Frameanalyse

Ethernet II:

Preamble	Destination MAC address	Source MAC address	Type	User Data	Frame Check Sequence (FCS)
8 Byte	6 Byte	6 Byte	2 Byte	46 - 1500 Byte	4 Byte

Wireshark zeigt nur die grünen Felder an. Für Ethernet_II ist der Wert des Typ/Längenfeldes > 1500 (dezimal)
Typecodes:

0-1500 (dez)	length field (IEEE 802.3 and/or 802.2)
0x0800	IP(v4), Internet Protocol version 4
0x0806	ARP, Address Resolution Protocol
0x8100	802.1Q Virtual LAN
0x8137	IPX, Internet Packet eXchange (Novell)
0x86dd	IPv6, Internet Protocol version 6

Ethernet IEEE 802.3 mit LLC: (IEEE 802.2 Logical Link Control)

Bitfolge 1010101010..	Ethernet - Frame min. 64 Byte max. 1518 Byte								Inter Frame Gap 9,6µs
Preamble und SFD	6 Byte Dest.-Addr	6 Byte Source-Addr	2 Byte Length	1 Byte DSAP	1 Byte SSAP	1 Byte Control	min 42 Bytes max 1497 Bytes Daten	4 Byte FCS	

Wireshark zeigt nicht an: Preamble, SFD, FCS, Inter Frame Gap (s.o.)
Typecodes für DSAP/SSAP:

0x04	IBM SNA Path Control (individual)
0x05	IBM SNA Path Control (group)
0x06	ARPANET Internet Protocol (IP)
0x42	Spanning Tree Protokoll (BPDU)
0x80	Xerox Network Systems (XNS)
0x98	ARPANET Address Resolution Protocol (ARP)
0xAA	IEEE Ethernet 802.3 SNAP-Format
0xE0	Novell NetWare

Ethernet mit eingeschobenem VLAN-Tag (IEEE 802.1q):

Bitfolge 1010101010..		Ethernet - Frame min. 68 Byte max. 1522 Byte							Inter Frame Gap 9,6µs
Preamble	SFD	6 Byte Dest.-Addr	6 Byte Source-Addr	4 Byte Tag	2 Byte Type	min 46 Bytes max 1500 Bytes Daten	4 Byte FCS		

Zwischen der Source-MAC-Adresse und dem 2-Byte-Typ/Längenfeld wird der 4 Byte VLAN-Header eingeschoben. Wireshark zeigt nicht an: Preamble, SFD, FCS, Inter Frame Gap (s.o.). Dieses Beispiel zeigt einen Ethernet_II mit VLAN.

ARP/RARP:

16 32 bits

<table>
<tr><td colspan="2">Hardware Type</td><td>Protocol Type</td></tr>
<tr><td>HLen (8)</td><td>Plen (8)</td><td>Operation</td></tr>
<tr><td colspan="3">Sender Hardware Address</td></tr>
<tr><td colspan="3">Sender Protocol Address</td></tr>
<tr><td colspan="3">Target Hardware Address</td></tr>
<tr><td colspan="3">Target Protocol Address</td></tr>
</table>

Feld „Operation“:

1	ARP request.
2	ARP response.
3	RARP request.
4	RARP response.

IPv4:

4 8 16 32 bits

<table>
<tr><td>Version</td><td>IHL</td><td>Type of service</td><td colspan="2">Total length</td></tr>
<tr><td colspan="3">Identification</td><td>Flags</td><td>Fragment offset</td></tr>
<tr><td colspan="2">Time to live</td><td>Protocol</td><td colspan="2">Header checksum</td></tr>
<tr><td colspan="5">Source address</td></tr>
<tr><td colspan="5">Destination address</td></tr>
<tr><td colspan="5">Option + Padding (nur wenn IHL > 5!)</td></tr>
</table>

IHL (Internet Header Length): Länge des Headers. Wert 5 heißt 5*4 = 20 Byte!

→ Also kein „Option“-Feld !

Protokoll-Feld:

Dezimal	**Hex**	**Protokoll**
1	0x01	ICMP
4	0x04	IP
6	0x06	TCP
17	0x11	UDP
27	0x1B	RDP
41	0x29	Ipv6
50	0x32	ESP
51	0x33	AH
58	0x3A	IPv6-ICMP

IPv6:

4	4	16	24	32 bits
Ver.	Priority	Flow label		
Payload length			Next header	Hop limit
Source address (128 Bits)				
Destination address (128 bits)				

Version: immer 6

Next header: siehe IPv4 Protokoll-Feld

ICMP:

8	16	32 bits
Type	Code	Checksum
Identifier		Sequence number
Address mask		

Type	Code	Description
0		Echo reply.
3		Destination unreachable.
3	0	Net unreachable.
3	1	Host unreachable.
3	2	Protocol unreachable.
3	3	Port unreachable.
5		Redirect.
5	0	Redirect datagrams for the network.
5	1	Redirect datagrams for the host.
5	2	Redirect datagrams for the type of service and network.
5	3	Redirect datagrams for the type of service and host.
8		Echo. (request)
11		Time exceeded.
11	0	Time to live exceeded in transit.
135	0	Neighbor Solicitation
136	0	Neighbor advertisement

ICMPv6:

8	16	32 bits
Type	Code	Checksum

Type/Code siehe oben (ICMP).

UDP:

16	32 bits
Source port	Destination port
Length	Checksum

TCP:

<table>
<tr><th colspan="8">16</th><th>32 bits</th></tr>
<tr><td colspan="8">Source port</td><td>Destination port</td></tr>
<tr><td colspan="9">Sequence number</td></tr>
<tr><td colspan="9">Acknowledgement number</td></tr>
<tr><td>Offset</td><td>Resrvd</td><td>U</td><td>A</td><td>P</td><td>R</td><td>S</td><td>F</td><td>Window</td></tr>
<tr><td colspan="8">Checksum</td><td>Urgent pointer</td></tr>
<tr><td colspan="9">Option + Padding (nur selten)</td></tr>
</table>

Well-Known-Ports (TCP/UDP):

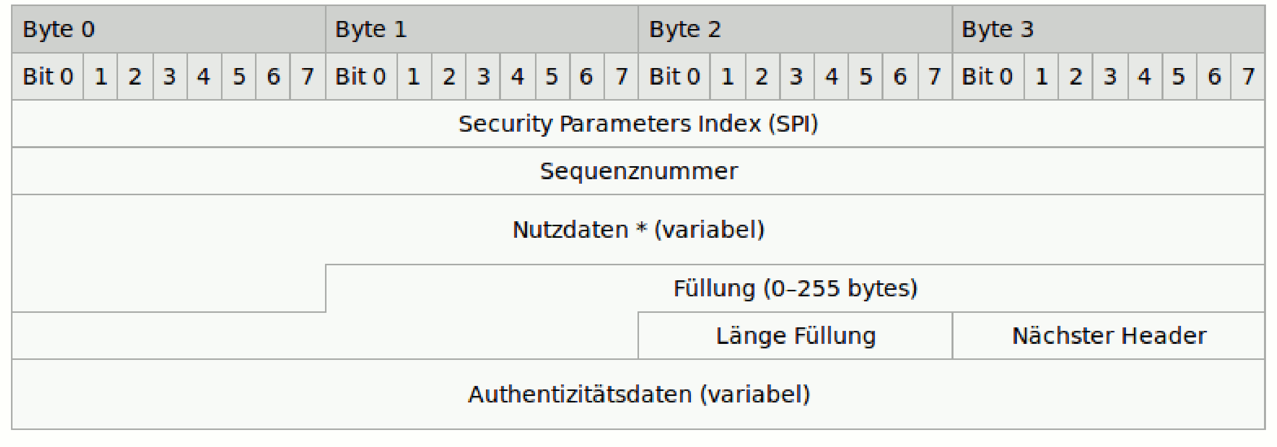
22	ssh	123	ntp
23	telnet	143	imap
25	smtp	161	snmp
53	dns	162	snmptrap
67	dhcp Server/Relay	443	https
68	dhcp Client	546	Dhcp-v6 Client
69	tftp	547	Dhcp-v6 Server/Relay
80	http		

IPSec → AH-Header

Byte 0								Byte 1								Byte 2								Byte 3							
Bit 0	1	2	3	4	5	6	7	Bit 0	1	2	3	4	5	6	7	Bit 0	1	2	3	4	5	6	7	Bit 0	1	2	3	4	5	6	7
Nächster Header								Nutzdaten-Länge								reserviert															
Security Parameters Index (SPI)																															
Feld mit Sequenznummer																															
Authentizitätsdaten (variabel)																															

Next-Header: Werte wie im Protokoll-Feld des IP-Headers (s.o.)

IPSec → ESP-Header



Byte 0								Byte 1								Byte 2								Byte 3							
Bit 0	1	2	3	4	5	6	7	Bit 0	1	2	3	4	5	6	7	Bit 0	1	2	3	4	5	6	7	Bit 0	1	2	3	4	5	6	7
Security Parameters Index (SPI)																															
Sequenznummer																															
Nutzdaten * (variabel)																															
								Füllung (0–255 bytes)																							
																Länge Füllung								Nächster Header							
Authentizitätsdaten (variabel)																															

Next-Header: Werte wie im Protokoll-Feld des IP-Headers (s.o.)