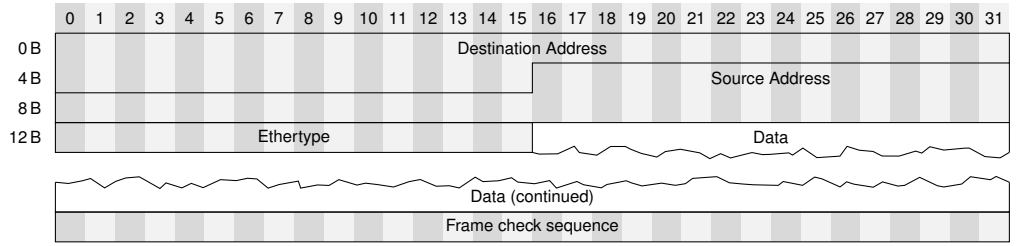
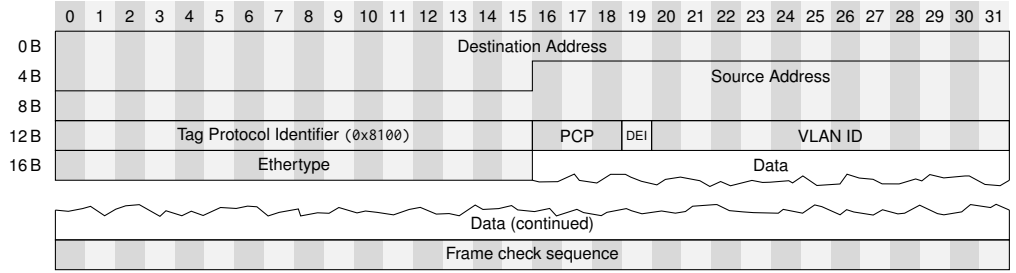
Chair of Network Architectures and Services
Department of Informatics
Technical University of Munich

Ethernet / IEEE 802.3 / IEEE 802.1q Frame and Ethertypes



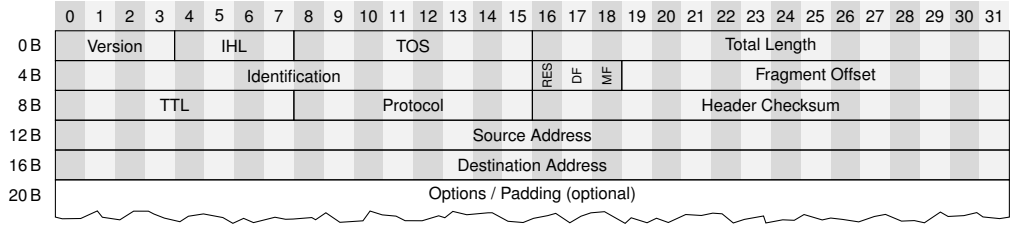
IEEE 802.3 Header with FCS



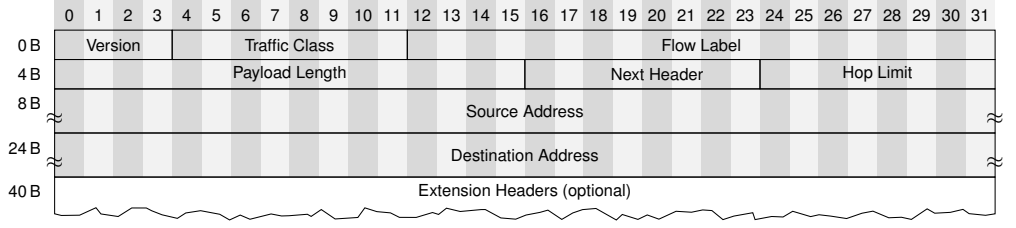
IEEE 802.1q Header with FCS

Ethertype	Keywrd	Protocol
0x0800	IPv4	Internet Protocol, Version 4
0x0806	ARP	Address Resolution Protocol
0x0842	WoL	Wake-on-LAN Magic Packet
0x8035	RARP	Reverse Address Resolution Protocol
0x814c	SNMP	Simple Network Management Protocol
0x86dd	IPv6	Internet Protocol, Version 6

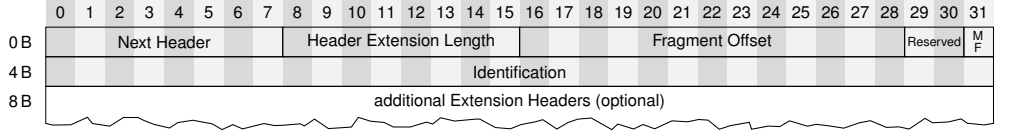
IPv4/6 Headers



IPv4 Header



IPv6 Header

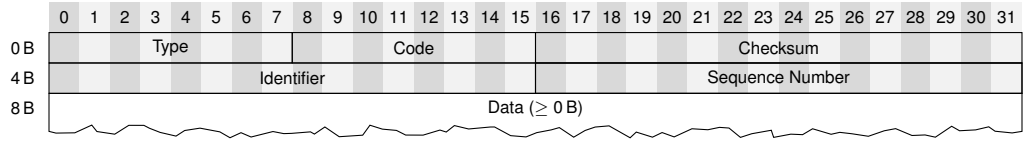


IPv6 Fragmentation Header

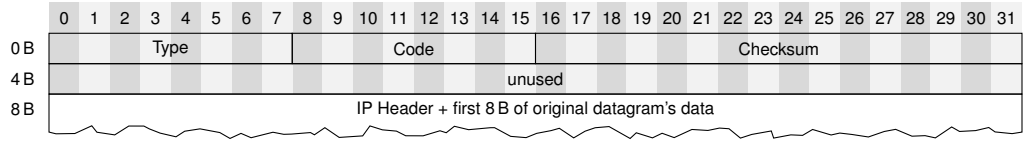
IPv4/6 IP Protocol Numbers/Next Header

No / NH	Protocol
0x01	ICMPv4 (Internet Control Message)
0x04	IPv4 encapsulation
0x06	TCP (Transmission Control)
0x11	UDP (User Datagram)
0x2c	IPv6 Fragmentation Header
0x2f	GRE (General Routing Encapsulation)
0x3a	ICMPv6 (ICMP for IPv6)
0x84	SCTP (Stream Control Transmission)

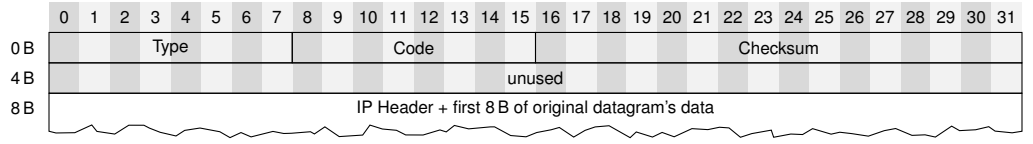
ICMPv4



ICMPv4 Echo Request/Reply



ICMPv4 Time Exceeded



ICMPv4 Destination Unreachable

Type	Code	Description
0 – Echo Reply	0	Echo reply
1 and 2		*Reserved*
3 – Destination Unreachable	0	Destination network unreachable
	1	Destination host unreachable
	2	Destination protocol unreachable
	3	Destination port unreachable
	4	Fragmentation required, and DF flag 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
	14	Host Precedence Violation
	15	Precedence cutoff in effect
4 – Source Quench	0	Source quench (congestion control)
5 – Redirect Message	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 Request	0	Echo request
11 – Time Exceeded	0	TTL expired in transit
	1	Fragment Reassembly Time Exceeded

Selected ICMPv4 types/codes

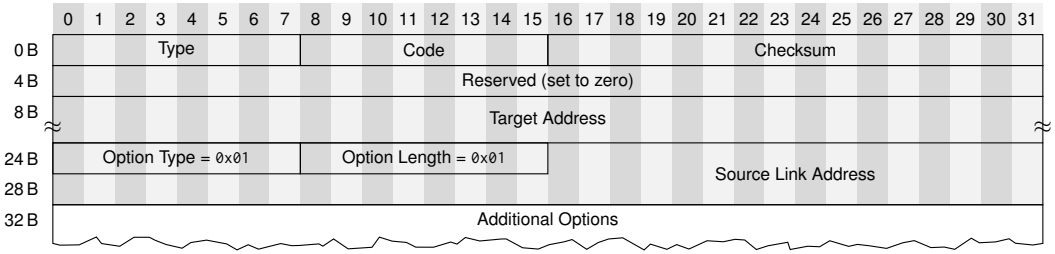
ACN - WS 2022

ICMPv6

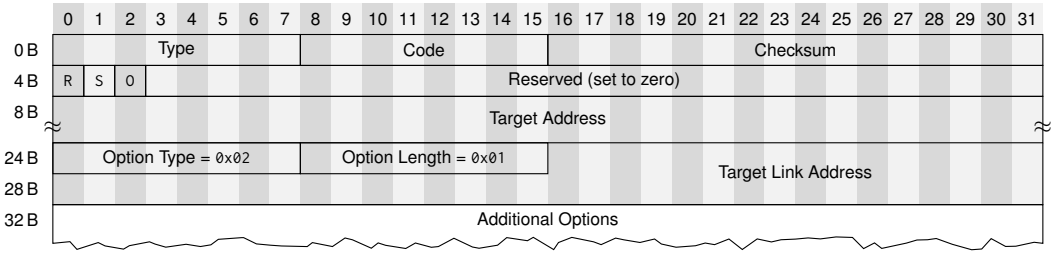
Note: The following ICMPv6 messages are identical to their ICMPv4 counterparts: *

- Echo Request / Reply
- Destination Unreachable
- Time Exceeded

Restrictions for minimal length and alignment (padding) apply to the ICMPv6 types / codes (see below).



Neighbor Solicitation



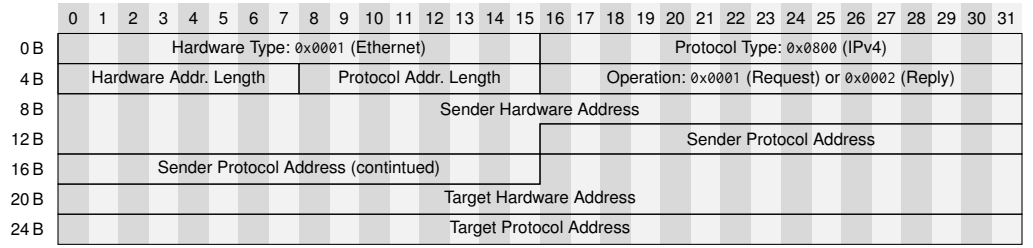
Flags: R = Router, S = Solicited, O = Override

Neighbor Advertisement

Type	Code	Description
0		*Reserved*
1 – Destination Unreachable	0	No route to destination
	1	Communication administratively prohibited
	2	Beyond scope of source address
	3	Address unreachable
	4	Port unreachable
	5	Source address failed ingress/egress policy
	6	Reject route to destination
	7	Error in source routing header
2 – Packet too big	0	Packet too big
3 – Time Exceeded	0	Hop limit exceeded in transit
	1	Fragment reassembly time exceeded
128 – Echo Request	0	Echo Request
129 – Echo Reply	0	Echo Reply
133 – Router Solicitation	0	*Neighbor Discovery Protocol (NDP)*
134 – Router Advertisement	0	*Neighbor Discovery Protocol (NDP)*
135 – Neighbor Solicitation	0	*Neighbor Discovery Protocol (NDP)*
136 – Neighbor Advertisement	0	*Neighbor Discovery Protocol (NDP)*
137 – Redirect Message	0	*Neighbor Discovery Protocol (NDP)*

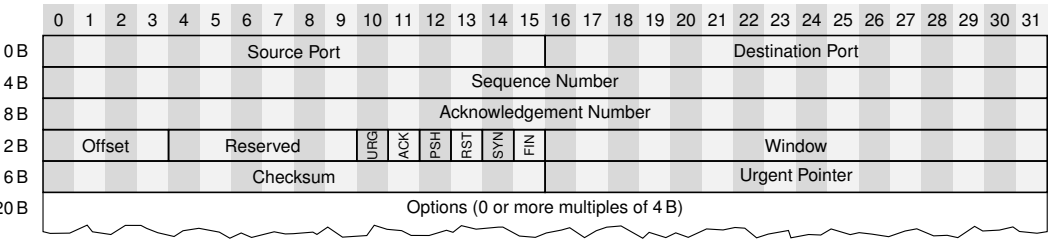
Selected ICMPv6 types/codes

ARP

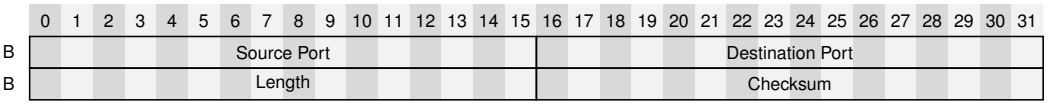


ARP Packet Format

TCP/UDP header and selected well-known ports



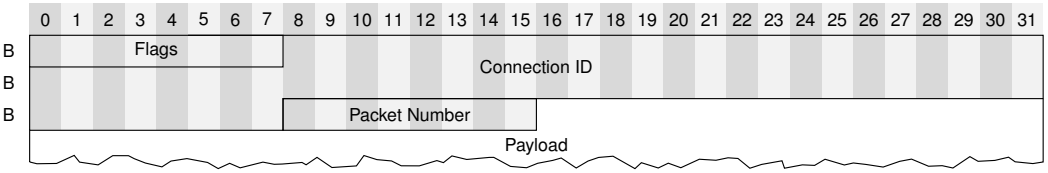
TCP Header



UDP Header

Port	Service Name	Port	Service Name
20/21	ftp	68	bootpc
22	ssh	80	http
23	telnet	443	https (tcp) / quic (udp)
25	smtp	546	dhcpv6-client
53	domain (dns)	547	dhcpv6-server
67	bootps	853	dns over tls

QUIC



QUIC Header

Disclaimer: QUIC allows several different header formats, depending on the used version and the given flags some fields can be omitted. However, for the exam you only need this header format.

ACN - WS 2022