Packet Analysis Reference Guide v3.0

Headers, Tables, Tools and Notes

Compiled & Written by
James Summers, CISSP - ISSAP, ISSMP, CISA
GCIA, GCIH, G7799, GAWN-C, GSEC, GFSP, GPCI
CCNA, CCDA, CS-CFWS, CS-CISecS, 4001 Rec, MCSE
james@vsnry.com

This page purposely left blank

Table of Contents

Subnet Breakdown (Binary to Decimal)

CIDR	Octet	Mask
/8	1	255
/9	2	128
/10	2	192
/11	2	224
/12	2	240
/13	2	248
/14	2	252
/15	2	254
/16	2	255
/17	3	128
/18	3	192
/19	3	224
/20	3	240
/21	3	248
/22	3	252
/23	3	254
/24	3	255
/25	4	128
/26	4	192
/27	4	224
/28	4	240
/29	4	248
/30	4	252
/32	4	255

Classes	
A	0
B	10
C	110
D	1110

							192 (2)					128 (1)							
												192 (2)					192 (2)		
				00000000	0		01000000	64			10000000	128			11000000	192			
				00000001	1		01000001	65			10000001	129			11000001	193			
				00000010	2		01000010	66			10000010	130			11000010	194			
			252	00000011	3		01000011	67			10000011	131			11000011	195			
			(6)	00000100	4		01000100	68			10000100	132			11000100	196			
				00000101	5		01000101	69			10000101	133			11000101	197			
				00000110	6		01000110	70			10000110	134			11000110	198			
		248	252	00000111	7		01000111	71			10000111	135			11000111	199			
		(5)	(6)	00001000	8		01001000	72			10001000	136			11001000	200			
				00001001	9		01001001	73			10001001	137			11001001	201			
				00001010	10		01001010	74			10001010	138			11001010	202			
			252	00001011	11		01001011	75			10001011	139			11001011	203			
			(6)	00001100	12		01001100	76			10001100	140			11001100	204			
				00001101	13		01001101	77			10001101	141			11001101	205			
				00001110	14		01001110	78			10001110	142			11001110	206			
		248	252	00001111	15		01001111	79			10001111	143			11001111	207			
		(5)	(6)	00010000	16		01010000	80			10010000	144			11010000	208			
				00010001	17		01010001	81			10010001	145			11010001	209			
				00010010	18		01010010	82			10010010	146			11010010	210			
			252	00010011	19		01010011	83			10010011	147			11010011	211			
			(6)	00010100	20		01010100	84			10010100	148			11010100	212			
				00010101	21		01010101	85			10010101	149			11010101	213			
				00010110	22		01010110	86			10010110	150			11010110	214			
		248	252	00010111	23		01010111	87			10010111	151			11010111	215			
		(5)	(6)	00011000	24		01011000	88			10011000	152			11011000	216			
				00011001	25		01011001	89			10011001	153			11011001	217			
				00011010	26		01011010	90			10011010	154			11011010	218			
			252	00011011	27		01011011	91			10011011	155			11011011	219			
			(6)	00011100	28		01011100	92			10011100	156			11011100	220			
				00011101	29		01011101	93			10011101	157			11011101	221			
				00011110	30		01011110	94			10011110	158			11011110	222			
224	240	248	252	00011111	31		01011111	95			10011111	159			11011111	223			
(3)	(4)	(5)	(6)	00100000	32		01100000	96			10100000	160			11100000	224			
				00100001	33		01100001	97			10100001	161			11100001	225			
				00100010	34		01100010	98			10100010	162			11100010	226			
			252	00100011	35		01100011	99			10100011	163			11100011	227			
			(6)	00100100	36		01100100	100			10100100	164			11100100	228			
				00100101	37		01100101	101			10100101	165			11100101	229			
				00100110	38		01100110	102			10100110	166			11100110	230			
		248	252	00100111	39		01100111	103			10100111	167			11100111	231			
		(5)	(6)	00101000	40		01101000	104			10101000	168			11101000	232			
				00101001	41		01101001	105			10101001	169			11101001	233			
				00101010	42		01101010	106			10101010	170			11101010	234			
			252	00101011	43		01101011	107			10101011	171			11101011	235			
			(6)	00101100	44		01101100	108			10101100	172			11101100	236			
				00101101	45		01101101	109			10101101	173			11101101	237			
				00101110	46		01101110	110			10101110	174			11101110	238			
	240	248	252	00101111	47		01101111	111			10101111	175			11101111	239			
	(4)	(5)	(6)	00110000	48		01110000	112			10110000	176			11110000	240			
				00110001	49		01110001	113			10110001	177			11110001	241			
				00110010	50		01110010	114			10110010	178			11110010	242			
			252	00110011	51		01110011	115			10110011	179			11110011	243			
			(6)	00110100	52		01110100	116			10110100	180			11110100	244			
				00110101	53		01110101	117			10110101	181			11110101	245			
				00110110	54		01110110	118			10110110	182			11110110	246			
		248	252	00110111	55		01110111	119			10110111	183			11110111	247			
		(5)	(6)	00111000	56		01111000	120			10111000	184			11111000	248			
				00111001	57		01111001	121			10111001	185			11111001	249			
				00111010	58		01111010	122			10111010	186			11111010	250			
			252	00111011	59		01111011	123			10111011	187			11111011	251			
			(6)	00111100	60		01111100	124			10111100	188			11111100	252			
				00111101	61		01111101	125			10111101	189			11111101	253			
				00111110	62		01111110	126			10111110	190			11111110	254			
				00111111	63		01111111	127			10111111	191			11111111	255			

Subnet Breakdown (Binary to Hexadecimal)

						192	(2)			128	(1)				
										192	(2)			192	(2)
			00000000	00		01000000	40		10000000	80		11000000	C0
			00000001	01		01000001	41		10000001	81		11000001	C1
			00000010	02		01000010	42		10000010	82		11000010	C2
		252	00000011	03		01000011	43		10000011	83		11000011	C3
		(6)	00000100	04		01000100	44		10000100	84		11000100	C4
			00000101	05		01000101	45		10000101	85		11000101	C5
			00000110	06		01000110	46		10000110	86		11000110	C6
	248	252	00000111	07		01000111	47		10000111	87		11000111	C7
	(5)	(6)	00001000	08		01001000	48		10001000	88		11001000	C8
			00001001	09		01001001	49		10001001	89		11001001	C9
			00001010	0A		01001010	4A		10001010	8A		11001010	CA
		252	00001011	0B		01001011	4B		10001011	8B		11001011	CB
		(6)	00001100	0C		01001100	4C		10001100	8C		11001100	CC
			00001101	0D		01001101	4D		10001101	8D		11001101	CD
			00001110	0E		01001110	4E		10001110	8E		11001110	CE
	240	248	252	00001111	0F		01001111	4F		10001111	8F		11001111	CF
	(4)	(5)	(6)	00010000	10		01010000	50		10010000	90		11010000	D0
				00010001	11		01010001	51		10010001	91		11010001	D1
				00010010	12		01010010	52		10010010	92		11010010	D2
			252	00010011	13		01010011	53		10010011	93		11010011	D3
			(6)	00010100	14		01010100	54		10010100	94		11010100	D4
				00010101	15		01010101	55		10010101	95		11010101	D5
				00010110	16		01010110	56		10010110	96		11010110	D6
		248	252	00010111	17		01010111	57		10010111	97		11010111	D7
		(5)	(6)	00011000	18		01011000	58		10011000	98		11011000	D8
				00011001	19		01011001	59		10011001	99		11011001	D9
				00011010	1A		01011010	5A		10011010	9A		11011010	DA
			252	00011011	1B		01011011	5B		10011011	9B		11011011	DB
			(6)	00011100	1C		01011100	5C		10011100	9C		11011100	DC
				00011101	1D		01011101	5D		10011101	9D		11011101	DD
				00011110	1E		01011110	5E		10011110	9E		11011110	DE
224	240	248	252	00011111	1F		01011111	5F		10011111	9F		11011111	DF
(3)	(4)	(5)	(6)	00100000	20		01100000	60		10100000	A0		11100000	E0
				00100001	21		01100001	61		10100001	A1		11100001	E1
				00100010	22		01100010	62		10100010	A2		11100010	E2
			252	00100011	23		01100011	63		10100011	A3		11100011	E3
			(6)	00100100	24		01100100	64		10100100	A4		11100100	E4
				00100101	25		01100101	65		10100101	A5		11100101	E5
				00100110	26		01100110	66		10100110	A6		11100110	E6
		248	252	00100111	27		01100111	67		10100111	A7		11100111	E7
		(5)	(6)	00101000	28		01101000	68		10101000	A8		11101000	E8
				00101001	29		01101001	69		10101001	A9		11101001	E9
				00101010	2A		01101010	6A		10101010	AA		11101010	EA
			252	00101011	2B		01101011	6B		10101011	AB		11101011	EB
			(6)	00101100	2C		01101100	6C		10101100	AC		11101100	EC
				00101101	2D		01101101	6D		10101101	AD		11101101	ED
				00101110	2E		01101110	6E		10101110	AE		11101110	EE
	240	248	252	00101111	2F		01101111	6F		10101111	AF		11101111	EF
	(4)	(5)	(6)	00110000	30		01110000	70		10110000	B0		11110000	F0
				00110001	31		01110001	71		10110001	B1		11110001	F1
				00110010	32		01110010	72		10110010	B2		11110010	F2
			252	00110011	33		01110011	73		10110011	B3		11110011	F3
			(6)	00110100	34		01110100	74		10110100	B4		11110100	F4
				00110101	35		01110101	75		10110101	B5		11110101	F5
				00110110	36		01110110	76		10110110	B6		11110110	F6
		248	252	00110111	37		01110111	77		10110111	B7		11110111	F7
		(5)	(6)	00111000	38		01111000	78		10111000	B8		11111000	F8
				00111001	39		01111001	79		10111001	B9		11111001	F9
				00111010	3A		01111010	7A		10111010	BA		11111010	FA
			252	00111011	3B		01111011	7B		10111011	BB		11111011	FB
			(6)	00111100	3C		01111100	7C		10111100	BC		11111100	FC
				00111101	3D		01111101	7D		10111101	BD		11111101	FD
				00111110	3E		01111110	7E		10111110	BE		11111110	FE
				00111111	3F		01111111	7F		10111111	BF		11111111	FF

Equations

TCP & IP Equations

TCP Options Length =

(TCP Header Length * 4 byte multiplier) - (Minimum TCP Header Length * 4 byte multiplier)
(TCP Header Length * 4 byte multiplier) - 20 bytes

Length of IP Packet Payload =

IP total Length - ((IP Header Length * 4 byte multiplier) + (TCP Header Length * 4 byte multiplier))

Logic Equations

1 AND 1 is 1	1 OR 1 is 1	1 XOR 1 is 0
1 AND 0 is 0	1 OR 0 is 1	1 XOR 0 is 1
0 AND 1 is 0	0 OR 1 is 1	0 XOR 1 is 1
0 AND 0 is 0	0 OR 0 is 0	0 XOR 0 is 0

Subneting Equations

Number of hosts on a subnet =

2^n-2

Where n is the number of bits in the ip address / subnet dedicated to the host
Remember the -2 is because host bits of all 0's is the network address and all 1's is the broadcast address for that subnet

Number of subnets that can be created from n subnet bits =

2^n

Where n is the number of bits dedicated to the subnet
Note: This assume you have something like "ip subnet zero" on your network device. Otherwise you have to - 2 from your total where all the subnet bits are 0's or 1's

Number of host bits needed for X hosts to be on the same subnet =

$$\frac{\ln(X+2)}{\ln 2}$$

Where X is the number of hosts required on the subnet.
Note: **ln** is the nature log. **Round up to the nearest whole number.**

Number of network and subnet bits needed for X hosts to be on the same subnet =

$$32 - \frac{\ln(X+2)}{\ln 2}$$

Where X is the number of hosts required on the subnet.
Note: **ln** is the nature log. **Round up to the nearest whole number.**

Determining the network address from IP and subnet mask by doing a logical AND on the IP with the subnet mask

00000011 10101010 01010101 11111110	10.170.85.254 is the IP address
11111111 11111111 11111111 11110000	255.255.255.240 is the subnet mask
00000011 10101010 01010101 11110000	10.170.85.240 is the network address for the subnet

Converting Binary or Hexadecimal to Decimal

The equation: $(b^p * n_p) + \ldots + (b^1 * n_1) + (b^0 * n_0)$

b is the base (b = 2 for binary and b = 16 for hexadecimal)
p is the position of the number (counting starts from the rightmost character as 0)
n is the number in the p^{th} position

Examples:

Convert from binary to decimal 10101111

$(2^7 * 1) + (2^6 * 0) + (2^5 * 1) + (2^4 * 0) + (2^3 * 1) + (2^2 * 1) + (2^1 * 1) + (2^0 * 1)$

$128 + 0 + 32 + 0 + 8 + 4 + 2 + 1 =$ **175**

Convert from hexadecimal to decimal AC89

$(16^3 * A) + (16^2 * C) + (16^1 * 8) + (16^0 * 9)$

This is where you need to know hex A is decimal 10 and hex C is decimal 12

$(16^3 * 10) + (16^2 * 12) + (16^1 * 8) + (16^0 * 9)$

$(4096 * 10) + (256 * 12) + (16 * 8) + (1 * 9)$

$40960 + 3072 + 128 + 9 =$ **44169**

Header Offset Shortcuts

Field	Length (bits)	TCPDUMP Filter	Notes
IP Header Length	4	ip[0] &0x0F	Remember to use a 4 byte multiplier to find header length in bytes
IP Packet Length	16	ip[2:2]	There is no multipler for this length field
IP TTL	8	ip[8]	
IP Protocol	8	ip[9]	

Dec	Hex	Proto	Dec	Hex	Proto	Dec	Hex	Proto
1	0x01	ICMP	9	0x09	IGRP	50	0x32	ESP
2	0x02	IGMP	17	0x11	UDP	51	0x33	AH
6	0x06	TCP	47	0x2F	GRE	88	0x58	EIGRP

IP Address - Src	32	ip[12:4]	
IP Address - Dst	32	ip[16:4]	
IP Fragmentation	flag=3	ip[6] &0x20 = 0x20	More Fragment bit is set.
	offset=13	ip[6:2] &0x1fff != 0x0000	Fragment offset in not 0
ICMP Type	8	icmp[0]	
ICMP Code	8	icmp[1]	
TCP Src Port	16	tcp[0:2]	
TCP Dst Port	16	tcp[2:2]	
TCP Header Length	4	tcp[12] &0x0F	Remember to use a 4 byte multiplier to find header length in bytes
TCP Flags	8	tcp[13]	
TCP Windows Size	16	tcp[14:2]	
UDP Src Port	16	udp[0:2]	
UDP Dst Port	16	udp[2:2]	
UDP Header Length	16	upd[4:2]	There is no multipler for this length field

OSI vs. TCP/IP

OSI			TCP/IP	
	Application	7	Application	
	Presentation	6		
	Session	5		
	Transport	4	Transport (TCP)	
	Network	3	Internet (Network) (IP)	
	Data Link	2	Network Access (Data Link)	
	Physical	1		

Application Layer (Layer 7)

Determines the network services required.

Examples: DNS, FTP, LDP, Telent, TFTP, SMTP and WWW

Presentation Layer (Layer 6)

Presents data to the application layer. Essentially functions as a translator from computer to human readable form.

Examples: HTTP, TIFF, JPEG, MIDI and MPEG

Session Layer (Layer 5)

Establishes and maintains the connection between systems and formats the data for transfer between nodes.

Examples: NFS, SQL, RPC

Transport Layer (Layer 4)

Defines how to address physical locations, how to make connections between nodes, and how to handle the network of messages. This layer is responsible for **end-to end** integrity and control of the session and handles the sequencing of packets.

Examples: TCP, UDP, SPX

Network Layer (Layer 3)

Defines how packets of data are routed between end systems over interconnected networks. Routing error detection, and control of node data traffic are managed at this layer.

Examples: IP, OSPF, ICMP, RIP

Data Link Layer (Layer 2)

Defines the protocols that computers use in order to access the network for transmitting and receiving messages.
Has two sub layers: *Logical Link Control* and *Media Access Control*.

Examples: ARP, SLIP, PPP

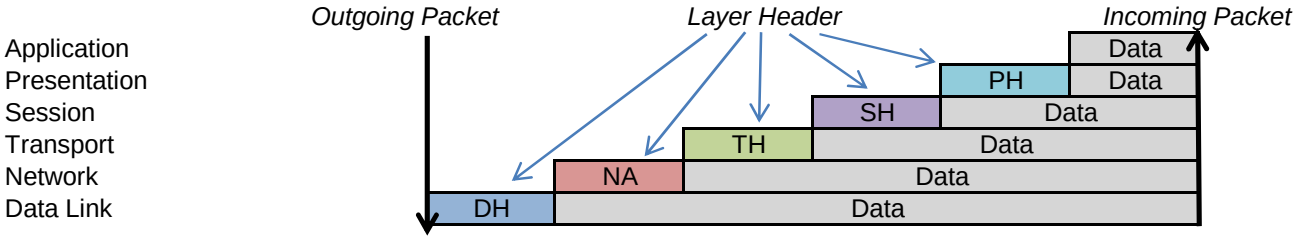
Physical Layer (Layer 1)

Defines the physical connection (RJ48, BNC, HSSI, etc…) between a host and a network and converts the bits into voltages or light impulses for transmission.

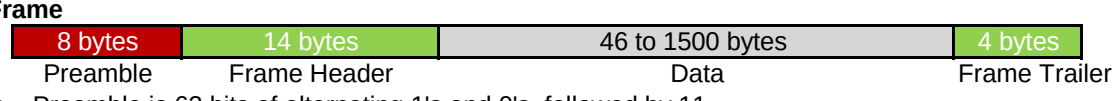
Examples: HSSI, X.21, EIA/TIA-232 and EIA/TIA-449

Encapsulation (In reverse is demultiplexing.)

For outgoing packets, the data + header from an upper layer is packaged into the data of the layer below it. For incomming packets, the layer header information is strip off and used to determine where the remaining data is to go.



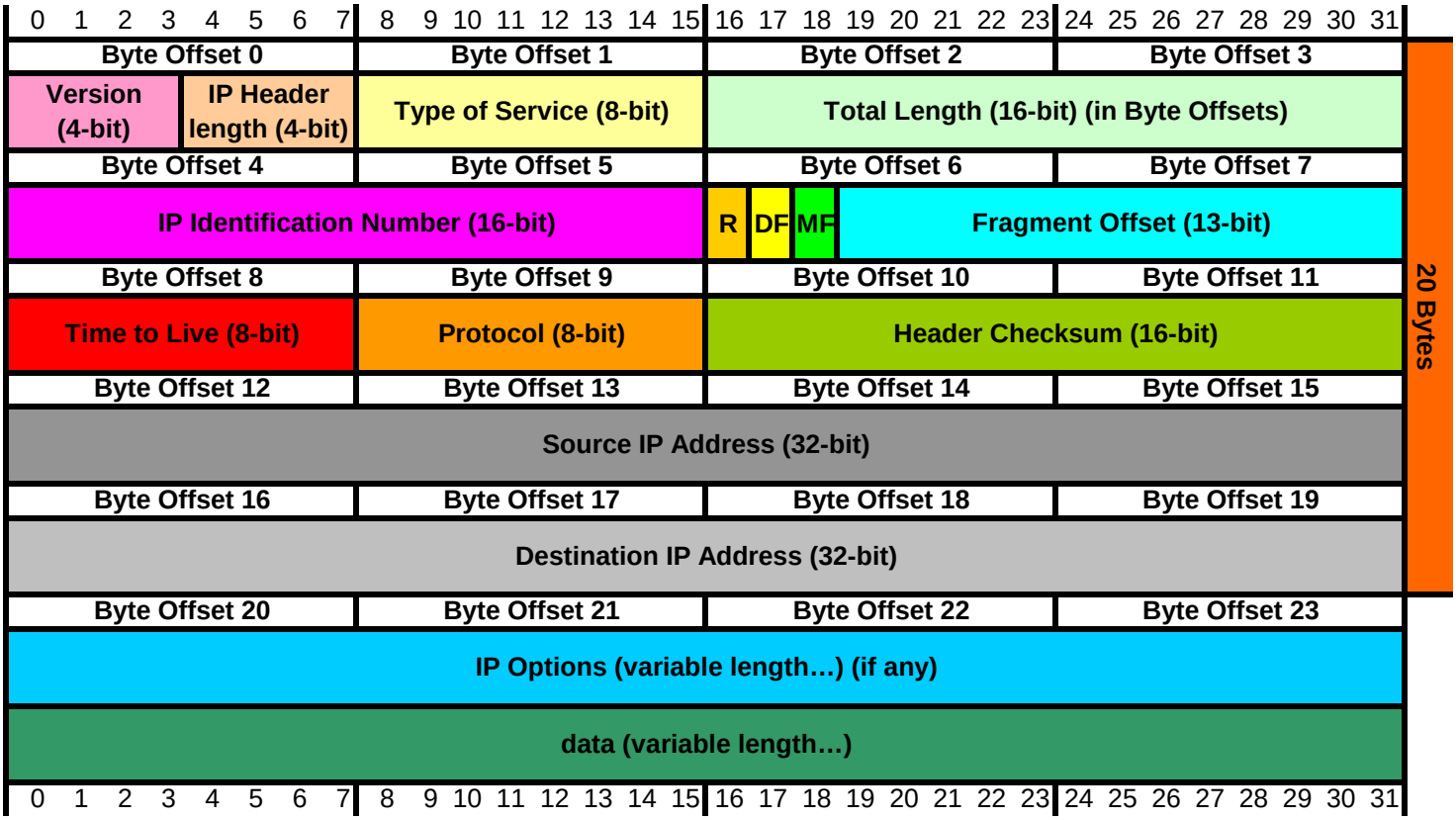
Ethernet Frame



Manchester encoding - Preamble is 62 bits of alternating 1's and 0's. followed by 11.

TCP vs. UDP

IPv4 Header (RFC 791)



IP Version Number

Valid values are: 4 for IP version 4 6 for IP version 6

IP Header Length (4 byte multiplier)

Number of 32-bit words in IP header minimum value 5 (5 x 4 = 20 bytes) maximum value 15 (15 x 4 = 60 bytes)

Type of Service (Used by gateways as a QoS type field) (Most OS's default to 0)

If the first 3 high order bits are 1's, then possible it came from busy router that had to set tags to get through a backlog

Total Length (No multiplier)

Number of bytes in packet maximum length = 65,535

IP Identification Number

Uniquely identifies every datagram sent by host, value typically incremented by 1 (AKA Fragment ID)

Flags

R is reserved and must be set to 0

D is Don't Fragment Flag 1=Don't Fragment 0=Can Fragment

MF is More Fragments 1=More Fragments 0=No Fragment or no more Fragments

(frag x:y@z where x is the fragment ID, y is # of bytes (must be divisible by 8) and z is the fragment offset)

(In Ethernet the MTU 1500 should see middle fragments of size 1480 (1480 data + 20 ip header = 1500)

Fragment Offset (8 byte multiplier) (Measured in units of 64 bits) (Max fragment offset 65528 (8191*8))

Position of this fragment in the original datagram value is multiplied by 8 to get bytes

Time To Live

IP Protocol

D	Hex		D	Hex		D	Hex		D	Hex	
1	0x01	ICMP	9	0x09	IGRP	47	0x2F	GRE	88	0x58	EIGRP
2	0x02	IGMP	17	0x11	UDP	50	0x32	ESP	89	0x59	OSPF
6	0x06	TCP	47	0x2F	GRE	51	0x33	AH			

Header Checksum

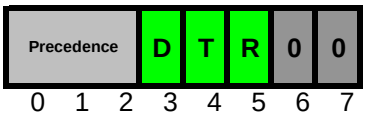
Covers IP header only Validated along the path from source to destination

Options (0-40 bytes; 1st @ 20th byte offset; padded 4-byte boundary) (Processed by each router as packet passes)

D	Hex		D	Hex	
0	0x00	End of Option list	68	0x44	Timestamp
1	0x01	No operation (pad)	131	0x83	Loose source route (security risk)
7	0x07	Record Route (security risk)	137	0x89	Strict source route (security risk)

IPv4 Header (cont.)

Type of Service (Used by gateways as a QoS type field) (Most OS's default to 0)



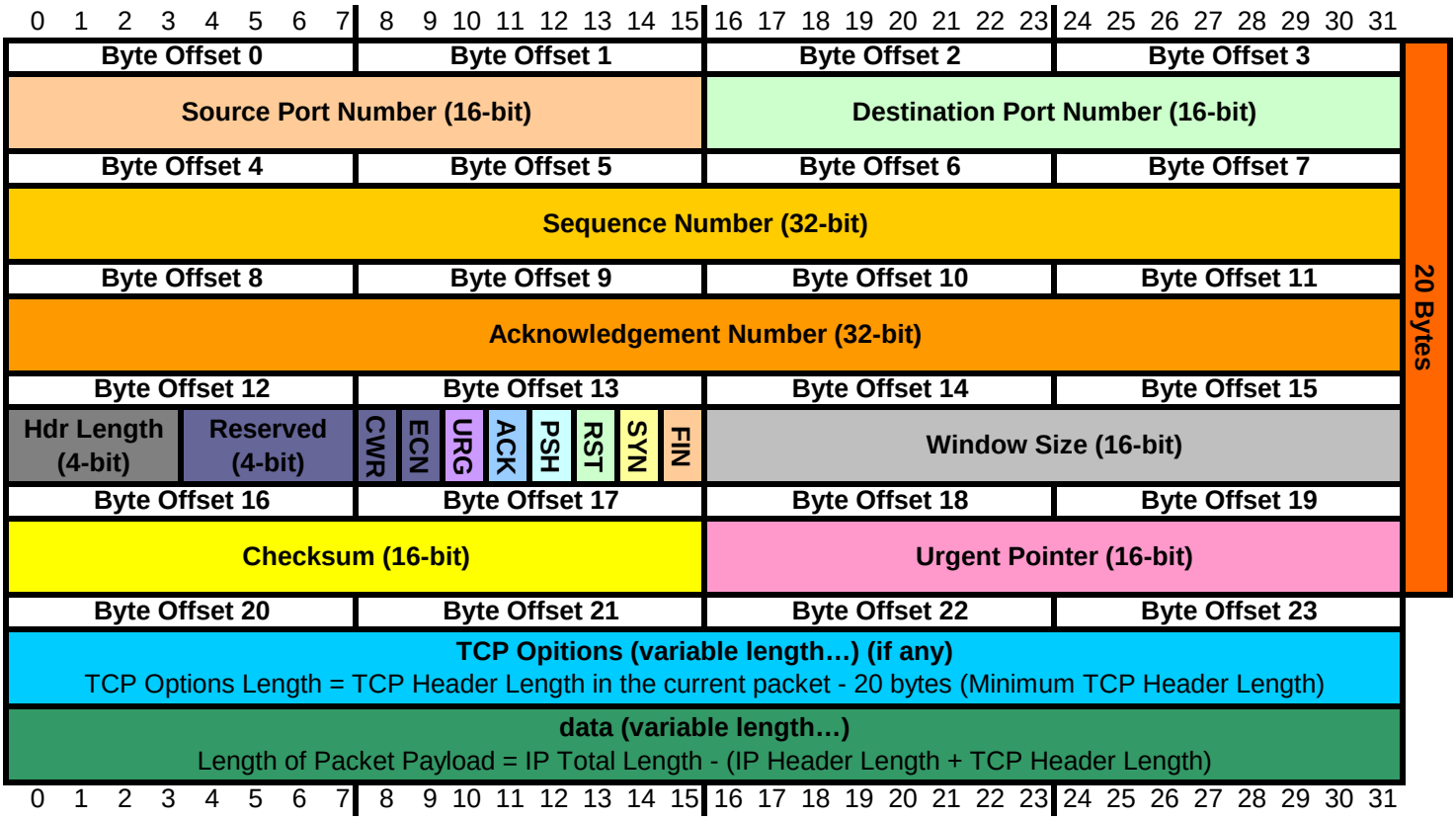
Bit 0 - 2 Precedence
Bit 3 0 = Normal Delay 1 = Low Delay
Bit 4 0 = Normal Throughput 1 = High Throughput
Bit 5 0 = Normal Reliability 1 = High Reliability
Bit 6 & 7 Reserved for future use (Always set to 0)

Precedence			
1	1	1	Network Control
1	1	0	Internetwork Control
1	0	1	CRITIC / ECP
1	0	0	Flash Override
0	1	1	Flash
0	1	0	Immediate
0	0	1	Priority
0	0	0	Routine

Telnet

Protocol	**TOS Value**
Telnet	1000
FTP Control	1000
FTP Data	0100
TFTP	1000
SMTP Command	1000
SMTP Data	0100
DNS UDP Query	1000
DNS TCP Query	0000
DNE Zone Transfer	0100
NNTP	
ICMP - Erros	0000
ICMP - Requests	0000
ICMP - Responces	Same as request
Any IGP	0010
EGP	0000
SNMP	0010
BOOTP	0000

Transmission Control Protocol - TCP Header (RFC 793)



Common Port Numbers

D	Hex		D	Hex		D	Hex		D	Hex	
7	0x07	echo	25	0x19	smtp	119	0x77	nntp	389	0x185	ldap
19	0x13	chargen	53	0x35	domain	137	0x89	netbios-ns	443	0x1BB	https (ssl)
20	0x14	ftp-data	79	0x4F	finger	139	0x8B	netbios-ssn	445	0x1BD	ms-ds
21	0x15	ftp-control	80	0x50	http	143	0x8F	imap			
22	0x16	ssh	110	0x6E	pop3	179	0xB3	bgp			

Sequence Number
32-bit number uniquely identifies initial byte of segment data.

Acknowledgement Number
Represents next byte of data receiving host expects: (last received sequence number + 1)

Header Length (4 byte multiplier)
Number of 32-bit words in TCP header minimum value 5 (5x4=20bytes) maximum value 15 (5x15=60bytes)

Reserved 4 bits set to 0

Congestion Window Reduced (CWR)
Set to 0 unless ECN is used. (1 = sender cuts congestion window in half)

Explicit Congestion Notification Echo (ECN)
Set to 0 unless ECN is used. (1 = receiver cuts congestion window in half)

Flags
URG = Urgent ACK = Acknowledgment PSH = Push RST = Reset SYN = Syncronize
FIN = Finish (Note: Push means don't buffer data but push it to be processes as soon as it comes in.)

Window Size
Acts as flow control. Window size dynamically changes as data is received. A 0 window size tells src host to wait.

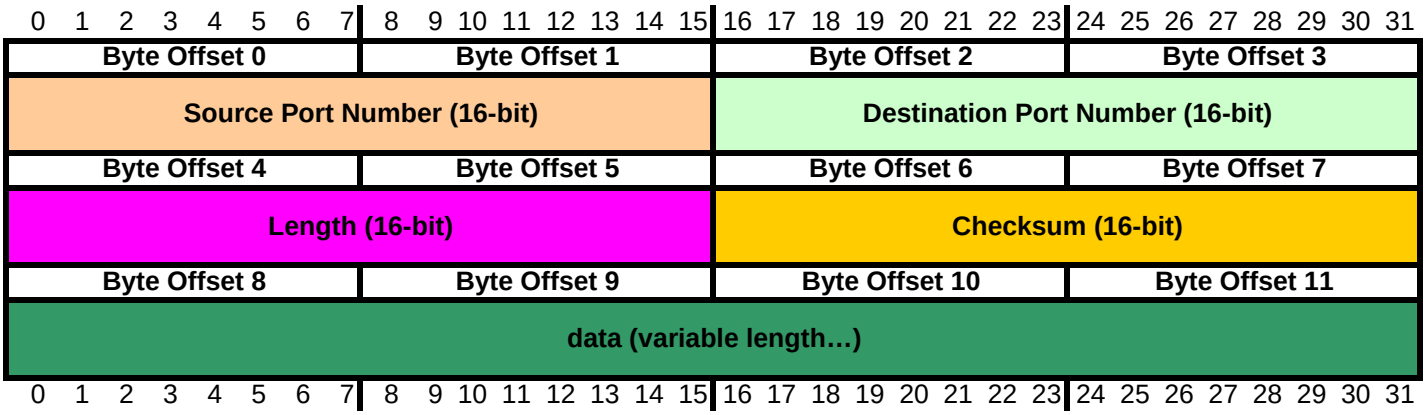
Checksum
Covers psedo header (IP Header source and destinstation addresses, the protocol and the computed TCP length (the TCP header length the and data length in octets)) and the TCP header

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

Options

0 End of Options List	2 Maximum segment size	4 Selective ACK ok
1 No Operation (pad)	3 Window scale	8 Timestamp

User Datagram Protocol - UDP Header (RFC 768)



Common Port Numbers

D	Hex	Protocol
7	0x07	echo
19	0x13	chargen
37	0x25	time
53	0x35	domain
67	0x43	bootps
68	0x44	bootpc

D	Hex	Protocol
69	0x45	tftp
123	0x7B	ntp
137	0x89	netbios-ns
138	0x8A	netbios-dgm
161	0xA1	snmp
162	0xA2	snmp-trap

D	Hex	Protocol
500	0x1F4	isakmp
514	0x202	syslog
520	0x208	rip
33434	829A	traceroute

Length

Number of bytes in the entire datagram including header

minimum value 8 bytes

(Which is the length of just the header with no data)

maximum value 65515 bytes (or 65507 bytes of UDP data)

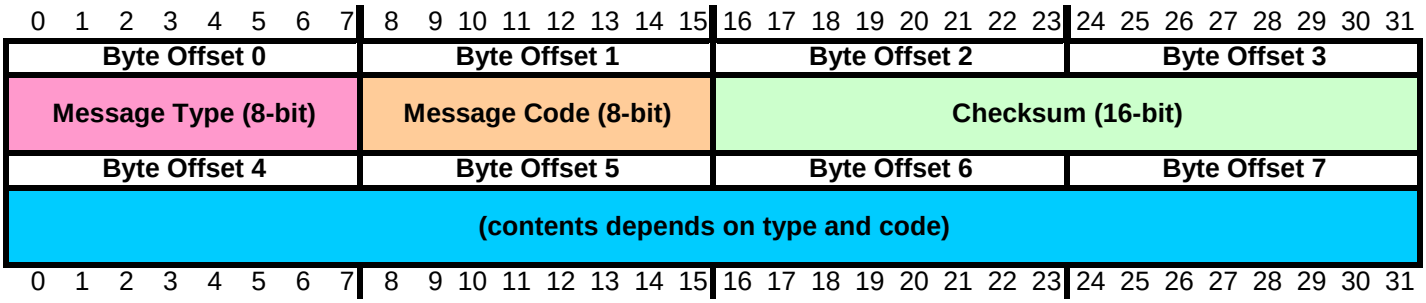
(Max IP is 65535 bytes - 20 byte header = 65515 bytes for UDP packet - 8 bytes of UDP header = 65507)

Checksum

Covers psedo header (IP Header source and destinstation addresses, the protocol and UDP length) and entire UDP datagram

(Note: By RFC, the crc is not required)

Internet Control Message Protocol - ICMP Header (RFC 792)

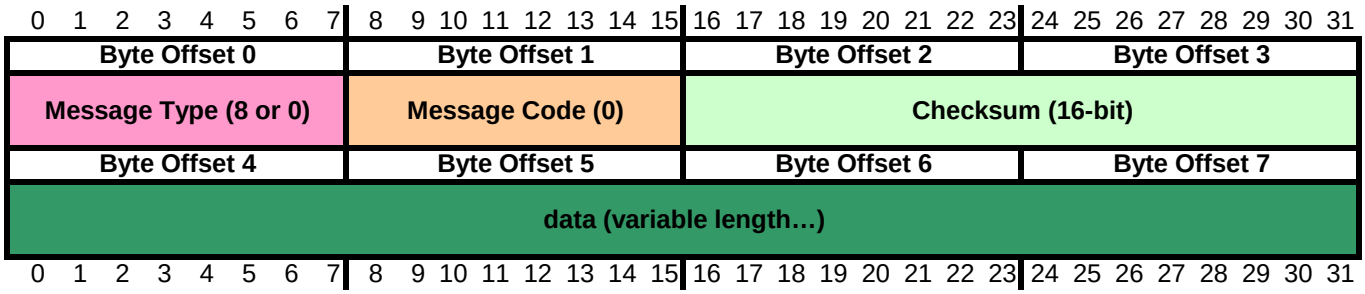


Common Types & Codes

Type	Type Description	Code	Message Code Description
0	Echo reply	0	
3	Destination Unreachable	0	Net Unreachable
		1	Host Unreachable
		2	Protocol Unreachable
		3	Port Unreachable
		4	Fragmentation Needed & Don't Fragment Flag Set
		5	Source Route Failed
		6	Destination Network Unknown
		7	Destination Host Unknown
		8	Source Route 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	0	
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	0	
9	Router Advertisement	0	
10	Router Selection	0	
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 Request	0	
14	Timestamp Reply	0	
15	Information Request	0	
16	Information Reply	0	
17	Address Mask Request	0	
18	Address Mask Reply	0	
30	Traceroute	0	
31	Datagram Conversion Error	0	
37	Domain Name Request	0	
38	Domain Name Reply	0	
40	Photuris (RFC 2521)	0	

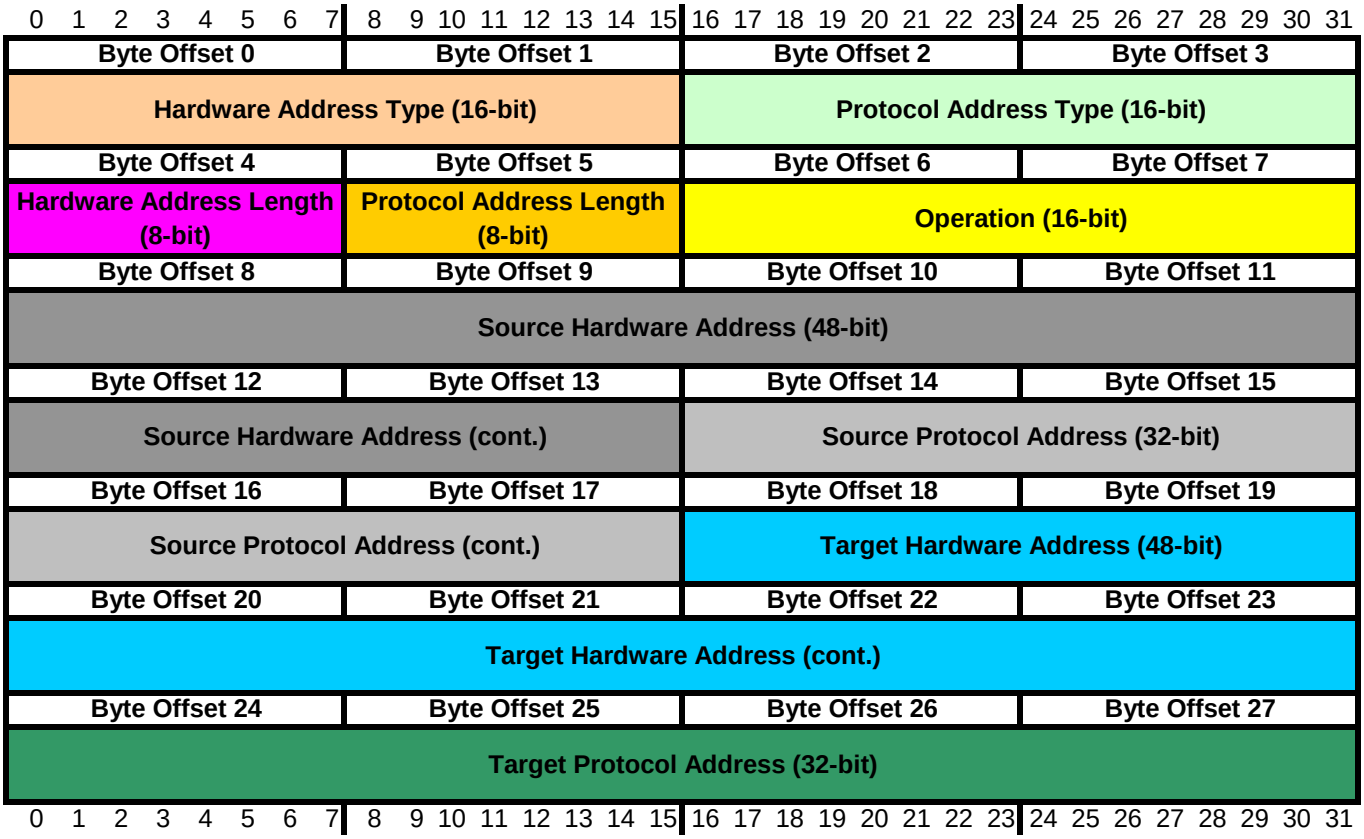
(Note: Byte offset 4-5: identification #)
(Note: Byte offset 6-7: sequence #)

PING (Echo/Echo Reply) - ICMP Header (792)



Type	Type Description	Code	Message Code Description
0	Echo reply	0	
8	Echo	0	

Address Resolution Protocol - ARP (RFC 826)



ARP maps the logical address (IP) to the physical address (MAC)

Hardware Address Type

1	Ethernet
6	IEEE 802 Lan

Protocol Address Type

2048	IPv4 (0x0800)

Hardware Address Length

6	for Ethernet/IEEE 802

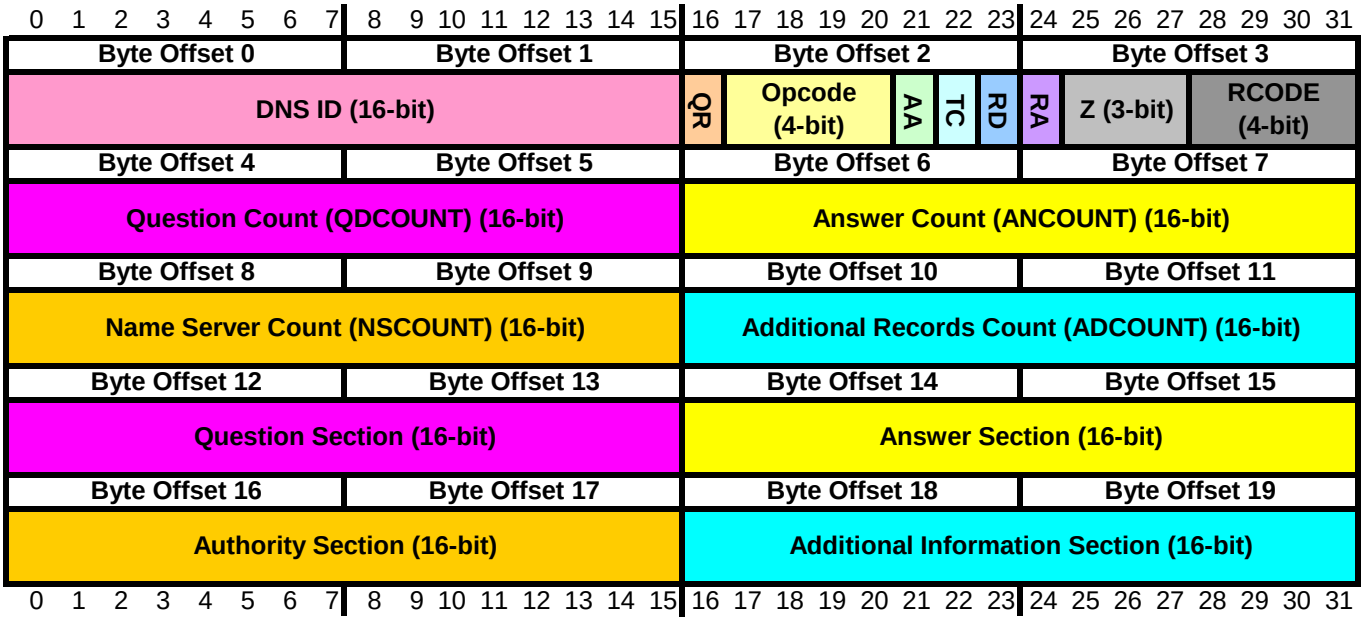
Protocol Address Length

4	for IPv4

Operation

1	Request
2	Reply

Domain Name System - DNS (RFC 1035)



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

(Number of entries in Question section)

ANCOUNT

(Number of resource records in Answer section)

NSCOUNT

(Number of name server resource records in Authority section)

ARCOUNT

(Number of resource records in Additional Information section)

dig version.bind txt chaos @ *server name*
dig @ *server name* txt chaos version.bind

Dynamic Routing Protocols

RIPv1

Distance Vector
Default Administrative Distance 120
Maximum hop count 15
Classful
Broadcast based (255.255.255.255)
No support for VLSM networks
Auto-summarization
No authentication
No support for discontiguous networks
Broadcast all routes every 30 seconds
Uses lowest hop count for best route (Bellman-Ford)
Slow convergence

Ripv2

Distance Vector
Default Administrative Distance 120
Maximum hop count 15
Classless
Uses multicast (224.0.0.9)
Supports Variable Length Subnet Mask(VLSM) networks
Auto-summarization
Allows for MD5 authentication
Supports discontiguous networks
Broadcast all routes every 30 seconds
Uses lowest hop count for best route (Bellman-Ford)
Slow convergence

IGRP (Cisco Proprietary / No longer supported)

Distance Vector
Default Administrative Distance 100
Maximum hop count 255 (default 100)
Classful
Broadcast based (255.255.255.255)
No support for VLSM networks

No authentication
No support for discontiguous networks
Broadcast all routes every 90 seconds
Uses bandwidth and delay for best route
Uses autonomous system numbers

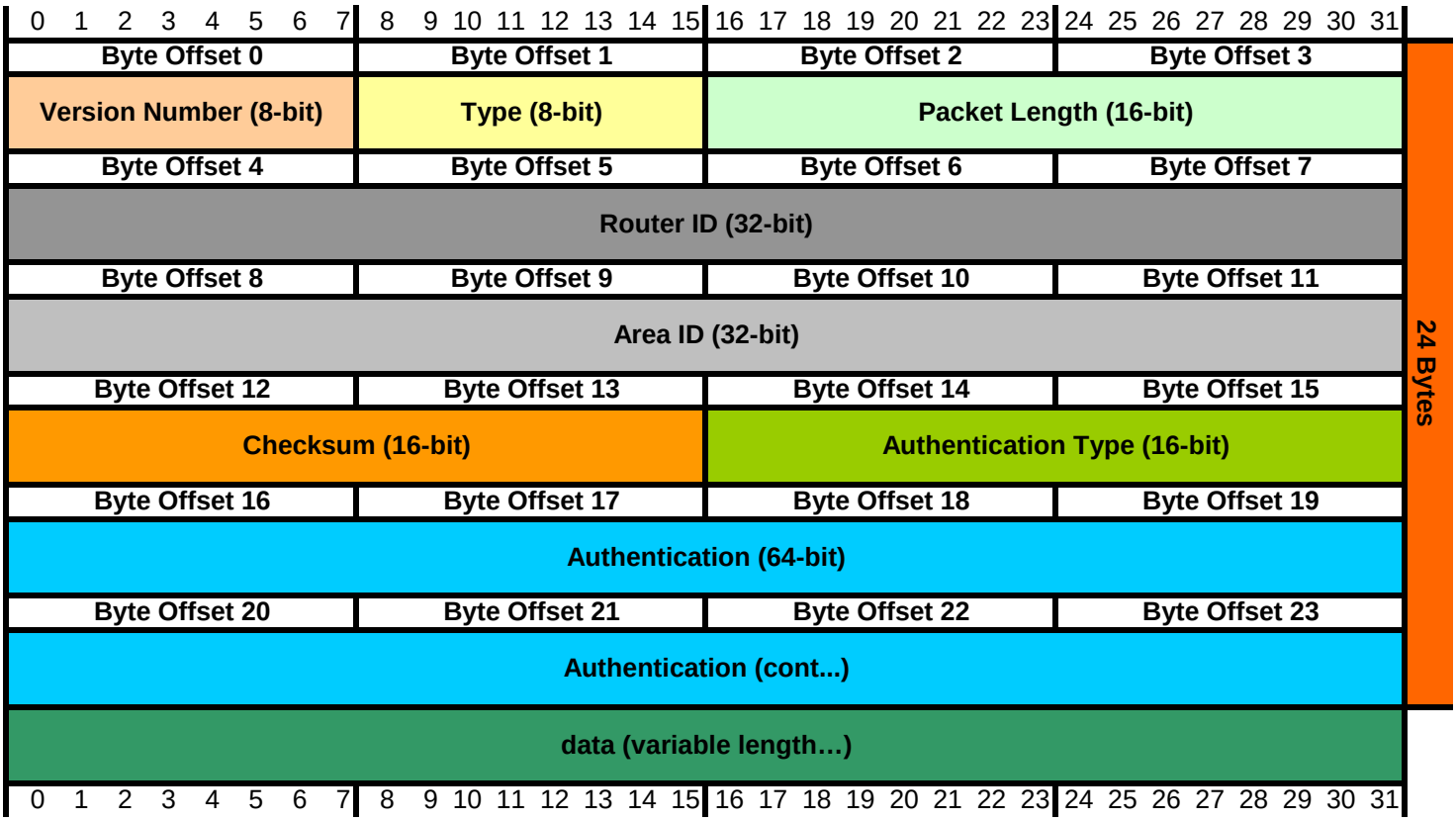
EIGRP (Cisco Proprietary)

Hybrid
Default Administrative Distance 90 (External is 170)
Maximum hop count 255 (default 100)
Classless
Broadcast based (255.255.255.255)
Supports Variable Length Subnet Mask(VLSM) networks
Auto and manual summarization
Allows for authentication
Supports discontiguous networks & route summaries
No periodic route updates. Hello messages with neighbors
Best Path selection via Diffusing Update Alogorithm (DUAL)
Uses autonomous system numbers
Comunication via Reliable Transport Protocol (RTP)
Support for IPv4 and IPv6

OSPF

Link State
Default Administrative Distance 110
Maximum hop count limit - none
Classful
Broadcast based (255.255.255.255)
Supports Variable Length Subnet Mask(VLSM) networks
Manual summarization
Allows for authentication
Supports discontiguous networks & route summaries
Multicast on change
Uses bandwidth and delay for best route (Dijkstra)
Uses autonomous system numbers
Fast convergence
Uses wildcard masks (inverse) in Cisco routers

OSPF v2 (RFC 1583)



Version Number

Valid values are: 12 forOSPF version 2

Type

Type	Description
1	Hello
2	Databse Description
3	Link State Update

Type	Description
4	Link state Update
5	Link State Acknowledgment

Packet Length (Used by gateways as a QoS type field) (Most OS's default to 0)

The length of the protocol packet in bytes includinging the standard OSPF header

Router ID

The router ID of the packet's sour maximum length = 65,535

Area ID

Identifies the are that this packet belongs to. Packets travelling over a virtual link are labelled with the backbone Area ID og 0.0.0.0

Checksum

Standard IP checksum of the entire contents of the OSPF packet excluding the 64-bit authentication field.

Authentication Type

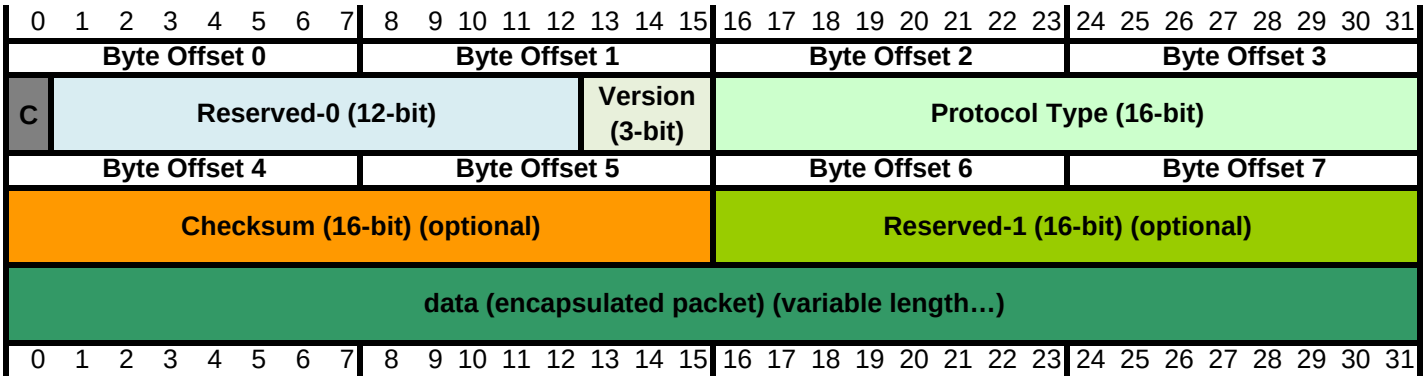
Identifies the authentication scheme to be used for the packet.

Type	Description
0	No authentication
1	Simple password in the clear
rest	Reserved for assignment by the IANA

Authentication

Used by the authentication scheme

Generic Routing Encapsulation - GRE (RFC 2784)



Checksum Present Bit

If the checksum bit is set to 1 then the Checksum and Reserved-1 fields are present.

Reserved-0

If bits 1 through 5 are non-zero then the packet should be discarded unless receiver implements RFC 1701.
Bits 6 through 12 are reserved for future use. The bits must be set to 0 and ignored on receipt.

Version Number

The version number fields must be 0.

Protocol Type

Contains the protocol type of the payload packet. Values are listed in the "ETHER TYPES" section of RFC 1700

Type	Value (Hex)
XNS	0600, 0807
IP version 4	0800
ARP	806
IP (VINES)	0BAD, 80C4
DRP	6003
LAT	6004
DRP	6003

Type	Value
LAVC	6007
IPX	8037
AppleTalk	809B
ARP (Atalk)	80F3
NetWare	8137
IP version 6	86DD

Checksum

Standard IP checksum of the all the 16 bit words in the GRE header and payload packet.

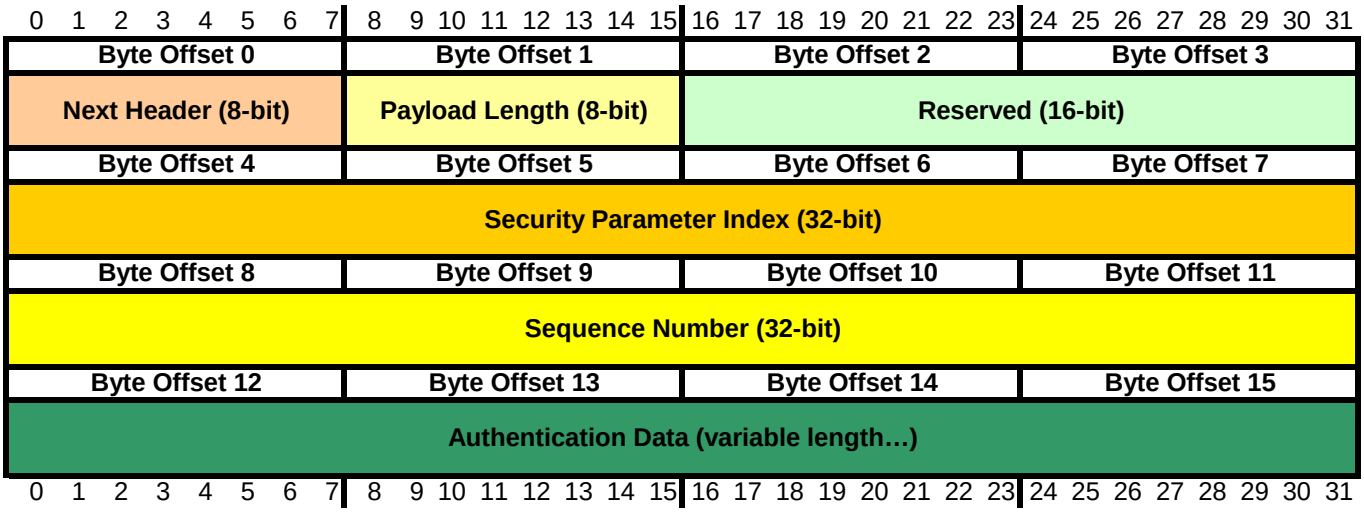
Reserved - 1

Reserved for future use. Only present if checksum bit is set and if present must be 0.

Authentication

Used by the authentication scheme

Authentication Header - AH (RFC 2402)



Next Header

Equivalent to the IP Protocol Identifier field in IPv4

D	Hex		D	Hex		D	Hex		D	Hex	
1	0x01	ICMP	9	0x09	IGRP	47	0x2F	GRE	88	0x58	EIGRP
2	0x02	IGMP	17	0x11	UDP	50	0x32	ESP	89	0x59	OSPF
6	0x06	TCP	47	0x2F	GRE	51	0x33	AH			

Payload Length

Specifies the length of the Authentication Header (number of 32-bit words - 2 for IPv6 compatibility)

Reserved

Zero filled field

Security Parameter Index (SPI)

Random 32-bit value used with destination IP address and IP Sec protocol to uniquely identify the SA.
The SPI is generally selected by the destination IP Sec node.

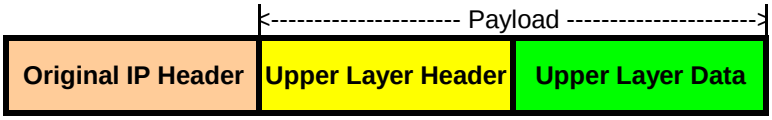
Sequence Number

A 32-bit sequence number starting at zero and incremented by one for each packet.
This monotonically increasing sequence number is the AH anti-replay mechanism.

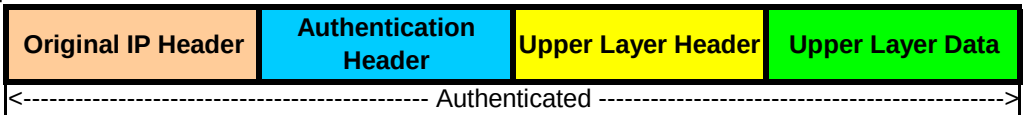
Authentication Data

A variable-length field that contains the Integrity Check Value (ICV) for the packet.
The length of the IVC must be an integral multiple of 32 bits (IPv4) or 64 bits (IPv6); will need to be padded or truncated to meet the requirement.

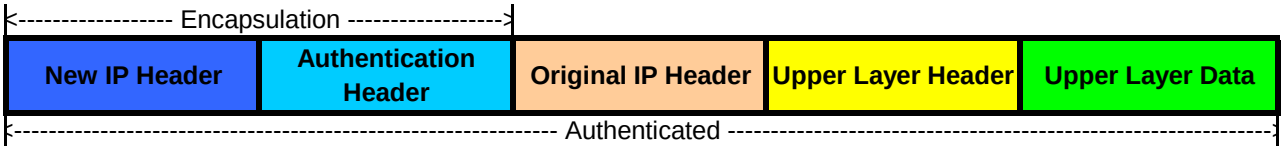
Original Packet

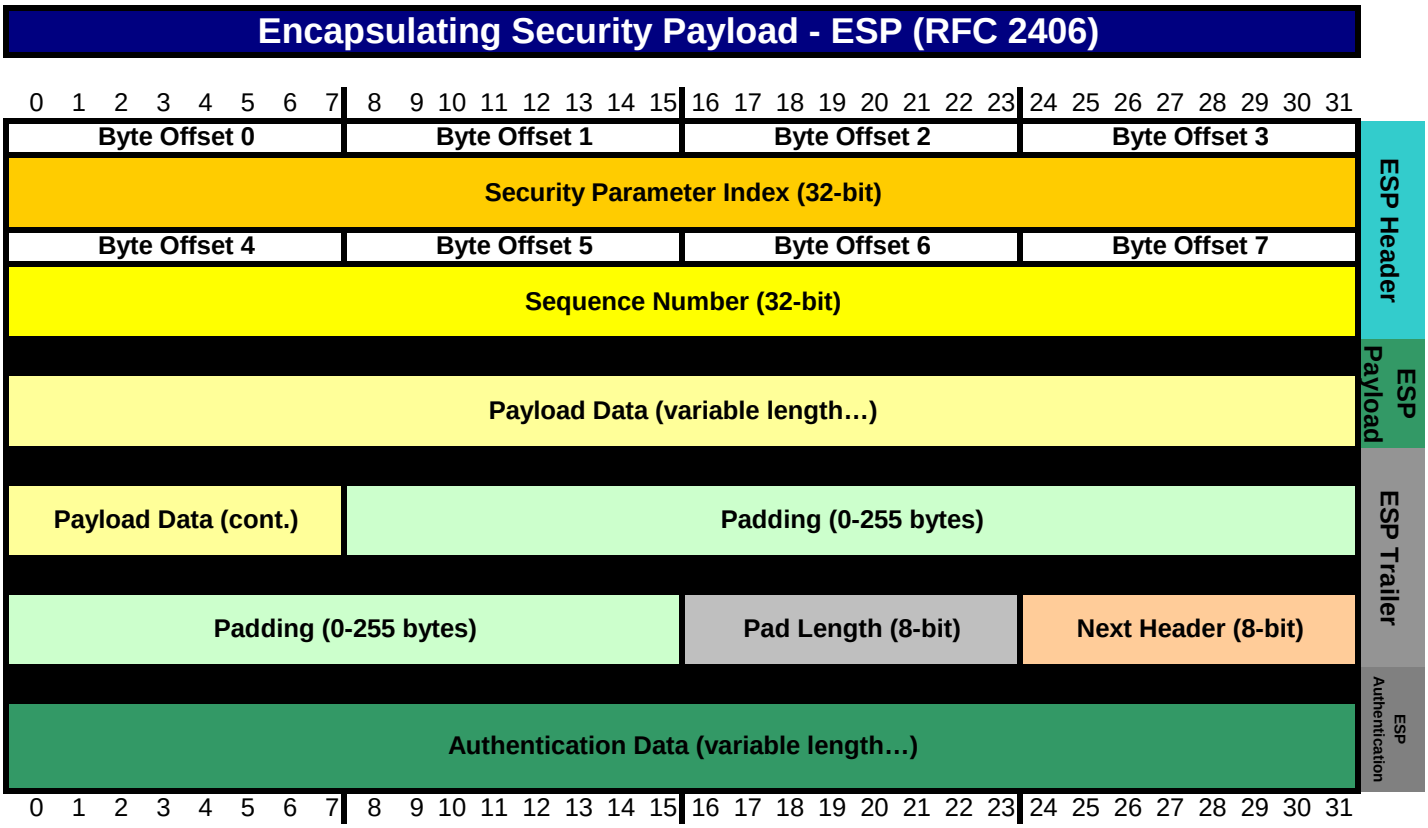


AH Transport Mode Packet



AH Tunnel Mode Packet





ESP Header

Security Parameter Index (SPI)

Random 32-bit value used with destination IP address and IP Sec protocol to uniquely identify the SA.
The SPI is generally selected by the destination IP Sec node.

Sequence Number

A 32-bit sequence number starting at zero and incremented by one for each packet.
This monotonically increasing sequence number is the AH anti-replay mechanism.

ESP Payload

Payload Data

A variable-length field containing the data to be protected by the ESP protocol; i.e., the original IP packet

ESP Trailer

Padding

A 0-255 byte field used for variety of purposes. It is primarily used to ensure that the Payload, Pad Length, & Next Header align on a 32-bit boundary. It can also be used if the ESP encryption algorithm requires a certain minimum number of bytes. Finally, it may be used to hide the real size of the payload (protect against traffic flow analysis)

Pad Length

8-bit value indicating the number of Pad bytes that were inserted.

Next Header

Equivalent to the IP Protocol Identifier field in IPv4

D	Hex		D	Hex		D	Hex		D	Hex	
1	0x01	ICMP	9	0x09	IGRP	47	0x2F	GRE	88	0x58	EIGRP
2	0x02	IGMP	17	0x11	UDP	50	0x32	ESP	89	0x59	OSPF
6	0x06	TCP	47	0x2F	GRE	51	0x33	AH			

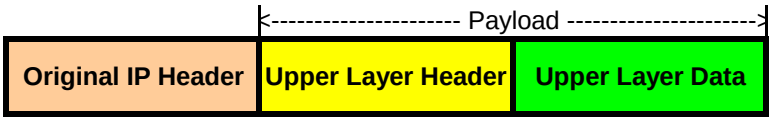
ESP Authentication

Authentication Data

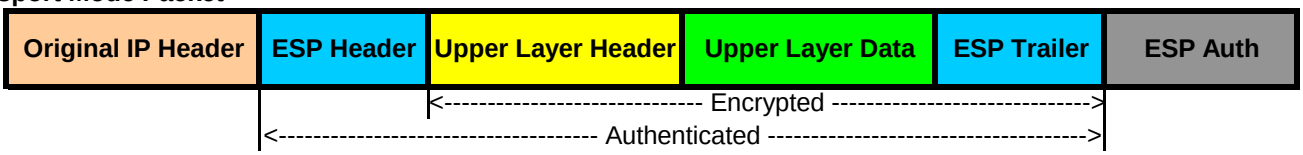
A variable-length field that contains the Integrity Check Value (ICV) for ESP the packet. The length of the this field is dependent upon the authentication function used. This field is present only if an authentication service is being employed in the SA.

Encapsulating Security Payload - ESP (cont.)

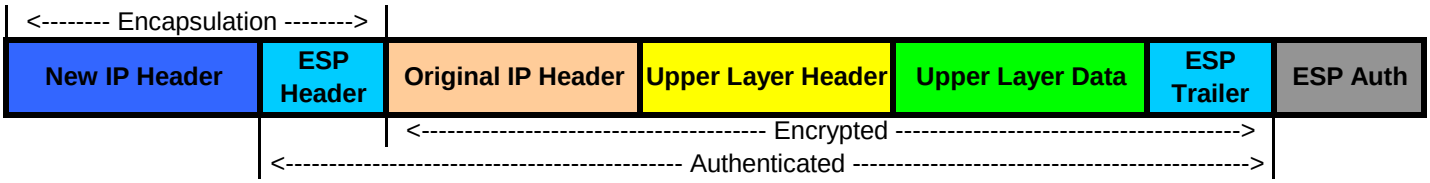
Original Packet

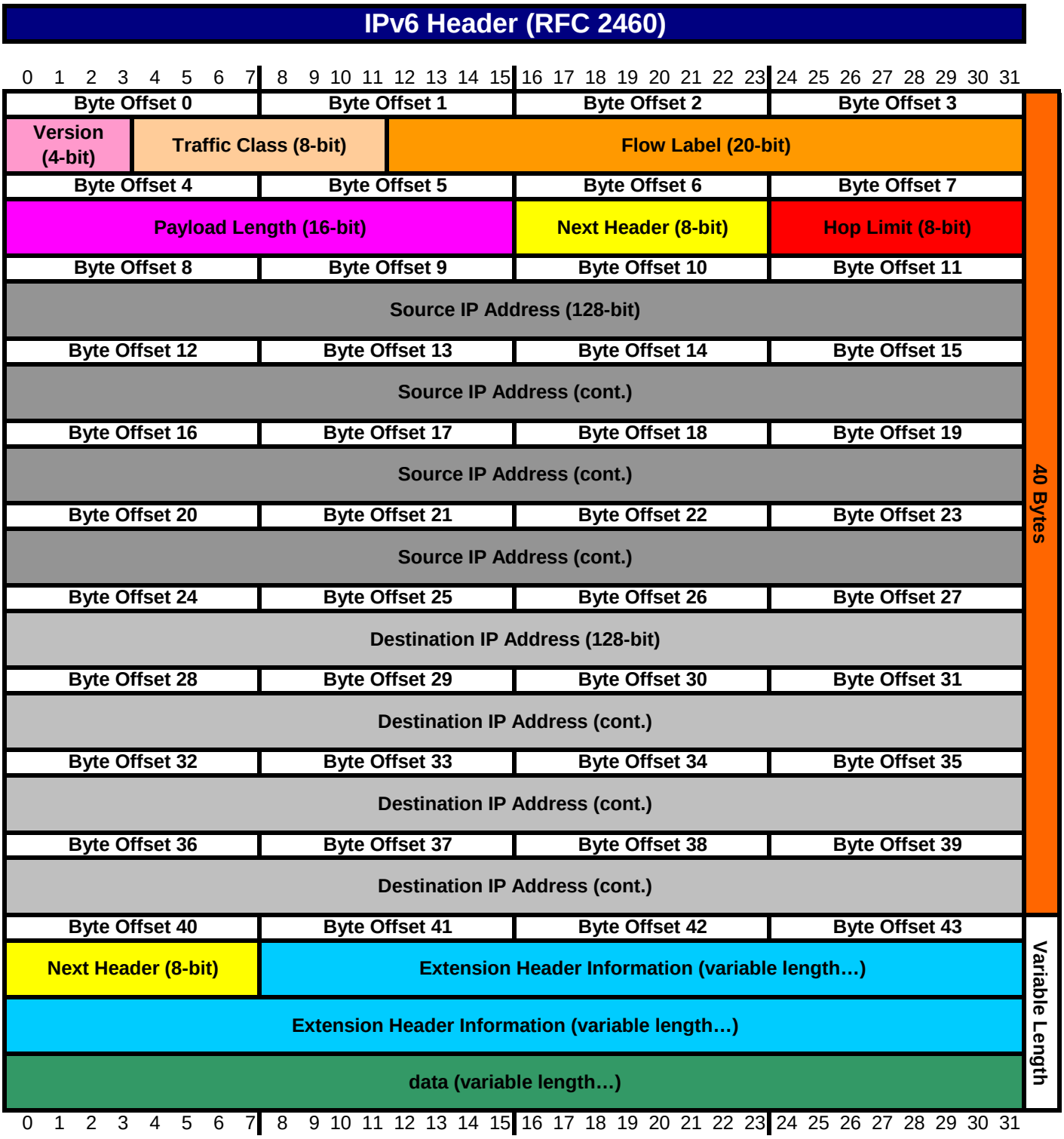


ESP Transport Mode Packet



ESP Tunnel Mode Packet





IP Version Number	6 for IP version 6 4 for IP version 4
Traffic Class	8-bit field similar to IPv4 type of service field
Flow Label	To tag packets of a specific flow to differentiate the packets at the network layer. (**QoS**)
Payload Length	The total length of the data portion of the packet
Next Header	Similar to the protocol field of IPv4 packet header
Hop Limit:	Similar to Time to Live field in IPv4 packet header
Source Address	128-bit source address field
Destination Address	128-bit destination address field

IPv6 (cont.)

A IPv6 Address is 16 bytes (128 bits) this give us 3.4 X 10^38

Samble IPv6 Address:

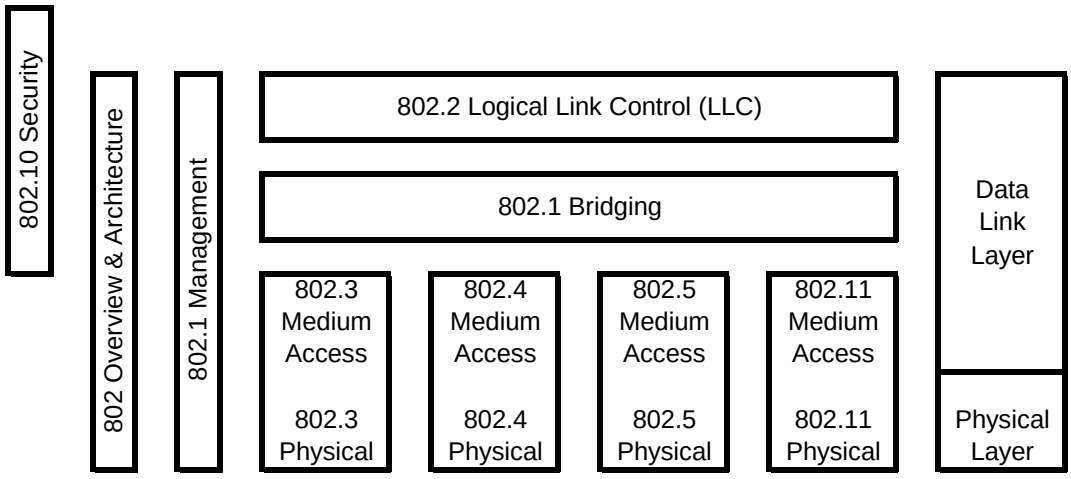
2001: 0db8: abdc:	1234:	0000: 0000: 9865: 4321
Global Prefix	Subnet	Interface ID

Special IPv6 Addresses

Address	Description
0:0:0:0:0:0:0:0	Equal ::. This is the equivalent to IPv4's 0.0.0.0.
0:0:0:0:0:0:0:1	Equals ::1. This is equivalent to IPv4's local host of 127.0.0.1.
0:0:0:0:0:0:192.168.100.1	IPv4 address written in a mixed IPv6 / IPv4 network environment.
2000::/3	The global unicast address range.
FC00::/7	The unique local unicast range. Same Idea as the IPv4 RFC 1918 private addresses.
FE80::/10	The link-local unicast range. Same Idea as the IPv4 RFC 1918 private addresses. **But for on a single LAN. Non routeable.**
FF00::/8	The multicast range.
3FFF:FFF::/32	Reserved for examples and documentation.
2001:0DB8::/32	Reserved for examples and documentation.
2002::/16	Used with 6to4, which is the strucuture that allows IPv6 packets to be transmitted over an IPv4 network without the need to configure explicit tunnels.

This page purposely left blank

IEEE Framing



Ethernet II

A physical layer standard that defines the CSMA/CD access method on a bus topology. **This is the most common frame type for Ethernet IP traffic.**

IEEE 802.1

Flavors of 802.1 (common)

802.1P	Provides a mechanism for implementing Quality of Service (QoS)
802.1Q	VLAN Tagging
802.1X	Port based network access control

IEEE 802.2

A data link layer standard used with 802.3, 802.4, and 802.5 & 802.11

IEEE 802.3

A physical layer standard that defines the CSMA/CD access method on a bus topology.

Flavors of 802.3

802.3 "RAW"	This framing does not use 802.2 LLC. **Novell used this framing.**
802.3 with 802.2	This framing does use the 802.2 LLC.
802.3 with 802.2 SNAP	This framing does have the LLC and SNAP. **Used in conjunction with Wireless traffic on the wired side.**

IEEE 802.4

This is Token Passing Bus Access Method and Physical Layer Specifications.

IEEE 802.5

Token Ring Access Method and Physical Layer Specifications.

IEEE 802.11

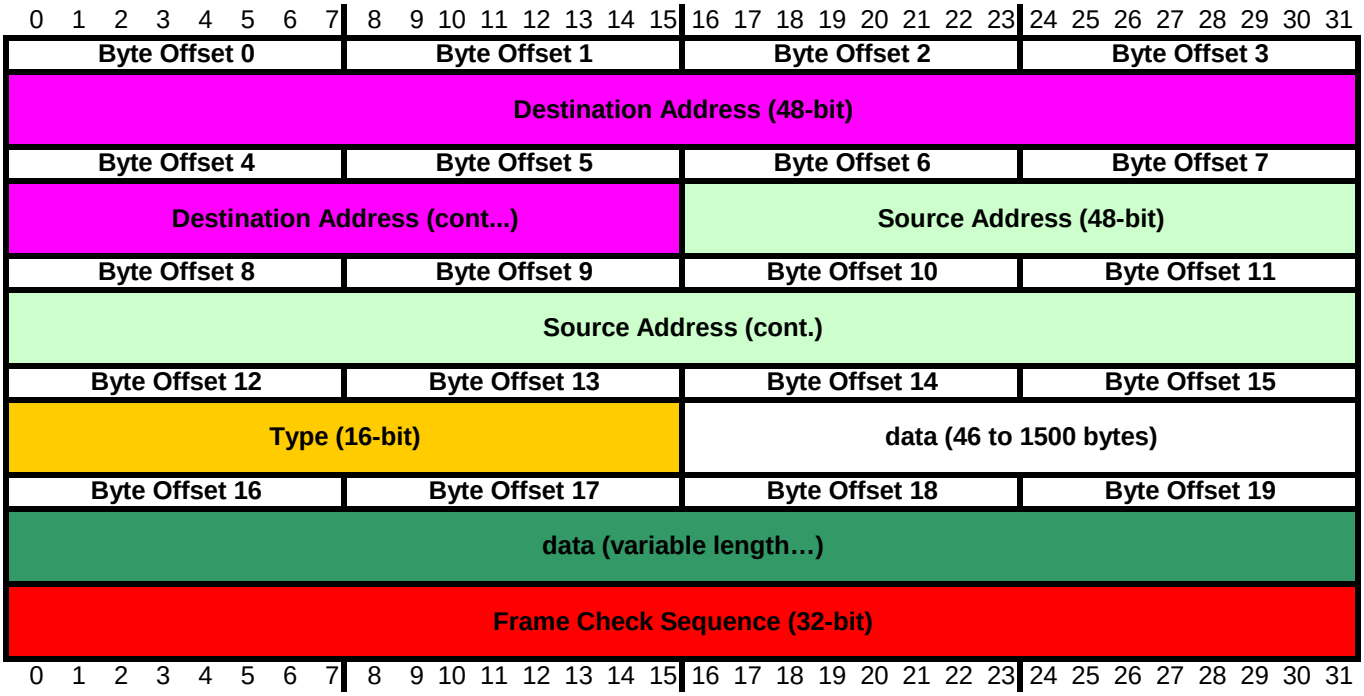
Wireless LAN Medium Access Control (MAC) and Physical Layer Specifications.

Flavors of 802.11 (common)

802.11a	54 Mbit/s using the 5 GHz band with up to 23 non overlapping channels. (~15 users per AP)
802.11b	11 Mbit/s using the 2.4 GHz band with 3 non-overlapping channels. (~25 users/AP)(Marketed - WiFi)
802.11g	54 Mbit/s using the 2.4 GHz band with 3 non-overlapping channels. (~20 users/AP)(Marketed - WiFi)
802.11n	Allows for greater Mbit/s using multiple-input multiple-output (MIMO), channel bonding and frame aggregation. This standard can be used in the 2.4 with 3 non overlapping channels and 5.0 GHz band with up to 23 non overlapping channels. (~15 users per AP)

Organizationally Unique Identifier (OUI) This is the first 3 bites of the Media Access Control (MAC) Address)
http://standards.ieee.org/regauth/oui/oui.txt

Ethernet II Frame Format (similar to IEEE 802.3)



Most common format of Ethernet packets today.

Preamble: 8 bytes (64 bit) At the head of each frame is a preamble used for synchronization 1010…10101011 this is know as Manchester encoding.

Destination Address: 6 byte (48 bit) destination media access control (MAC) address

Source Address: 6 byte (48 bit) source media access control (MAC) address

Type: 2 byte (16 bit) field that specifies the upper-layer protocol
Note: The **difference** between **Ethernet II** and **IEEE 802.3** is that this field in the IEEE standard is called the length field.

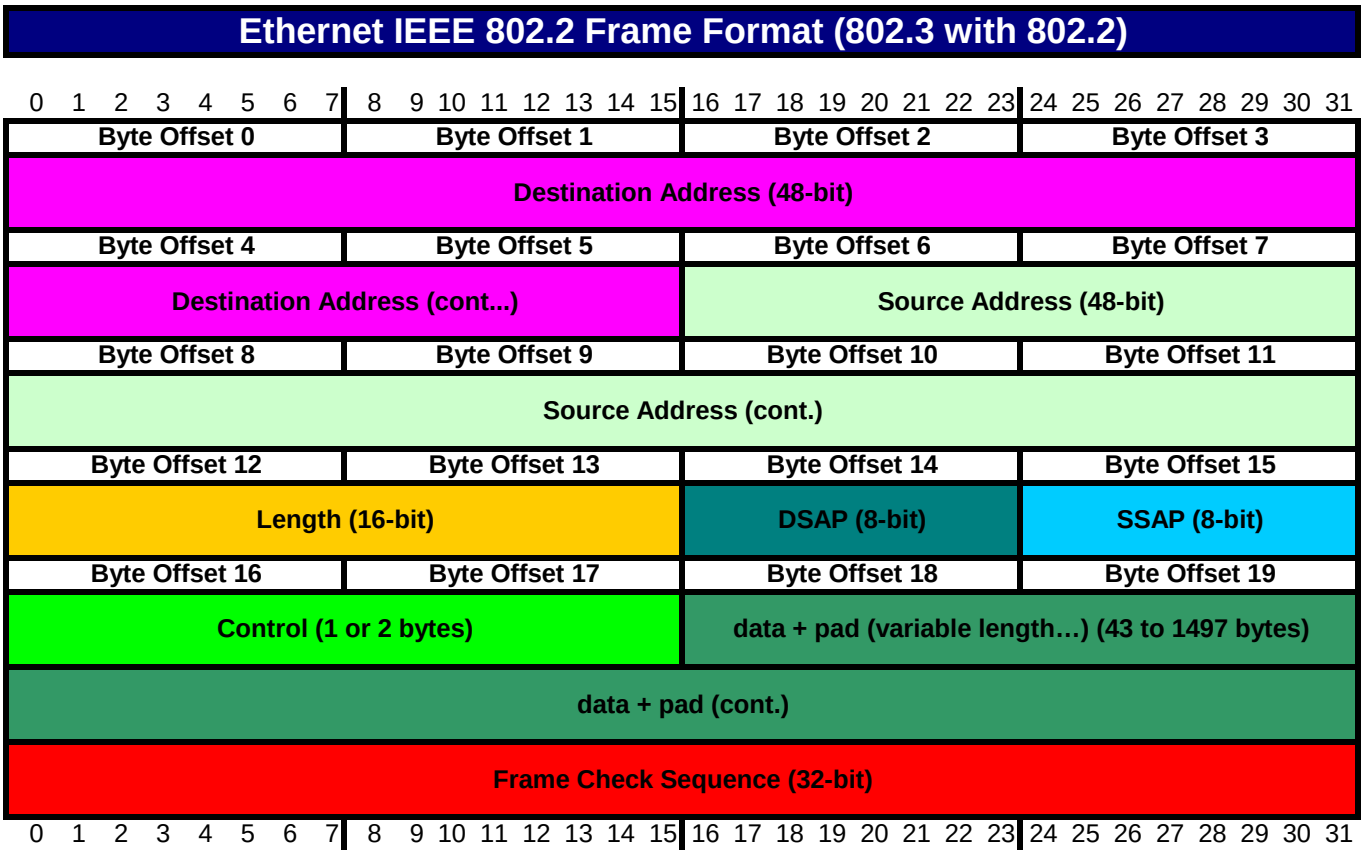
Type	Value (Hex)
XNS	0600, 0807
IP version 4	0800
ARP	0806
IP (VINES)	0BAD, 80C4
DRP	6003
LAT	6004
DRP	6003

Type	Value
LAVC	6007
IPX	8037
AppleTalk	809B
ARP (Atalk)	80F3
NetWare	8137
IP version 6	86DD

Data: 46 to 1500 bytes of upper-layer protocol information

Frame Check Sequence: The cyclic redundancy check (CRC) or checksum for the Ethernet Frame

Min Ethernet Frame:
14 byte frame header + **46** bytes of encapsulated data + **4** byte frame trailer = **64** bytes
Max Ethernet Frame:
14 byte frame header + **1500** bytes of encapsulated data + **4** byte frame trailer = **1518** bytes



Preamble: 8 bytes (64 bite) At the head of each frame is a preamble used for synchronization 1010…10101011

Destination Address: 6 byte (48 bit) destination media access control (MAC) address **(Part of 802.3 Header)**

Source Address: 6 byte (48 bit) source media access control (MAC) address **(Part of 802.3 Header)**

Length: 2 byte (16 bit) field that specifies the number of bytes (3-1500) in the LLC and data fields **(Part of 802.3 Header)**

Logical Link control The logical link control (LLC) is made up of the DSAP, SSAP and Control fields. This is a method for telling the 802.3 IEEE and Netware (RAW) formats. The IEEE 802.3 format has the LLS and the NetWare 802.3 "Raw" format does not. **(This is the 802.2 Header)**

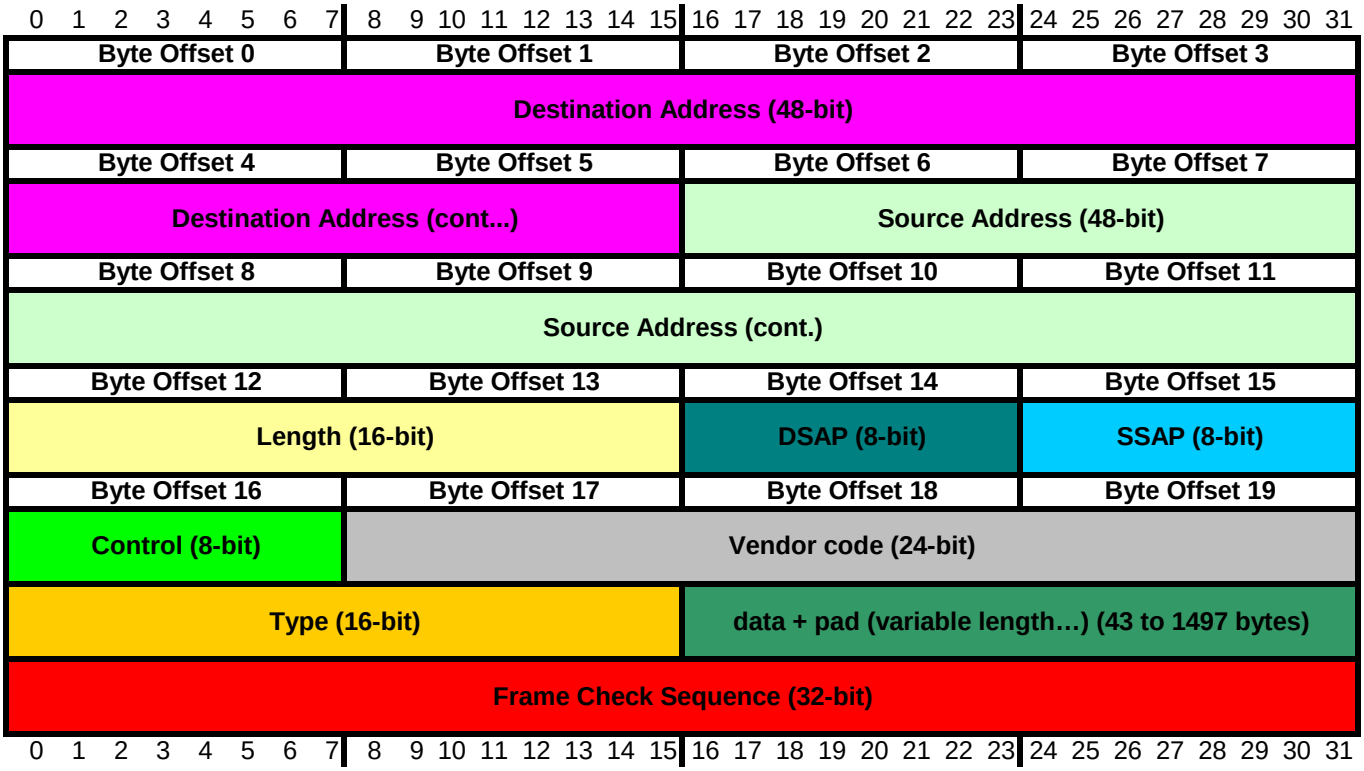
- **DSAP:** 1 byte destination service access point; receiving process at destination
- **SSAP:** 1 byte source service access point; sending process at source
- **Control:** 1 byte is various control information (Connection less)
  2 bytes are for connection-oriented LLC

Pad: Pads the frame to minimum of 46 bytes of data and LLC (so collisions can be detected)

Data: 46 to 1500 bytes of upper-layer protocol information

Frame Check Sequence: The cyclic redundancy check (CRC) or checksum for the Ethernet Frame

Ethernet IEEE 802.2 SNAP Frame Format (802.3 with 802.2 SNAP)



This is the Framing formate used on the Ethernet (wired) side with 802.11 with 802.2 SNAP for the wireless.

Preamble: 8 bytes (64 bite) At the head of each frame is a preamble used for synchronization 1010…10101011

Destination Address: 6 byte (48 bit) destination media access control (MAC) address **(Part of 802.3 Header)**

Source Address: 6 byte (48 bit) source media access control (MAC) address **(Part of 802.3 Header)**

Length: 2 byte (16 bit) field that specifies the number of bytes (3-1500) in the LLC and data fields

Logical Link control

The logical link control (LLC) is made up of the DSAP, SSAP and Control fields. This is a method for telling the 802.3 IEEE and Netware (RAW) formats. The IEEE 802.3 format has the LLS and the NetWare 802.3 "Raw" format does not. **(Part of the 802.2 SNAP Header)**

DSAP: 1 byte destination service access point; receiving process at destination (**Always AA**)

SSAP: 1 byte source service access point; sending process at source (**Always AA**)

Control: 1 byte is various control information (Connection less)
2 bytes are for connection-oriented LLC

SNAP Header The Subnet Access Protocol Header consists of the Vendor Code and Type fields

Vendor Code: 3 byte (24 bit) field to identify the vendor

Type: 2 byte (16 bit) field that specifies the upper-layer protocol

Type	Value
NetWare	8137
XNS	0600, 0807
IP	800
IP (VINES)	0BAD, 80C4
ARP	806

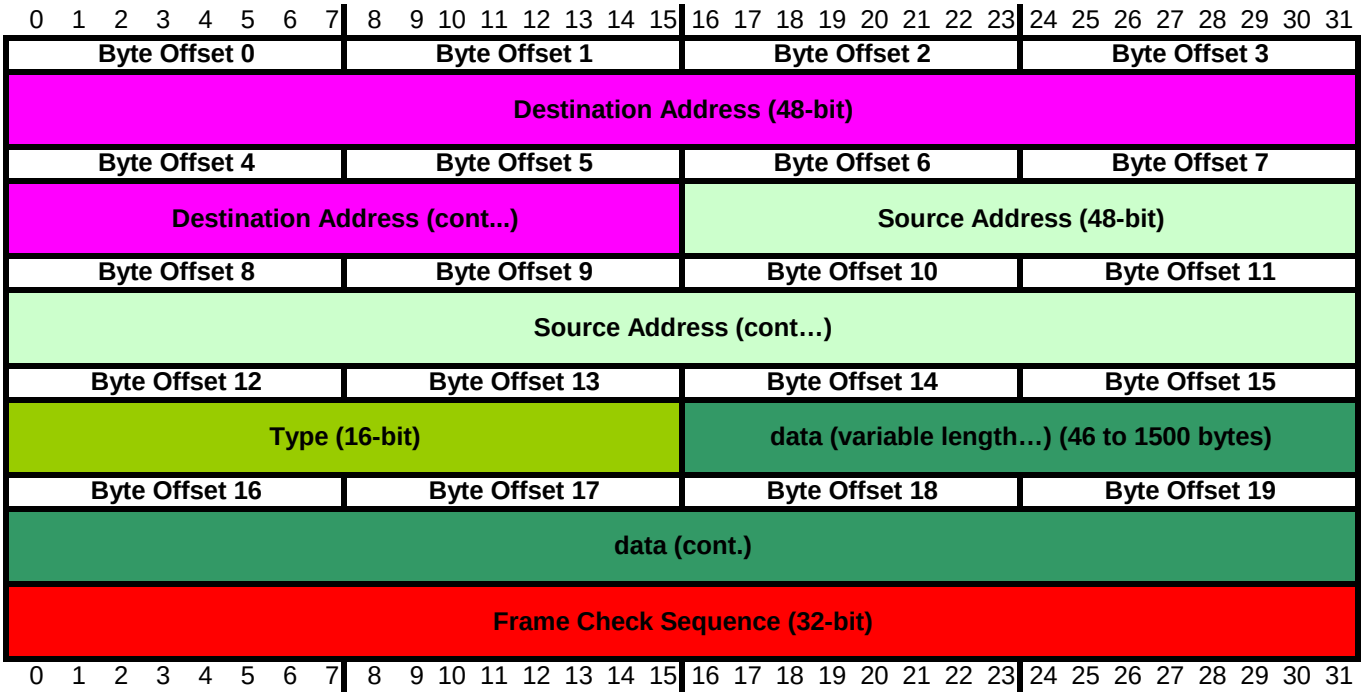
Type	Value
RARP	8035
DRP	6003
LAT	6004
LAVC	6007
ARP (Atalk)	80F3

Pad: Pads the frame to minimum of 46 bytes of data and LLC (so collisions can be detected)

Data: 46 to 1500 bytes of upper-layer protocol information

Frame Check Sequence: The cyclic redundancy check (CRC) or checksum for the Ethernet Frame

Ethernet Novell Netware 802.3 "Raw" Frame Format (802.3 without 802.2)



IP Version Number

Preamble: 8 bytes (64 bite) At the head of each frame is a preamble used for synchronization 1010…10101011

Destination Address: 6 byte (48 bit) destination media access control (MAC) address

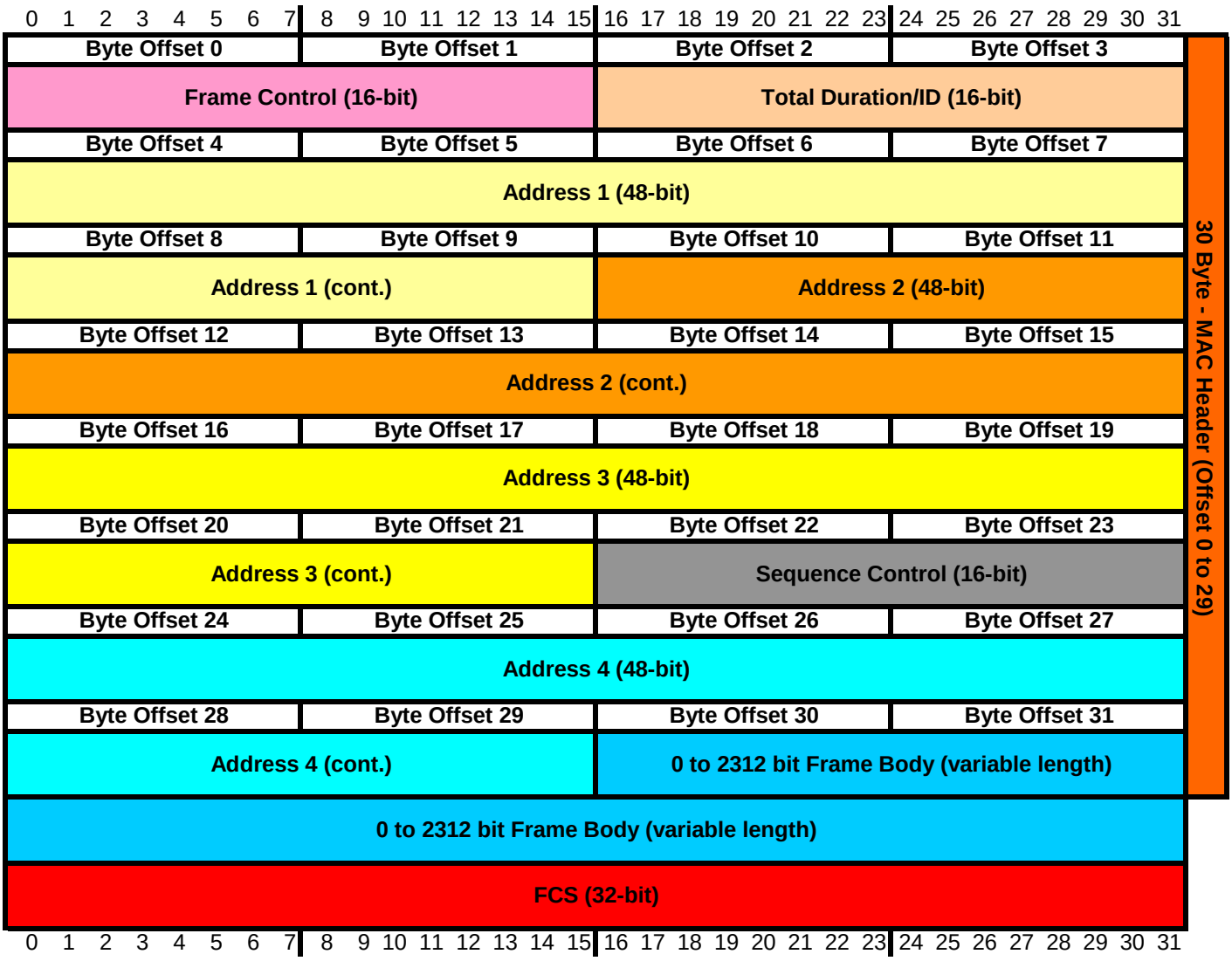
Source Address: 6 byte (48 bit) source media access control (MAC) address

Length: 2 byte (16 bit) field that specifies the number of bytes (46-1500) in the LLC and data fields Note the lack of the LLC fields, this is how you tell Netware 802.3 from IEEE 802.3

Data: 46 to 1500 bytes of upper-layer protocol information. IPX header starting with 2 byte checksum (usually FFF) followed by NetWare higher layers ('data')

Frame Check Sequence: The cyclic redundancy check (CRC) or checksum for the Ethernet Frame

802.11 (IEEE 1999 Reference Specification)



Frame Control Consists of the following subfields: Protocol Version (bits 0-1), Type (bits 2-3), Subtype (bits 4-7), To DS (bit 8), From DS (bit 9), More Fragment (bit 10), Retry (bit 11), Power management (bit 12), More Data (bit 13), WEP (bit 14) and Order (bit 15)

Duration / ID **Duration/ID field encoding**

15	14	bit 13 - 0	Usage
0	0 - 32767		Duration
1	0	0	Fixed value within frames transmitted during the CFP
1	0	1-16383	Reserved
1	1	0	Reserved
1	1	1-2007	Association Identificatier (AID) in PS-Poll frames (**Max association per AP is 2007**)
1	1	2008 - 16383	Reserved

Address Fields There are 4 address fields in the MAC frame format. These fields are used to indicate the BSSID, source address (SA), destination address (DA), transmitting station address (TA), and the receiving station address (RA).

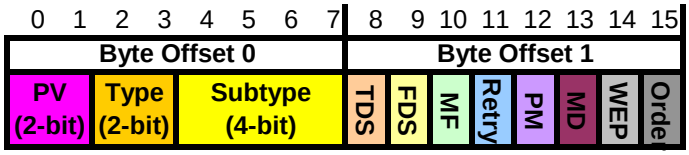
Sequence Control Consists of the following subfields: Fragment Number (bits 0-3) and Sequence Number (bits 4-15). Frames that have a payload larger than **2312 bytes** will be fragmented.

Frame Body Variable length field that contains information specific to individual frame types and subtypes.

FCS 32-bit check sum field calculated over all the fields of the MAC header and Frame body

802.11 (cont.)

Frame Control



Protocol Version Currently the value should always be 0

Type / Subtype The type and subtype field together identify the function of the frame

Type		Type	Subtype				
b3	b2	Description	b7	b6	b5	b4	Subtype Description
0	0	Management	0	0	0	0	Association Request
0	0	Management	0	0	0	1	Association Response
0	0	Management	0	0	1	0	Reassociation Request
0	0	Management	0	0	1	1	Reassociation Response
0	0	Management	0	1	0	0	Probe Request
0	0	Management	0	1	0	1	Probe Response
0	0	Management	0110-0111				Reserved
0	0	Management	1	0	0	0	Beacon
0	0	Management	1	0	0	1	Announcement traffic indication message (ATIM)
0	0	Management	1	0	1	0	Disassociation
0	0	Management	1	0	1	1	Authentication
0	0	Management	1	1	0	0	Deauthentication
0	0	Management	1101-1111				Reserved
0	1	Control	0000-1001				Reserved
0	1	Control	1	0	1	0	Power Save (PS)-Poll
0	1	Control	1	0	1	1	Request To Send (RTS)
0	1	Control	1	1	0	0	Clear To Send (CTS)
0	1	Control	1	1	0	1	Acknowledgment (ACK)
0	1	Control	1	1	1	0	Contention-Free (CF)-End
0	1	Control	1	1	1	1	CF-End + CF-Ack
1	0	Data	0	0	0	0	Data
1	0	Data	0	0	0	1	Data + CF-Ack
1	0	Data	0	0	1	0	Data + CF-Poll
1	0	Data	0	0	1	1	Data + CF-Ack + CF-Poll
1	0	Data	0	1	0	0	Null function (no data)
1	0	Data	0	1	0	1	CF-Ack (no data)
1	0	Data	0	1	1	0	CF-Poll (no data)
1	0	Data	0	1	1	1	CF-Ack + CF-Poll (no data)
1	0	Data	1000-1111				Reserved
1	1	Reserved	0000-1111				Reserved

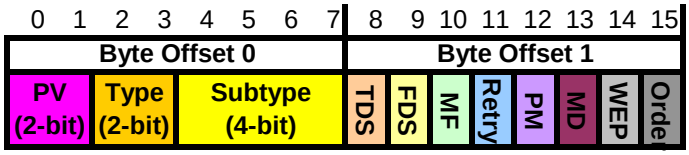
Miscellaneous Info

802.11a	54 Mbit/s using the 5 GHz band
802.11b	11 Mbit/s using the 2.4 GHz band (Marketed under the name WiFi)
802.11g	54 Mbit/s using the 2.4 GHz band (Marketed under the name WiFi)
802.11n	Allows for greater Mbit/s using multiple-input multiple-output (MIMO), channel bonding and frame aggregation. This standard can be used in the 2.4 and 5.0 GHz band.

802.11 header information was compiled from the 802.11 1999 reference specification available at http://standards.ieee.org/getieee802/download/802.11-1999.pdf

802.11 (cont.)

Frame Control



To DS Set to 1 in data type frames destined for the DS. This includes all data type frames sent by wireless stations associated with an AP. The To DS field is set to 0 in all other frames.

From DS Set to 1 in data type frames exiting the DS. It is set to 0 in all other frames.

DS TO/From DS Values

To	From	Meaning
0	0	A data frame direct from one wireless station to another wireless within the same IBSS, as well as all management and control type frames. (**AD HOC**) **Address 1 is Destination, Address 2 is Source, Address 3 is BSSID***
0	1	Data frame destined for the DS (**to** a wired network) from a wireless station (**Infrastructure**) **Address 1 is Destination, Address 2 is BSSID, Address 3 is Source**
1	0	Data frame exiting the DS (**from** a wired network) to a wireless station (**Infrastructure**) **Address 1 is BSSID, Address 2 is Source, Address 3 is Destination**
1	1	Wireless distribution system (**WDS**) frame being distributed from one AP to another AP **Address 1 is Receiver, Address 2 is Transmitter** **Address 3 is Destination, Address 4 is Source**

* **Note:** The BSSID in an IBSS network is a randomly-selected value with the first 2 bits consistenly set to 01. The value is in the range of 40:00:00:00:00:00 to 7f:ff:ff:ff:ff:ff.

More Fragments Set to 1 in all data management type frames that have another fragment of the current MSDU or current MMPDU to follow. It is set to 0 in all other frames.

Retry Set to 1 in any data or management type frame that is a retransmission of an earlier frame. It is set to 0 in all other frames. A receiving station uses this indication to aid in the process of eliminating duplicate frames.

Power Management

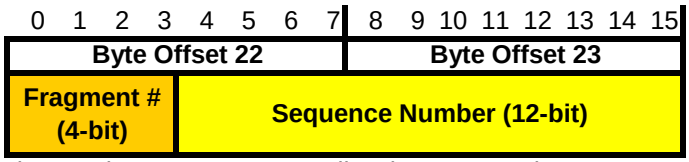
Set to 1 indicates that the STA will be in power-save mode. A value of 0 indicates that the STA will be in active mode. This field is always set to 0 in frames transmitted by an AP.

More Data Set to 1 in directed data type frames transmitted by a contention-free (CF)-Pollable STA to the point coordinator (PC) in response to a CF-Poll to indicate that the STA has at least one additional buffered MSDU available for transmission in response to a subsequent CF-Poll. Set to 0 in all other directed frames.

WEP Set to 1 if the Frame Body field contains information that has been processed by the WEP algorithm. The WEP field is set to 0 in all other frames. When the WEP bit is set to 1, the Frame Body field is expanded.

Order Set to 1 if any data type frame that contains an MSDU, or fragment thereof, which is being transferred using the Strictly Ordered service class. Set to 0 in all other frames.

Sequence Control



Fragment field Field value can be 0 to 4096. Normally 0 because packets are not normally fragmented. Each fragment is assigned a unique fragment number with the entirety of the packet identified with a single sequence number. Note: Frames that have a payload larger than 2312 bytes will be fragmented.

Kismet	
Commands	
Key	**Description**
QUICK REFERENCE	
e	List Kismet servers
z	Toggle fullscreen zoom of network view
m	Toggle muting of sound and speech
t	Tag (or untag) selected network
g	Group tagged networks
u	Ungroup current group
c	Show clients in current network
L	Lock channel hopping to the current network channel
H	Return to normal channel hopping
+	Expand groups
-	Collapse groups
^L	Force a screen redraw
POPUP WINDOWS	
h	Help
n	Name current network
i	detailed information about selected network
s	Sort network list
l (lower case L)	Show wireless card power levels
d	Dump printable strings
r	Packet rate graph
a	Statistics
p	Dump packet type
f	Follow network center
w	Track alerts
x	Cloase popup window
Q	Quit

Definitions of Symbols

Network/Group Types:		
Symbol	**Name**	**Description**
P	Probe Request	No associated connection yet
A	Access Point	Standard wireless network
H	ad-hoc	Point-to-point wireless network (IBSS)
T	Turbocell	Turbocell (aka Karlnet or Lucent Outdoor Router) network
G	Group	Group of wireless networks
D	Data	data only network with no control packets
Status Flags		
Symbol	**Description**	
F	Vulnerable factory configuration.	
T#	Address range of # octets found via TCP traffic	
U#	Address range of # octets found via UDP traffic	
A#	Address range of # octets found via ARP traffic	
D	Address range found via observed DHCP traffic	
W	WEPed network decrypted with user-supplied key	

Information obtained from the Kismet help screen

TCPDUMP / WINDUMP

windump -i <interface> -nX	capture from interface (-i <interface>) do not convert names(-n) and print out hex and ascii (-X)
windump -i <interface> -nX -s0	capture from interface (-i <interface>) do not convert names(-n), print out hex and ascii (-X) and capture all the packet
windump -r <file> -nXp	capture from file (-r <file>), do not convert names (-n), print out hex and ascii (-X), not in promiscuous mode (-p)

Keywords

host (host)	**ip**	**vrrp**	**ether multicast**
src host (host)	**ip6**	**ip broadcast**	**vlan** (vlan_id)
dst host (host)	**arp**	**ip proto** (protocol)	**atalk**
gateway (host)	**icmp**	**ip protochan** (protocol)	**decnet**
net (net/len)	**icmp6**	**ip6 proto** (protocol)	**decnet src**
src net (net)	**tcp**	**ip6 protochain** (protocol)	**decnet host**
dst net (net)	**udp**	**ip multicast**	**iso**
port (port)	**ah**	**ip6 multicast**	**stp**
src port (port)	**esp**	**ether host** (MAC)	**ipx**
dst port (port)	**igmp**	**ether src** (MAC)	**netbeui**
less (length)	**igrp**	**ether dst** (MAC)	
greater (length)	**rarp**	**ether proto** (protocol)	

Bit Masking	tcpflags	icmptype			
And unwanted bits with 0	tcp-fin		icmp-echoreply	icmp-echo	icmp-paramprob
And wanted bits with 1	tcp-syn		icmp-unreachable	icmp-ireq	icmp-tstamp
0 AND 0 = 0	tcp-rst		icmp-sourcequench		icmp-tstampreply
0 AND 1 = 0	tcp-push		icmp-redirect		icmp-ireq
1 AND 0 = 0	tcp-ack		icmp-routeradvert		icmp-ireqreply
1 AND 1 = 1	tcp-urg		icmp-routersolicit		icmp-maskreq
			icmp-timxceed		icmp-maskreply

Expressions: >, <, >=, <=, =, !=, +, -, *, /, &, | **!** or **not** **&&** or **and** **||** or **or**

filter format <protocol header>[offset:length]<relation><value>

tcpdump [command line options] ['filter']

windump [command line options] ["filter"]

Examples

host A and B	Connections between host A and host B					
ip[9] = 1	icmp	ip[9] = 6	tcp	ip[9] = 17	udp	ip[9] = 0x11
tcp[2:2] < 20	The TCP dst port is greater than 20			udp[6:2] != 0	Non-zero UDP checksum	
tcp[tcpflags]=tcp-syn	Only Syn	tcp[13] &0x02 != 0	At minimum the SYN bit set			
tcp[tcpflags]=tcp-ack	Only Ack	tcp[13] &0x10 != 0	At minimum the ACK bit set			
tcp[tcpflags]=tcp-fin	or	tcp[13] &0xff=0x01	Only the FIN bit is set			tcp[13] &0xff = 1
tcp[13] &0xff =16	or	tcp[13] &0xff = 0x10	Only the ACK bit is set			
icmp[0]=3 and icmp[1]=2	icmp type 3 is destination unreachable category and a code of 2 specifies that this is an ICMP protocol unreachable (**Good filter for detecting protocol scans**)					
(tcp and (tcp[13] &0x0f != 0) and not port 25 and not port 20)	A tcp packet where any combination of PSH, RST, SYN, FIN are set and the packet is not port 25 or 20					
udp[21:4]=0x56455253	Looks for “VERS” in udp payload for VERSION.BIND					
tcp[20:4] = 0x5353482d	Looks for “SSH-” in TCP payload					
ip[6:2] & 0x3fff != 0	Look for ALL fragmented ip packets					
ip[6] &0x20 = 0x20 or ip[6:2] &0x1fff != 0	Look for more fragment bit set **or** fragment offset greater than 0 (**Look for ALL fragmented ip packets**)					
ip[6] &0x20 = 0 and ip[6:2] &0x1fff != 0	Look for more fragment bit **not** set **and** fragment offset greater than 0 (**Last fragment packets**)					

TCPDUMP / WINDUMP (cont.)

Command Line Options

Options	Description
-a	Attempt to convert network and broadcast addresses to names
-A	
-B <size>	Set driver's buffer size to size in KiloBytes. The default buffer size is 1 megabyte (i.e 1000).
-c <count>	Exit after receiving <count> of packets
-C <file size>	Before writing a raw packet to a savefile, check whether the file is currently larger than file_size and, if so, close the current savefile and open a new one.
-d	Dump the compiled packet-matching code in a human readable form to standard output and stop
-dd	Dump packet-matching code as a C program fragment
-ddd	ddd Dump packet-matching code as decimal numbers (preceded with a count)
-D	Print the list of the interface cards available on the system. WINDUMP ONLY
-e	Print the link-level header on each dump line
-E <algo:secret>	Use algo:secret for decrypting IPsec ESP packets where algorithms may be des-cbc, 3des-cbc, blowfish-cbc, rc3-cbc, cast128-cbc, or none.
-f	Print 'foreign' internet addresses numerically rather than symbolically
-F <file>	Use file as input for the filter expression
-i <interface>	Listen on interface (defaults to lowest numbered interface)
-l	Make stdout line buffered. ``tcpdump -l | tee dat'' or ``tcpdump -l > dat & tail -f dat''
-L	
-m <module>	Load SMI MIB module definitions from file module
-n	Don't convert addresses to names
-nn	Don't convert addresses or port numbers (port numbers are resolved based on information the the linux /etc/service file or the windows %windir%\system32\drivers\etc\services file.)
-N	Don't print domain name qualification of host names
-O	Do not run the packet-matching code optimizer
-p	Don't put the interface into promiscuous mode
-q	Quick output – print less protocol information
-r <file>	Read packets from file (created with the –w option)
-R	Assume ESP/AH packets to be based on old specs
-s <snaplen>	Snarf snaplen bytes of data from each packet (default is 68)
1518 Max Ethernet Frame (14 byte Ethernet header + 1500 byte IP + 4 byte Ethernet trailer) 64 Min Ethernet Frame (14 byte Ethernet header + 64 byte IP + 4 byte Ethernet trailer) **Note: -s0 mean full ethernet packet**	
-S	Print absolute, rather than relative TCP sequence numbers
-t	Don't print a timestamp on each dump line
-T <type>	Force packets selected by "expressions" to be interpreted the specified type (cnfp, rpc, rtp, snmp, wb)
-tt	Print an unformatted timestamp on each dump line
-ttt	Print a delta (in micro-seconds) between current and previous line on each dump line
-tttt	Print a timestamp in default format proceeded by date on each dump line
-u	Print undecoded NFS handles
-U	
-v	Verbose output (TOS, TTL, IP ID, Fragment Offset, IP Flags, length)
V	
-w <file>	Write the raw packet to file rather than parsing and printing to stdout
-x	Print each packet (minus link level header) in hex
-X	Print each packet in hex and ascii
-y <datalinktype>	

http://www.tcpdump.org/tcpdump_man.html
http://windump.polito.it/docs/manual.htm#Wdump

NGREP

ngrep
<-hXViwqpevxlDtT> <-IO pcap_dump> <-n num> <-d dev> <-A num> <-s snaplen> <-S limitlen>
<match expression>
<bpf filter>

Command Line Options	
-A (num)	is dump num packets after a match
-D	is replay pcap_dumps with their recorded time intervals
-d (device)	is use a device different from the default (pcap)
-e	is show empty packets
-h	is help/usage
-i	is ignore case
-I (file)	is read packet stream from pcap format file pcap_dump (**Capitol i**)
-l	is make stdout line buffered
-n (num)	is look at only num packets
-O (file)	is dump matched packets in pcap format to pcap_dump
-p	is don't go into promiscuous mode
-q	is be quiet
-S (limitlen)	is set the limitlen on matched packets
-s (snaplen)	is set the bpf caplen
-t	is print timestamp every time a packet is matched
-T	is print delta timestamp every time a packet is matched
-V	is version information
-v	is invert match
-w	is word-regex (expression must match as a word)
-X	is interpret match expression as hexadecimal
-x	is print in alternate hexdump format

<match expression>	is either an extended regular expression or a hexadecimal string. see the man page for more information.
<bpf filter>	is any bpf filter statement.

Examples:

ngrep " icmp	print all UDP packets
ngrep " tcp	print all TCP packets
ngrep " udp	print all UDP packets
ngrep " port 53	print all packets to or from TCP or TDP port 53
ngrep " tcp port 53	print all packets to or from only TCP port 53
ngrep - v " tcp port 53	print all packets but those to or from TCP port 53
ngrep 'USER|PASS' tcp port 21	print all packets to or from TCP port 21 where USER or PASS
ngrep 'SSH-' port tcp 22	print all packets to or from TCP port 22 where SSH-
ngrep 'LILWORD' port 138	print Microsoft browsing traffic for NT domain LILWORLD
ngrep -iq 'rcpt to|mail from' tcp port 25	monitor current delivery and print sender and recipients
ngrep 'user' port 110	monitor POP3
ngrep -q 'abcd' icmp	"pinging" host running a Microsoft operating system?
ngep -i -I <input file> "Yahoo"	read from input file and search for case insensitive "Yahoo"

Note: You can use "frame contains <string>" in ethereal to do similar searches.

http://www.packetfactory.net/projects/ngrep/usage.html

Ethereal / Wireshark

Wireless Filters

wlan.fc.wep = 1	Displays all the frames that do have the **WEP** bit (or privacy bit) set
wlan.fc.wep != 1	Displays all the frames that do **NOT** have the **WEP** bit (or privacy bit) set
eapol and eap.type == 17	Will display **Cisco Leap** packets
eap.type == 17 and eap.code == 2	Will display only **Cisco Leap** packets that are **EAP responses**
wlan_mgt.tag.number == 221	Displays **TKIP** or **AES** packets
wlan.bssid == <mac>	Displays only packets that have the specified BSSID
wlan.fc.type_subtype eq 32	Displays only data frames
wlan.fc.type_subtype eq 11 or wlan.fc.type_subtype < 6	Display all probe request and response packets
wlan.fc.type_subtype != 8	Will exclude all the beacon frames from a wireless packet capture
wlan.da[0:1] == 1	Displays packets where the 1st byte in the destination MAC address is 0x01, a multicast address. http://www.iana.org/assignments/multicast-addresses http://www.cavebear.com/Cavebear/ethernet/multicast.html

(wlan.fc.wep != 1) and (wlan.fc.type_subtype eq 32) and !(STP or http or nbus or arp or dns or browser or rip)

General IP Filters

ip.proto == 0x??	Display ICMP if ??=01, TCP if ??= 06 and UDP if ??=11	
tcp.flags.syn == 0	tcp.flags.ack == 0	tcp.flags.fin == 0
tcp.flags.reset == 0	tcp.flags.push == 0	

IPSec Filters

ip.proto == 0x??	Display IPSec AH if ??=51 and ESP if ??=50
isakmp or udp.port eq 500 or udp.port eq 10000 or udp.port eq 5150	Displays ISAKMP traffic (Note 500/CheckPoint, 10000/Cisco, 5150/agere)
isakmp[18] eq 4	Display IPSec ISAKMP packets using aggressive IKE mode

OS Finger Printing

browser.os_major < 5	Display pre-Windows 2000 Clients (Note: eq 5 WK2000 System)

Finds Data In A Packet

data contains "HTTP/1.1 240"	Displays a packets with HTTP error code 240 in the header
http.cookie contains "x"	Displays data "x" list in the cookie

Organizationally Unique Identifiers	1st 24 bits of MAC. OUI to Org. http://standards.ieee.org/regauth/oui/oui.txt

Windows TCP / UDP Ports			
Port	**Protocol**	**Application protocol**	**System service name**
n/a	GRE	GRE (IP protocol 47)	Routing and Remote Access
n/a	ESP	IPsec ESP (IP protocol 50)	Routing and Remote Access
n/a	AH	IPsec AH (IP protocol 51)	Routing and Remote Access
7	TCP	Echo	Simple TCP/IP Services
7	UDP	Echo	Simple TCP/IP Services
9	TCP	Discard	Simple TCP/IP Services
9	UDP	Discard	Simple TCP/IP Services
13	TCP	Daytime	Simple TCP/IP Services
13	UDP	Daytime	Simple TCP/IP Services
17	TCP	Quotd	Simple TCP/IP Services
17	UDP	Quotd	Simple TCP/IP Services
19	TCP	Chargen	Simple TCP/IP Services
19	UDP	Chargen	Simple TCP/IP Services
20	TCP	FTP default data	FTP Publishing Service
21	TCP	FTP control	FTP Publishing Service
21	TCP	FTP control	Application Layer Gateway Service
23	TCP	Telnet	Telnet
25	TCP	SMTP	Simple Mail Transfer Protocol
25	UDP	SMTP	Simple Mail Transfer Protocol
25	TCP	SMTP	Exchange Server
25	UDP	SMTP	Exchange Server
42	TCP	WINS Replication	Windows Internet Name Service
42	UDP	WINS Replication	Windows Internet Name Service
53	TCP	DNS	DNS Server
53	UDP	DNS	DNS Server
53	TCP	DNS	Internet Connection Firewall/Internet Connection Sharing
53	UDP	DNS	Internet Connection Firewall/Internet Connection Sharing
67	UDP	DHCP Server	DHCP Server
67	UDP	DHCP Server	Internet Connection Firewall/Internet Connection Sharing
69	UDP	TFTP	Trivial FTP Daemon Service
80	TCP	HTTP	Windows Media Services
80	TCP	HTTP	World Wide Web Publishing Service
80	TCP	HTTP	SharePoint Portal Server
88	TCP	Kerberos	Kerberos Key Distribution Center
88	UDP	Kerberos	Kerberos Key Distribution Center
102	TCP	X.400	Microsoft Exchange MTA Stacks
110	TCP	POP3	Microsoft POP3 Service
110	TCP	POP3	Exchange Server
119	TCP	NNTP	Network News Transfer Protocol
123	UDP	NTP	Windows Time
123	UDP	SNTP	Windows Time
135	TCP	RPC	Message Queuing
135	TCP	RPC	Remote Procedure Call
135	TCP	RPC	Exchange Server
135	TCP	RPC	Certificate Services
135	TCP	RPC	Cluster Service
135	TCP	RPC	Distributed File System
135	TCP	RPC	Distributed Link Tracking
135	TCP	RPC	Distributed Transaction Coordinator
135	TCP	RPC	Event Log
135	TCP	RPC	Fax Service
135	TCP	RPC	File Replication

The page is from the text provided at http://support.microsoft.com/kb/832017

Windows TCP / UDP Ports			
Port	**Protocol**	**Application protocol**	**System service name**
135	TCP	RPC	Group Policy
135	TCP	RPC	Local Security Authority
135	TCP	RPC	Remote Storage Notification
135	TCP	RPC	Remote Storage Server
135	TCP	RPC	Systems Management Server 2.0
135	TCP	RPC	Terminal Services Licensing
135	TCP	RPC	Terminal Services Session Directory
137	UDP	NetBIOS Name Resolution	Computer Browser
137	UDP	NetBIOS Name Resolution	Server
137	UDP	NetBIOS Name Resolution	Windows Internet Name Service
137	UDP	NetBIOS Name Resolution	Net Logon
137	UDP	NetBIOS Name Resolution	Systems Management Server 2.0
138	UDP	NetBIOS Datagram Service	Computer Browser
138	UDP	NetBIOS Datagram Service	Messenger
138	UDP	NetBIOS Datagram Service	Server
138	UDP	NetBIOS Datagram Service	Net Logon
138	UDP	NetBIOS Datagram Service	Distributed File System
138	UDP	NetBIOS Datagram Service	Systems Management Server 2.0
138	UDP	NetBIOS Datagram Service	License Logging Service
139	TCP	NetBIOS Session Service	Computer Browser
139	TCP	NetBIOS Session Service	Fax Service
139	TCP	NetBIOS Session Service	Performance Logs and Alerts
139	TCP	NetBIOS Session Service	Print Spooler
139	TCP	NetBIOS Session Service	Server
139	TCP	NetBIOS Session Service	Net Logon
139	TCP	NetBIOS Session Service	Remote Procedure Call Locator
139	TCP	NetBIOS Session Service	Distributed File System
139	TCP	NetBIOS Session Service	Systems Management Server 2.0
139	TCP	NetBIOS Session Service	License Logging Service
143	TCP	IMAP	Exchange Server
161	UDP	SNMP	SNMP Service
162	UDP	SNMP Traps Outbound	SNMP Trap Service
389	TCP	LDAP Server	Local Security Authority
389	UDP	LDAP Server	Local Security Authority
389	TCP	LDAP Server	Distributed File System
389	UDP	LDAP Server	Distributed File System
443	TCP	HTTPS	HTTP SSL
443	TCP	HTTPS	World Wide Web Publishing Service
443	TCP	HTTPS	SharePoint Portal Server
443	TCP	RPC over HTTPS	Exchange Server 2003
445	TCP	SMB	Fax Service
445	TCP	SMB	Print Spooler
445	TCP	SMB	Server
445	TCP	SMB	Remote Procedure Call Locator
445	TCP	SMB	Distributed File System
445	TCP	SMB	License Logging Service
445	TCP	SMB	Net Logon
464	TCP	Kerberos Password V5	Net Logon
500	UDP	IPsec ISAKMP	Local Security Authority
515	TCP	LPD	TCP/IP Print Server
548	TCP	File Server for Macintosh	File Server for Macintosh
554	TCP	RTSP	Windows Media Services

The page is from the text provided at http://support.microsoft.com/kb/832017

Windows TCP / UDP Ports			
Port	**Protocol**	**Application protocol**	**System service name**
563	TCP	NNTP over SSL	Network News Transfer Protocol
593	TCP	RPC over HTTPS endpoint mapper	Remote Procedure Call
593	TCP	RPC over HTTPS	Exchange Server
636	TCP	LDAP SSL	Local Security Authority
636	UDP	LDAP SSL	Local Security Authority
993	TCP	IMAP over SSL	Exchange Server
995	TCP	POP3 over SSL	Exchange Server
1067	TCP	Installation Bootstrap Service	Installation Bootstrap protocol server
1068	TCP	Installation Bootstrap Service	Installation Bootstrap protocol client
1270	TCP	MOM-Encrypted	Microsoft Operations Manager 2000
1433	TCP	SQL over TCP	Microsoft SQL Server
1433	TCP	SQL over TCP	MSSQL$UDDI
1434	UDP	SQL Probe	Microsoft SQL Server
1434	UDP	SQL Probe	MSSQL$UDDI
1512	TCP	WINS	Windows Internet Name Service
1512	UDP	WINS	Windows Internet Name Service
1645	UDP	Legacy RADIUS	Internet Authentication Service
1646	UDP	Legacy RADIUS	Internet Authentication Service
1701	UDP	L2TP	Routing and Remote Access
1723	TCP	PPTP	Routing and Remote Access
1755	TCP	MMS	Windows Media Services
1755	UDP	MMS	Windows Media Services
1801	TCP	MSMQ	Message Queuing
1801	UDP	MSMQ	Message Queuing
1812	UDP	RADIUS Authentication	Internet Authentication Service
1813	UDP	RADIUS Accounting	Internet Authentication Service
1863	TCP	Microsoft Messenger Protocol	MSN Messenger
1863	UDP	Microsoft Messenger Protocol	MSN Messenger
1900	UDP	SSDP	SSDP Discovery Service
2101	TCP	MSMQ-DCs	Message Queuing
2103	TCP	MSMQ-RPC	Message Queuing
2105	TCP	MSMQ-RPC	Message Queuing
2107	TCP	MSMQ-Mgmt	Message Queuing
2383	TCP	OLAP Services 9.0	SQL Server: Downlevel OLAP Client Support (SQL 2005)
2393	TCP	OLAP Services 7.0 / 8.0	SQL Server: Downlevel OLAP Client Support
2394	TCP	OLAP Services 7.0 / 8.0	SQL Server: Downlevel OLAP Client Support
2460	UDP	MS Theater	Windows Media Services
2535	UDP	MADCAP	DHCP Server
2701	TCP	SMS Remote Control (control)	SMS Remote Control Agent
2701	UDP	SMS Remote Control (control)	SMS Remote Control Agent
2702	TCP	SMS Remote Control (data)	SMS Remote Control Agent
2702	UDP	SMS Remote Control (data)	SMS Remote Control Agent
2703	TCP	SMS Remote Chat	SMS Remote Control Agent
2703	UPD	SMS Remote Chat	SMS Remote Control Agent
2704	TCP	SMS Remote File Transfer	SMS Remote Control Agent
2704	UDP	SMS Remote File Transfer	SMS Remote Control Agent
2725	TCP	SQL Analysis Services	SQL Analysis Server
2869	TCP	UPNP	Universal Plug and Play Device Host
2869	TCP	SSDP event notification	SSDP Discovery Service
3268	TCP	Global Catalog Server	Local Security Authority
3269	TCP	Global Catalog Server over SSL	Local Security Authority over SSL
3343	UDP	Cluster Services	Cluster Service

The page is from the text provided at http://support.microsoft.com/kb/832017

Windows TCP / UDP Ports			
Port	**Protocol**	**Application protocol**	**System service name**
3389	TCP	Terminal Services	NetMeeting Remote Desktop Sharing
3389	TCP	Terminal Services	Terminal Services
3478	UDP	STUN	OCS A/V Edge Server for STUN Communications
3527	UDP	MSMQ-Ping	Message Queuing
4011	UDP	BINL	Remote Installation
4500	UDP	NAT-T	Local Security Authority
5000	TCP	SSDP legacy event notification	SSDP Discovery Service
5004	UDP	RTP	Windows Media Services
5005	UDP	RTCP	Windows Media Services
5061	TCP	SIP/MTLS	OCS Access Edge Server Communication
5062	TCP	SIP/MTLS	OCS Access Edge Server Authentication
6001	TCP	Information Store	Exchange Server 2003
6002	TCP	Directory Referral	Exchange Server 2003
6004	TCP	DSProxy/NSPI	Exchange Server 2003
8057	TCP	PSOM/MTLS	OCS Web Conferencing Edge Server
42424	TCP	ASP.Net Session State	ASP.NET State Service
50000-59999	TCP	OCS A/V Edge Server	Used for inbound and outbound media transfer
51515	TCP	MOM-Clear	Microsoft Operations Manager 2000
1024-65534	TCP	RPC (DCOM)	Randomly allocated high TCP ports
			Used with RPC endpoint Mapper listening on TCP 135

The page is from the text provided at http://support.microsoft.com/kb/832017

Kerberos

1 Authentication service (AS) Exchange
2 Ticket-Granting Service (TGS) Exchange
3 Client/Server (CS) Excahnge

The AS Excahnge is where the Kerberos key distribution (KDC)

IPC$ Inter-Process Communication

OS Fingerprinting

OS	Version	Platform	TTL	Window	DF	TOS	TCP Options
DC-Osx	1.1-95	Pyramid/NILE	30	8192	n	0	
Windows	9x/NT	Intel	32	5000-9000	y	0	
NetApp	OnTap	5.1.2-5.2.2	54	8760	y	0	
HPJetDirect	?	HP_Printer	59	2100-2150	n	0	
AIX	4.3.X	IBM/RS6000	60	16000-16100	y	0	MSS
AIX	4.2.X	IBM/RS6000	60	16000-16100	n	0	
Cisco	11.2	7507	60		y	0	
DigitalUnix	4	Alpha	60		y	16	
IRIX	6.x	SGI	60		y	16	
OS390	2.6	IBM/S390	60		n	0	
Reliant	5.43	Pyramid/RM1000	60		n	0	
FreeBSD	3.x	Intel	64		y	16	
JetDirect	G.07.x	J311A	64		n	0	
Linux	2.2.x	Intel	64	32120	y	0	MSS, SackOK, wscale, Timestamp, one NOP
Linux	2.4	Intel	64	5840			MSS, SackOK, wscale, Timestamp, one NOP
OpenBSD	2.x	Intel	64		n	16	MSS, Timestamp, wscale, sacks OK, 5 nops
0s/400	r4.4	AS/400	64		y	0	
SCO	R5	Compaq	64		n	0	
Solaris	8	Intel/Sparc	64		y	0	
FTX(Unix)	3.3	STRATUS	64	32678	n	0	
Unisys	x	Mainframe	64	32768	n	0	
Netware	4.11	Intel	128	32000-32768	y	0	
Windows	9x/NT	Intel	128	5000-9000	y	0	
Windows	2000	Intel	128	17000-18000	y	0	MSS, SackOK, 2 NOPs
Windows	XP Pro	Intel	128	???	??	0	MSS, nop, nop, SackOk
Cisco	12	2514	255	3800-5000	n	192	
Solaris	2.x	Intel/Sparc	255	8760	y	0	

ADDITIONAL NOTES

#

Cisco IOS 12.0 normally starts all IP sessions with IP ID of 0

Solaris 8 uses a smaller TTL (64) then Solaris 7 and below (255).

Windows 2000 uses a much larger Window Size then NT.

The page is from the text provided at http://project.honeynet.org/papers/finger/traces.txt

Decimal to Hexadecimal to ASCII Chart

Dec	Hex	ASCII
0	0	NUL
1	1	SOH
2	2	STX
3	3	ETX
4	4	EOT
5	5	ENQ
6	6	ACK
7	7	BEL
8	8	BS
9	9	HT
10	A	LF
11	B	VT
12	C	FF
13	D	CR
14	E	SO
15	F	SI
16	10	DLE
17	11	DC1
18	12	DC2
19	13	DC3
20	14	DC4
21	15	NAK
22	16	SYN
23	17	ETB
24	18	CAN
25	19	EM
26	1A	SUB
27	1B	ESC
28	1C	FS
29	1D	GS
30	1E	RS
31	1F	US

Dec	Hex	ASCII
32	20	SP
33	21	!
34	22	"
35	23	#
36	24	$
37	25	%
38	26	&
39	27	'
40	28	(
41	29	)
42	2A	*
43	2B	+
44	2C	,
45	2D	-
46	2E	.
47	2F	/
48	30	0
49	31	1
50	32	2
51	33	3
52	34	4
53	35	5
54	36	6
55	37	7
56	38	8
57	39	9
58	3A	:
59	3B	;
60	3C	<
61	3D	=
62	3E	>
63	3F	?

Dec	Hex	ASCII
64	40	@
65	41	A
66	42	B
67	43	C
68	44	D
69	45	E
70	46	F
71	47	G
72	48	H
73	49	I
74	4A	J
75	4B	K
76	4C	L
77	4D	M
78	4E	N
79	4F	O
80	50	P
81	51	Q
82	52	R
83	53	S
84	54	T
85	55	U
86	56	V
87	57	W
88	58	X
89	59	Y
90	5A	Z
91	5B	[
92	5C	\
93	5D	]
94	5E	^
95	5F	_

Dec	Hex	ASCII
96	60	'
97	61	a
98	62	b
99	63	c
100	64	DEL
101	65	e
102	66	f
103	67	g
104	68	h
105	69	i
106	6A	j
107	6B	k
108	6C	l
109	6D	m
110	6E	n
111	6F	o
112	70	p
113	71	q
114	72	r
115	73	s
116	74	t
117	75	u
118	76	v
119	77	w
120	78	x
121	79	y
122	7A	z
123	7B	{
124	7C	|
125	7D	}
126	7E	~
127	7F	DEL

Dec	Hex	ASCII
128	80	Ç
129	81	ü
130	82	é
131	83	â
132	84	ä
133	85	à
134	86	å
135	87	ç
136	88	ê
137	89	ë
138	8A	è
139	8B	ï
140	8C	î
141	8D	ì
142	8E	Ä
143	8F	Å
144	90	É
145	91	æ
146	92	Æ
147	93	ô
148	94	ö
149	95	ò
150	96	û
151	97	ù
152	98	ÿ
153	99	Ö
154	9A	Ü
155	9B	¢
156	9C	£
157	9D	¥
158	9E	Pts
159	9F	ƒ

Dec	Hex	ASCII
160	A0	á
161	A1	í
162	A2	ó
163	A3	ú
164	A4	ñ
165	A5	Ñ
166	A6	ª
167	A7	º
168	A8	¿
169	A9	⌐
170	AA	¬
171	AB	½
172	AC	¼
173	AD	¡
174	AE	«
175	AF	»
176	B0	▒
177	B1	▒
178	B2	▓
179	B3	│
180	B4	┤
181	B5	╡
182	B6	╢
183	B7	╖
184	B8	╕
185	B9	╣
186	BA	║
187	BB	╗
188	BC	╝
189	BD	╜
190	BE	╛
191	BF	┐

Dec	Hex	ASCII
192	C0	└
193	C1	┴
194	C2	┬
195	C3	├
196	C4	─
197	C5	┼
198	C6	╞
199	C7	╟
200	C8	╚
201	C9	╔
202	CA	╩
203	CB	╦
204	CC	╠
205	CD	═
206	CE	╬
207	CF	╧
208	D0	╨
209	D1	╤
210	D2	╥
211	D3	╙
212	D4	╘
213	D5	╒
214	D6	╓
215	D7	╫
216	D8	╪
217	D9	┘
218	DA	┌
219	DB	▉
220	DC	▊
221	DD	▋
222	DE	▌
223	DF	▍

Dec	Hex	ASCII
224	E0	α
225	E1	ß
226	E2	Γ
227	E3	π
228	E4	Σ
229	E5	σ
230	E6	µ
231	E7	τ
232	E8	Φ
233	E9	Θ
234	EA	Ω
235	EB	δ
236	EC	∞
237	ED	φ
238	EE	ε
239	EF	∩
240	F0	≡
241	F1	±
242	F2	≥
243	F3	≤
244	F4	⌠
245	F5	⌡
246	F6	÷
247	F7	≈
248	F8	°
249	F9	∙
250	FA	·
251	FB	√
252	FC	ⁿ
253	FD	²
254	FE	■
255	FF	Hardspace

References

1. Cisco, "The ABCs of IP Version 6", 2002
   URL: http://www.cisco.com/application/pdf/en/us/guest/products/iosswrel/c1127/cdccont_0900aecd8018e369.pdf

2. Honeynet Project, "Lists of fingerprints for passive fingerprint monitoring" May 23, 2000
   URL: http://project.honeynet.org/papers/finger/traces.txt

3. IANA, "ICMP TYPE NUMBERS", January 27, 2005
   URL: http://www.iana.org/assignments/icmp-parameters

4. IANA, "IP OPTION NUMBERS", June 06, 2001
   URL: http://www.iana.org/assignments/ip-parameters

5. IANA, "PROTOCOL NUMBERS", October 18, 2004
   URL: http://www.iana.org/assignments/protocol-numbers

6. IEEE, "Get IEEE 802" March, 9 2005
   URL: http://standards.ieee.org/getieee802/

7. IEEE, "Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications", June 12, 2003
   URL: http://standards.ieee.org/getieee802/download/802.11-1999.pdf

8. Kismet, "KISMET PANELS INTERFAC",
   URL: http://www.kismetwireless.net/

9. Packetfactory, "ngrep - network grep",
   URL: http://www.packetfactory.net/projects/ngrep/usage.html

10. POLITECNICO DI TORINO, "WinDump: tcpdump for Windows", March 14, 2002
    URL: http://windump.polito.it/docs/manual.htm#Wdump.

11. RFC Editor, "RFC Editor Homepage", August 12, 2002
    URL: http://www.rfc-editor.org/

12. SANS Institute's, "Audit 511: Auditing Wireless Networks, Part 1", 2005

13. SANS Institute's, "TCP/IP and tcpdump Pocket Reference Guide", June 2002
    URL: http://www.sans.org/resources/tcpip.pdf

14. tcpdump.org, "tcpdump man pages"
    URL: http://www.tcpdump.org/tcpdump_man.html

15. Todd Lammle, "CCNA: Cisco Certified Network Associate Study Guide"
    Wiley Publishing, Inc., Copyright 2007