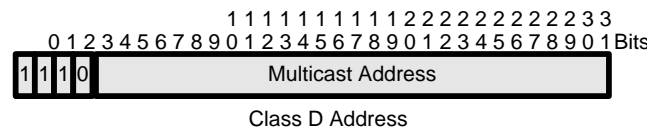
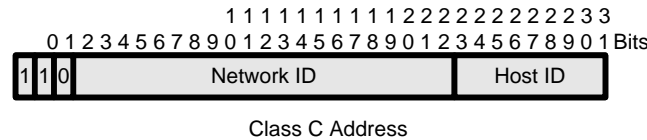
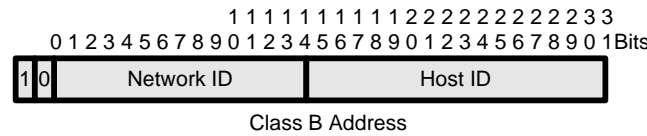
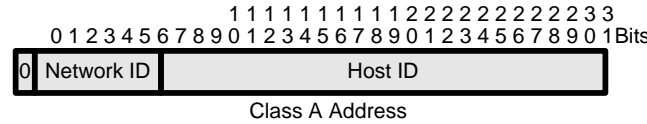
Hardware Type		Protocol Type
HA Lenght	PA Lenght	Operation
Sender HA (octets 0-1)*		
Sender HA (octets 4-5)		Sender PA (octets 0-1)
Sender PA (octets 2-3)		Target HA (octets 0-1)
Target HA (octets 2-5)		
Target PA (octets 0-3)		

*Field lenghts assume HA = 6 octets and PA = 4 octets

Field	Description
Hardware Type:	Hardware for wich the request is being made. Examples Include: 1 = Ethernet (10Mb) 3 = Amateur Radio AX.25 4 = Proteon ProNET Token Ring 5 = Chaos 6 = IEEE 802 Networks 7 = ARCNET 8 = Hyperchannel 11 = Local Talk
Protocol Type:	Protocol code, e.g., Ethertype
HA length:	Length of hardware address in octects
PA length:	Length of protocol address in octetcs
Operation:	Operation code for this message: 1 = ARP request 2 = ARP reply 3 = RARP request 4 = RARP reply
Sender HA:	Sender's hardware address (48 bits for Ethernet)
Sender PA:	Sender's protocol address (32 bits for IP)
Target HA:	Target hardware address (48 bits for Ethernet)
Target PA:	Target protocol address (32 bits for IP)



Bit 0-2:	Precedence
111 - Network Control	011 - Flash
110 - Internet Control	010 - Immediate
001 - CRITIC / ECP	001 - Priority
100 - Flash override	000 - Routine
Bit 3:	0 = Normal Delay, 1 = Low Delay
Bit 4:	0 = Normal Throughput, 1 = High Throughput
Bit 5:	0 = Normal Reliability, 1 = High Reliability
Bit 6 - 7:	Reserved for Future Use (set to 0)



Options (variable):	Options from the sender, e.g. a route specification
Padding (variable):	Provided so that the IP header ends on a 32 bit boundary.
Data (variable):	A multiple of 8 bits, not to exceed 65,535 octets for IP.

Header checksum (16 bits):	A checksum on the IP header that may be recomputed at each gateway.
Source address (32 bits):	The internet address of the originating host.
Destination address (32 bits):	The internet address of the destination host.

Field	Description
Version (4 bits)	The IP version number (currently 4).
Internet Header length (4 bits)	The length of the header in 32 bit words.
Type of service (8 bits)	Flags to specify precedence, delay, throughput and reliability parameters.

Decimal	Keyword	Description
1	ICMP	Internet Control Message
2	IGMP	Internet Group Management
6	TCP	Transmission Control
8	EGP	Exterior Gateway Protocol
12	PUP	PUP
16	CHAOS	Chaos
17	UDP	User Datagram
22	XNS-IDP	Xerox NS IDP
29	ISO-TP4	ISO Transport Protocol Class 4
80	ISO-IP	ISO Internet Protocol
83	VINES	VINES

Internet Control Message Protocol Header

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

Type	Code	Checksum
Data (variable length)		

User Datagram Protocol Header

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 Bits

Source Port	Destination Port
Length	Checksum
Data	

Field Description

Type: Type of ICMP message. Examples include:

- 0 = Echo Reply
- 3 = Destination Unreachable
- 4 = Source Quench
- 5 = Redirect
- 8 = Echo
- 11 = Time Exceeded
- 12 = Parameter Problem
- 13 = Timestamp
- 14 = Timestamp Reply
- !7 = Adress Mask Request
- 18 = Address Mask Reply

Code: Parameters of the message that can be briefly encoded.

Checksum: Checksum of the ICMP message.

Data: Additional information related to the message.

Variable Length Subnet Mask Table

X.X.X.128 /25			
Subnet	Network	Hosts	Broadcast
subnet 1	.0	.1 - .126	.127
subnet 2	.128	.129 - .254	.255

Subnet	Hex Mask	Decimal		
255.255.255.0	FF-FF-FF-00	/24	1	254
255.255.255.12	FF-FF-FF-80	/25	2	126
255.255.255.19	FF-FF-FF-C0	/26	4	62
255.255.255.22	FF-FF-FF-E0	/27	8	30
255.255.255.24	FF-FF-FF-F0	/28	16	14
255.255.255.24	FF-FF-FF-F8	/29	32	6
255.255.255.25	FF-FF-FF-FC	/30	64	2

Class	Lowest Address	Highest Address
A	0.1.1.0	126.0.0.0
B	128.0.0.0	191.255.0.0
C	192.0.1.0	223.255.255.0
D	224.0.0.0	239.255.255.255
E	240.0.0.0	247.255.255.255

X.X.X.192 /26			
Subnet	Network	Hosts	Broadcast
subnet 1	.0	.1 - .62	.63
subnet 2	.64	.65 - .126	.127
subnet 3	.128	.129 - .190	.191
subnet 4	.192	.193 - .254	.255

X.X.X.248 /29			
Subnet	Network	Hosts	Broadcast
subnet 1	.0	.1 - .6	.7
subnet 2	.8	.9 - .14	.15
subnet 3	.16	.17 - .22	.23
subnet 4	.24	.25 - .30	.31
subnet 5	.32	.33 - .38	.39
subnet 6	.40	.41 - .46	.47
subnet 7	.48	.49 - .54	.55
subnet 8	.56	.57 - .62	.63
subnet 9	.64	.65 - .70	.71
subnet 10	.72	.73 - .78	.79
subnet 11	.80	.81 - .86	.87
subnet 12	.88	.89 - .94	.95
subnet 13	.96	.97 - .102	.103
subnet 14	.104	.105 - .110	.111
subnet 15	.112	.113 - .118	.119
subnet 16	.120	.121 - .126	.127
subnet 17	.128	.129 - .134	.135
subnet 18	.136	.137 - .142	.143
subnet 19	.144	.145 - .150	.151
subnet 20	.152	.153 - .158	.159
subnet 21	.160	.161 - .166	.167
subnet 22	.168	.169 - .174	.175
subnet 23	.176	.177 - .182	.183
subnet 24	.184	.185 - .190	.191
subnet 25	.192	.193 - .198	.199
subnet 26	.200	.201 - .206	.207
subnet 27	.208	.209 - .214	.215
subnet 28	.216	.217 - .222	.223
subnet 29	.224	.225 - .230	.231
subnet 30	.232	.233 - .238	.239
subnet 31	.240	.241 - .246	.247
subnet 32	.248	.249 - .254	.255

X.X.X.252 /30							
Subnet	Network	Hosts	Broadcast	Subnet	Network	Hosts	Broadcast
subnet 1	.0	.1 - .2	.3	subnet 33	.128	.129 - .130	.131
subnet 2	.4	.5 - .6	.7	subnet 34	.132	.133 - .134	.135
subnet 3	.8	.9 - .10	.11	subnet 35	.136	.137 - .138	.139
subnet 4	.12	.13 - .14	.15	subnet 36	.140	.141 - .142	.143
subnet 5	.16	.17 - .18	.19	subnet 37	.144	.145 - .146	.147
subnet 6	.20	.21 - .22	.23	subnet 38	.148	.149 - .150	.151
subnet 7	.24	.25 - .26	.27	subnet 39	.152	.153 - .154	.155
subnet 8	.28	.29 - .30	.31	subnet 40	.156	.157 - .158	.159
subnet 9	.32	.33 - .34	.35	subnet 41	.160	.161 - .162	.163
subnet 10	.36	.37 - .38	.39	subnet 42	.164	.165 - .166	.167
subnet 11	.40	.41 - .42	.43	subnet 43	.168	.169 - .170	.171
subnet 12	.44	.45 - .46	.47	subnet 44	.172	.173 - .174	.175
subnet 13	.48	.49 - .50	.51	subnet 45	.176	.177 - .178	.179
subnet 14	.52	.53 - .54	.55	subnet 46	.180	.181 - .182	.183
subnet 15	.56	.57 - .58	.59	subnet 47	.184	.185 - .186	.187
subnet 16	.60	.61 - .62	.63	subnet 48	.188	.189 - .190	.191
subnet 17	.64	.65 - .66	.67	subnet 49	.192	.193 - .194	.195
subnet 18	.68	.69 - .70	.71	subnet 50	.196	.197 - .198	.199
subnet 19	.72	.73 - .74	.75	subnet 51	.200	.201 - .202	.203
subnet 20	.76	.77 - .78	.79	subnet 52	.204	.205 - .206	.207
subnet 21	.80	.81 - .82	.83	subnet 53	.208	.209 - .210	.211
subnet 22	.84	.85 - .86	.87	subnet 54	.212	.213 - .214	.215
subnet 23	.88	.89 - .90	.91	subnet 55	.216	.217 - .218	.219
subnet 24	.92	.93 - .94	.95	subnet 56	.220	.221 - .222	.223
subnet 25	.96	.97 - .98	.99	subnet 57	.224	.225 - .226	.227
subnet 26	.100	.101 - .102	.103	subnet 58	.228	.229 - .230	.231
subnet 27	.104	.105 - .106	.107	subnet 59	.232	.233 - .234	.235
subnet 28	.108	.109 - .110	.111	subnet 60	.236	.237 - .238	.239
subnet 29	.112	.113 - .114	.115	subnet 61	.240	.241 - .242	.243
subnet 30	.116	.117 - .118	.119	subnet 62	.244	.245 - .246	.247
subnet 31	.120	.121 - .122	.123	subnet 63	.248	.249 - .250	.251
subnet 32	.124	.125 - .126	.127	subnet 64	.252	.253 - .254	.255

X.X.X.240 /28			
Subnet	Network	Hosts	Broadcast
subnet 1	.0	.1 - .14	.15
subnet 2	.16	.17 - .30	.31
subnet 3	.32	.33 - .46	.47
subnet 4	.48	.49 - .62	.63
subnet 5	.64	.65 - .78	.79
subnet 6	.80	.82 - .94	.95
subnet 7	.96	.97 - .110	.111
subnet 8	.112	.113 - .126	.127
subnet 9	.128	.129 - .142	.143
subnet 10	.144	.145 - .158	.159
subnet 11	.160	.161 - .174	.175
subnet 12	.176	.177 - .190	.191
subnet 13	.192	.193 - .206	.207
subnet 14	.208	.209 - .222	.223
subnet 15	.224	.225 - .238	.239
subnet 16	.240	.241 - .254	.255

Note:

Network and a subnet that have the same addresses. For example, if network 122.22.0.0 is subnetted as 255.255.255.0, subnet zero would be written as 122.22.0.0. This is identical to the network address.

RFC	Subject
768	User Datagram Protocol (UDP)
791	Internet Protocol (IP)
792	Internet Control Message Protocol (ICMP)
793	Transmission Control Protocol (TCP)
821	Simple Mail Transfer Protocol (SMTP)
826	An Ethernet Address Resolution Protocol (ARP)
854	TELNET Protocol Specification
903	A Reverse Address Resolution Protocol (RARP)
959	File Transfer Protocol (FTP)
1001	NETBIOS Service on a TCP/UDP Transport
1034	Domain Names - Concepts and Facilities
1042	Transmission of IP Datagrams over IEEE 802 Networks
1055	Serial Line Internet Protocol (SLIP)
1058	Routing Information Protocol (RIP)
1122	Requirements for Internet Hosts - Communication Layers
1157	A Simple Management Network Protocol (SNMP)
1213	Management Information Base: MIB-II
1390	Transmission of IP and ARP over FDDI Networks
1490	Multiprotocol Interconnect over Frame Relay
1583	OSPF Version 2
1661	The Point-to-Point Protocol (PPP)
1700	Assigned Numbers
2460	IPv6 Specification
1901	Community-based SNMPv2
2200	Internet Official Protocol Standards
2271	SNMP version 3

TELNET Options

Option	Name
0	Binary Transmission
1	Echo
2	Reconnection
3	Suppress Go Ahead
4	Approx Message Size Negotiation
5	Status
6	Timing Mark
7	Remote Controlled Trans and Echo
8	Output line Width
9	Output Page Size
10	Output Carriage-Return Disposition
11	Output Horizontal Tab Stops
12	Putput Horizontal Tab Disposition
13	Output Formfeed Disposition
14	Output Vertical Tabstops
15	Output Vertical Tab Disposition
16	Output Linefeed Disposition
17	Extended ASCII
18	Logout
19	Byte Macro
20	Data Entry Terminal
21	SUPDUP
22	SUPDUP output
23	Send location
24	Terminal Type
25	End of Record
26	TACACS User Identification
27	Output Marking
28	Terminal Location Number
29	Telnet 3270 Regime
30	X.3 PAD
31	Negotiate About Window Size
32	Terminal Speed
33	Remote Flow Control
34	Linemode
35	X Display Location
255	Extended-Options-List

See RFCs 1011 and 1123 for further details

File Transfer Protocol Commands

Access Control Commands	Service Commands
User Name (USER)	Retrieve (RETR)
Password (PASS)	Store (STOR)
Account (ACCT)	Append (APPE)
Change working Directory (CWD)	Allocate (ALLO)
Change to Parent Directory (CDUP)	Restart (REST)
Structure Mount (SMNT)	Rename from (RNFR)
Reinitialize (REIN)	Rename to (RNTO)
Logout (QUIT)	Abort (ABOR)
	Delete (DELE)
	Remove Directory (RMD)
	Make Directory (MKD)
	Print Working Directory (PWD)
	List (LIST)
	Name List (NLST)
	System (SYST)
	Status (STAT)
	Help (HELP)
	No operation (NOOP)

Transfer Parameter Commands

Data Port (PORT)
Passive (PASV)
Representation Type (TYPE)
File Structure (STRU)
Transfer Mode (MODE)

See RFC 959 for specific command usage

Simple Mail Transfer Protocol Commands

```

HELO <SP> <domain> <CRLF>
MAIL <SP> FROM: <reverse-path> <CRLF>
RCPT <SP> TO: <forward-path> <CRLF>
DATA <CRLF>
RSET <CRLF>
SEND <SP> FROM: <reverse-path> <CRLF>
SOML <SP> FROM: <reverse-path> <CRLF>
SAML <SP> FROM: <reverse-path> <CRLF>
VERFY <SP> <string> <CRLF>
EXPN <SP> <string> <CRLF>
HELP [<SP> <string>] <CRLF>
NOOP <CLRF>
QUIT <CLRF>
TURN <CLRF>
    
```

<SP> : space character
 <CRLF> : carriage return, line feed characters

See RFC 821 for further details