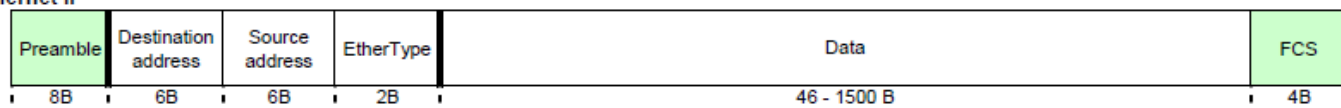
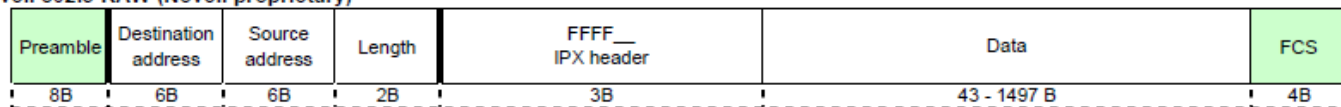


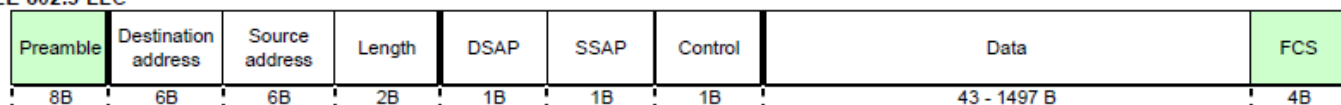
Ethernet II



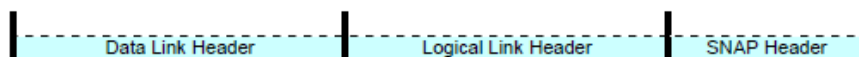
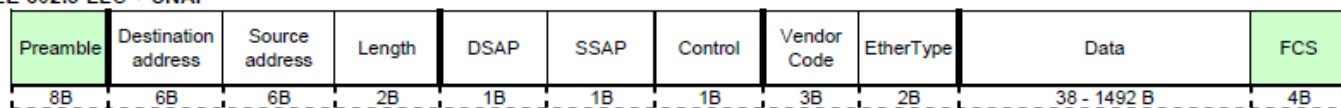
Novell 802.3 RAW (Novell proprietary)



IEEE 802.3 LLC



IEEE 802.3 LLC + SNAP



802.2 LLC Service Access Points (SAPs)

IEEE SAPs

Hex	Dec	Function
00	0	Null SAP
02	2	LLC Sublayer Management / Individual
03	3	LLC Sublayer Management / Group
06	6	IP (DoD Internet Protocol)
0E	14	PROWAY (IEC 955) Network Management, Maintenance and Installation
42	66	BPDU (Bridge PDU / 802.1 Spanning Tree)
4E	78	MMS (Manufacturing Message Service) EIA-RS 511
5E	94	ISI IP
7E	126	X.25 PLP (ISO 8208)
8E	142	PROWAY (IEC 955) Active Station List Maintenance
AA	170	SNAP (Sub-Network Access Protocol / non-IEEE SAPs)
E0	224	IPX (Novell NetWare)
F4	244	LAN Management
FE	254	ISO Network Layer Protocols
FF	255	Global DSAP

EtherType values


google for "IANA Ether Types" for up-to-date list

Hex	Dec	Description
0200	0512	XEROX PUP
0201	0513	PUP Addr Trans
0800	2048	Internet IP (IPv4)
0801	2049	X.75 Internet
0805	2053	X.25 Level 3
0806	2054	ARP (Address Resolution Protocol)
8035	32821	Reverse ARP
809B	32923	Appletalk
80F3	33011	AppleTalk AARP (Kinetics)
8100	33024	IEEE 802.1Q VLAN-tagged frames
8137	33079	Novell IPX
86DD	34525	IPv6
880B	34827	PPP
8847	34887	MPLS
8848	34888	MPLS with upstream-assigned label
8863	34915	PPPoE Discovery Stage
8864	34916	PPPoE Session Stage

UDP Header	
Bit Number	
1 1 1 1 1 1 1 1 1 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	
Source Port	Destination Port
Length	Checksum
UDP Header Information	
Common UDP Well-Known Server Ports	
7 echo	138 netbios-dgm
19 chargen	161 snmp
37 time	162 snmp-trap
53 domain	500 isakmp
67 bootps (DHCP)	514 syslog
68 bootpc (DHCP)	520 rip
69 tftp	33434 traceroute
137 netbios-ns	
Length	
(Number of bytes in entire datagram including header; minimum value = 8)	
Checksum	
(Covers pseudo-header and entire UDP datagram)	

ARP	
Bit Number	
1 1 1 1 1 1 1 1 1 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	
Hardware Address Type	Protocol Address Type
H/w Addr Len	Prot. Addr Len
Source Hardware Address	
Source Hardware Addr (cont.)	Source Protocol Address
Source Protocol Addr (cont.)	Target Hardware Address
Target Hardware Address (cont.)	
Target Protocol Address	
ARP Parameters (for Ethernet and IPv4)	
Hardware Address Type	
1 Ethernet	
6 IEEE 802 LAN	
Protocol Address Type	
2048 IPv4 (0x0800)	
Hardware Address Length	
6 for Ethernet/IEEE 802	
Protocol Address Length	
4 for IPv4	
Operation	
1 Request	
2 Reply	

DNS	
Bit Number	
1 1 1 1 1 1	
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5	
ID.	
QR	Opcode
AA	TC
RD	RA
Z	RCODE
QDCOUNT	
ANCOUNT	
NSCOUNT	
ARCOUNT	
Question Section	
Answer Section	
Authority Section	
Additional Information Section	
DNS Parameters	
Query/Response	
0 Query	
1 Response	
Opcode	
0 Standard query (QUERY)	
1 Inverse query (IQUERY)	
2 Server status request (STATUS)	
AA	
(1 = Authoritative Answer)	
TC	
(1 = TrunCation)	
RD	
(1 = Recursion Desired)	
RA	
(1 = Recursion Available)	
Z	
(Reserved; set to 0)	
Response code	
0 No error	
1 Format error	
2 Server failure	
3 Non-existent domain (NXDOMAIN)	
4 Query type not implemented	
5 Query refused	
QDCOUNT	
(No. of entries in Question section)	
ANCOUNT	
(No. of resource records in Answer section)	
NSCOUNT	
(No. of name server resource records in Authority section)	
ARCOUNT	
(No. of resource records in Additional Information section.)	



TCP/IP and tcpdump

POCKET REFERENCE GUIDE

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

tcpdump Usage	
tcpdump [-aenStvx] [-F file]	
[-i int] [-r file] [-s snaplen]	
[-w file] ['filter_expression']	
-e Display data link header.	
-F Filter expression in file.	
-i Listen on int interface.	
-n Don't resolve IP addresses.	
-r Read packets from file.	
-s Get snaplen bytes from each packet.	
-S Use absolute TCP sequence numbers.	
-t Don't print timestamp.	
-v Verbose mode.	
-w Write packets to file.	
-x Display in hex.	
-X Display in hex and ASCII.	

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

ICMP

Bit Number

1111111111222222222233
01234567890123456789012345678901

Type	Code	Checksum
Other message-specific information...		

Type Name/Codes (Code=0 unless otherwise specified)

0	Echo Reply
3	Destination Unreachable
0	Net Unreachable
1	Host Unreachable
2	Protocol Unreachable
3	Port Unreachable
4	Fragmentation Needed & DF Set
5	Source Route Failed
6	Destination Network Unknown
7	Destination Host Unknown
8	Source Host Isolated
9	Network Administratively Prohibited
10	Host Administratively Prohibited
11	Network Unreachable for TOS
12	Host Unreachable for TOS
13	Communication Administratively Prohibited
4	Source Quench
5	Redirect
0	Redirect Datagram for the Network
1	Redirect Datagram for the Host
2	Redirect Datagram for the TOS & Network
3	Redirect Datagram for the TOS & Host
8	Echo
9	Router Advertisement
10	Router Selection
11	Time Exceeded
0	Time to Live exceeded in Transit
1	Fragment Reassembly Time Exceeded
12	Parameter Problem
0	Pointer indicates the error
1	Missing a Required Option
2	Bad Length
13	Timestamp
14	Timestamp Reply
15	Information Request
16	Information Reply
17	Address Mask Request
18	Address Mask Reply
30	Traceroute

PING (Echo/Echo Reply)

Bit Number

1111111111222222222233
01234567890123456789012345678901

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

IP Header

Bit Number

1111111111222222222233
01234567890123456789012345678901

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

IP Header Contents

```

Version
4 IP version 4

Internet Header Length
Number of 32-bit words in IP header; minimum
value = 5 (20 bytes) & maximum value = 15 (60 bytes)

Type of Service (PreDTRCx) --> Differentiated Services
Precedence (000-111) 000
D (1 = minimize delay) 0
T (1 = maximize throughput) 0
R (1 = maximize reliability) 0
C (1 = minimize cost) 1 = ECN capable
x (reserved and set to 0) 1 = congestion experienced

Total Length
Number of bytes in packet; maximum length = 65,535

Flags (xDM)
x (reserved and set to 0)
D (1 = Don't Fragment)
M (1 = More Fragments)

Fragment Offset
Position of this fragment in the original datagram,
in units of 8 bytes

Protocol
1 ICMP 17 UDP 57 SKIP
2 IGMP 47 GRE 88 EIGRP
6 TCP 50 ESP 89 OSPF
9 IGRP 51 AH 115 L2TP

Header Checksum
Covers IP header only

Addressing
NET_ID RFC 1918 PRIVATE ADDRESSES
0-127 Class A 10.0.0.0-10.255.255.255
128-191 Class B 172.16.0.0-172.31.255.255
192-223 Class C 192.168.0.0-192.168.255.255
224-239 Class D (multicast)
240-255 Class E (experimental)
HOST_ID
0 Network value; broadcast (old)
255 Broadcast

Options (0-40 bytes; padded to 4-byte boundary)
0 End of Options list 68 Timestamp
1 No operation (pad) 131 Loose source route
7 Record route 137 Strict source route

```

TCP Header

Bit Number

1111111111222222222233
01234567890123456789012345678901

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

TCP Header Contents

Common TCP Well-Known Server Ports			
7 echo	110 pop3		
19 chargen	111 sunrpc		
20 ftp-data	119 nntp		
21 ftp-control	139 netbios-ssn		
22 ssh	143 imap		
23 telnet	179 bgp		
25 smtp	389 ldap		
53 domain	443 https (ssl)		
79 finger	445 microsoft-ds		
80 http	1080 socks		
Offset			
Number of 32-bit words in TCP header; minimum value = 5			
Reserved			
4 bits; set to 0			
ECN bits (used when ECN employed; else 00)			
CWR (1 = sender has cut congestion window in half)			
ECN-Echo (1 = receiver cuts congestion window in half)			
Flags (UAPRSF)			
U (1 = Urgent pointer valid)			
A (1 = Acknowledgement field value valid)			
P (1 = Push data)			
R (1 = Reset connection)			
S (1 = Synchronize sequence numbers)			
F (1 = no more data; Finish connection)			
Checksum			
Covers pseudoheader and entire TCP segment			
Urgent Pointer			
Points to the sequence number of the byte following urgent data.			
Options			
0 End of Options list	3 Window scale		
1 No operation (pad)	4 Selective ACK ok		
2 Maximum segment size	8 Timestamp		

Options Headers (Hop-by-Hop Options and Destination Options)

																Bit Number															
																1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 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															

Next Header	Hdr Ext Len	
Options		

}

4

8

Next Header
8-bit identifier for the header immediately following this one. Uses the same codes as the main IPv6 header.

Hdr Ext Len
8-bit length of the Hop-by-Hop Options header in 8-octet units not including the first 8 octets, i.e., (length in octets-8)/8.

Options
Variable-length field, containing the options.
NOTE: length **must** be a multiple of 8 octets long.

Option Encoding:

																1 1 1 1 1 1 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 ...															
Option Type								Opt Data Len								Option Data															
N W C T T T T T																															

Option Type	8-bit Identifier	
WW		indicate what to do if this option is not recognized:
00		skip this option and continue processing the header.
01		discard packet.
10		discard packet and send an ICMP Parameter Problem code 2 back to the source address pointing to the unrecognized Option Type.
11		discard packet and, if destination is not a multicast address, behave like type 10.
C		indicates whether the option data for this option can change en-route to the destination. Relevant if, in particular, an AH is present.
0		no change
1		can change
TTTT		rest of the option type code

Opt Data Len
8-bit length of the Option Data field of this option, in octets.

Option Data
Variable-length field.

Options which must be implemented:

I) Pad1 option, special case:
 0 1 2 3 4 5 6 7

NOTE: no length or field values!

II) PadN option:
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5
 1 Opt Data Len Option Data

Routing Header (similar to IPv4 LSRR and RR options)

Bit Number

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



Incidents@sans.org • +1 317.580.9756 • <http://www.sans.org> • <http://www.incidents.org>

```

tcpdump Usage

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

-e Display data link header.
-F Filter expression in file.
-i Listen on int interface.
-n Don't resolve IP addresses.
-r Read packets from file.
-s Get snaplen bytes from each packet
-S Use absolute TCP sequence numbers.
-t Don't print timestamp.
-v Verbose mode.
-w Write packets to file.
-x Display in hex.
-X Display in hex and ASCII.

```

Acronyms

AH	Authentication Header (RFC 2402)	ISAKMP	Internet Security Association & Key Management Protocol (RFC 2408)
ARP	Address Resolution Protocol (RFC 826)	L2TP	Layer 2 Tunneling Protocol (RFC 2661)
BGP	Border Gateway Protocol (RFC 1771)	NNTP	Network News Transfer Protocol (RFC 977)
CWR	Congestion Window Reduced (RFC 2401)	OSPF	Open Shortest Path First (RFC 1583)
DF	Don't Fragment bit (IP)	PO2P	Peer-to-Peer Protocol v3 (RFC 1460)
DHCP	Dynamic Host Configuration Protocol (RFC 2131)	RCF	Request for Comments
DNS	Domain Name System (RFC 1035)	RIP	Routing Information Protocol (RFC 2453)
EON	Explicit Congestion Notification (RFC 3168)	LDAP	Lightweight Directory Access Protocol (RFC 2251)
EGRP	Extended IGRP (Cisco)	SKIP	Simple Key-Management for Internet Protocols
ESP	Encapsulating Security Payload (RFC 2406)	SMTP	Simple Mail Transfer Protocol (RFC 821)
FTP	File Transfer Protocol (RFC 959)	SNMP	Simple Network Management Protocol (RFC 1157)
GRE	Generic Routing Encapsulation (RFC 2794)	SSH	Secure Shell
HTTP	Hypertext Transfer Protocol (RFC 1945)	SSL	Secure Sockets Layer (Netscape)
ICMP	Internet Control Message Protocol (RFC 792)	TCP	Transmission Control Protocol (RFC 793)
IGMP	Internet Group Management Protocol (RFC 2236)	TFTP	Trivial File Transfer Protocol (RFC 1350)
IGRP	Interior Gateway Routing Protocol (Cisco)	TOS	Type of Service field (IP)
IMAP	Internet Message Access Protocol (RFC 2060)	UDP	User Datagram Protocol (RFC 768)
IP	Internet Protocol (RFC 791)		

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

©SANS Institute June 2004

DNS

Bit Number

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
										1	1	1	1	1	1

ID.

QR	Opcode	AA	TC	RD	RA	Z	RCODE
QDCOUNT							
ANCOUNT							
NSCOUNT							
ARCOUNT							
Question Section							
Answer Section							
Authority Section							
Additional Information Section							

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

(No. of entries in Question section)

ANCOUNT

(No. of resource records in Answer section)

NSCOUNT

(No. of name server resource records in Authority section)

ARCOUNT

(No. of resource records in Additional Information section).

IPv6 Header

Bit Number

01234567890123456789012345678901

Version

Traffic Class

Flow Label

Payload Length

Next Header

Hop Limit

Source Address

Destination Address

481216202428323640

Version

Traffic Class

Flow Label

Payload Length

Next Header

Source Address

Destination Address

Version

Traffic Class

Flow Label

Payload Length

Next Header

Source Address

Destination Address

TCP Header

Bit Number

01234567890123456789012345678901

Source Port

Destination Port

Sequence Number

Acknowledgment Number

Offset

Reserved

Flags

Window

Checksum

Urgent Pointer

Options (optional)

4812162024

Common TCP Well-Known Server Ports

Offset

Reserved

Flags

Window

Checksum

Urgent Pointer

Options (optional)

Common TCP Well-Known Server Ports

Offset

Reserved

Flags

Window

Checksum

Urgent Pointer

Options (optional)

UDP Header

Bit Number

01234567890123456789012345678901

Source Port

Destination Port

Length

Checksum

48

Common UDP Well-Known Server Ports

Length

Checksum

ICMPv6 (header type 58)

Bit Number

01234567890123456789012345678901

Type

Code

Checksum

4

Type

Code

Checksum

Type

Code

Checksum

Fragment Header

Bit Number

01234567890123456789012345678901

Next Header

Reserved

Fragment Offset

Res

M

Identification

48

Next Header

Reserved

Fragment Offset

Res

M

Identification

Next Header

Reserved

Fragment Offset

Res

M

Identification

Checksums

Bit Number

01234567890123456789012345678901

Source Address

Destination Address

Upper-Layer Packet Length

Must be Zero (MBZ)

Next Header

48323640

Source Address

Destination Address

Upper-Layer Packet Length

Must be Zero (MBZ)

Next Header

Source Address

Destination Address

Upper-Layer Packet Length

Must be Zero (MBZ)

Next Header