Extension Headers

	0	1	2	3
0	NH	Length	Options…	
1	Options			

NH: Next Header following this Extension header.
Length: Length of this header in 8 byte units.
0 = 8 bytes
Options: depends on header type.

Extension Headers

Dec.	Hex	Header
0	0x00	Hop-By-Hop (HH)
43	0x2b	Routing Header (RH)
44	0x2c	Fragmentation Header (FH)
50	0x32	Encap. Security Payload (ESP)
51	0x33	Authentication Header (AH)
58	0x3a	ICMPv6 (ICMP6)
59	0x3b	No Next Header
60	0x3c	Destination Options (DH)

Note: TCP(6), UDP (17,0x11), and any other protocols must be the LAST header. Each extension header, but the destination header, may only appear once. The Hop-By-Hop header must be first. The order of the other headers is only recommended.

Options (HH, RH, DH)

0	1	
Type	Length	Value…

Length in bytes without type/length bytes.
Padding may be needed to fill multiple of 8 bytes.
Type 0: Pad 1 (Pad 1 byte)
Type 1: Pad n (pad multiple bytes)

SANS Technology Institute

The best. Made better.

The SANS Technology Institute develops leaders to strengthen enterprise and global information security. STI educates managers and engineers in information security practices and techniques, attracts top scholar-practitioners as faculty, and engages both students and faculty in real-world applied research.
Learn more at https://www.sans.edu

INTERNET STORM CENTER

A collaborative network security community. Learn about current issues, correlate your logs with others, free API and other resources to enhance your understanding of current threats.
https://isc.sans.edu

SANS

IPv6 Pocket Guide

Version January 2024

POCKET REFERENCE GUIDE

Please submit comments and corrections to jullrich@sans.edu
https://www.sans.org/posters/ipv6-pocket-guide

COURSES & GIAC CERTIFICATIONS

SEC 503
Network Monitoring and Threat Detection In-Depth

SEC 401
Security Essentials - Network, Endpoint, and Cloud

SEC 573
Automating Information Security with Python

SEC 560
Enterprise Penetration Testing

FOR 572
Network Forensics

LDR 512
Security Leadership Essentials for Managers

tcpdump usage

Avoid using “proto” as filter. “proto” will only check the IPv6 header’s “Next Header” field and the NH field of a fragment header. Use “protochain” instead.

Avoid the use of tcp[] / icmp6[] / udp[]

use ‘ip6’ instead of ‘ip’ and ‘icmp6’ instead of ‘icmp’ (ip and icmp are IPv4 only)

src/net works for IPv6 addresses.

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	Do not fragment flag (RFC 791)
DHCP	Dynamic Host Configuration Protocol (RFC 2131)
DNS	Domain Name System (RFC 1035)
ECN	Explicit Congestion Notification (RFC 3168)
ESP	Encapsulating Security Payload (RFC 2406)
FTP	File Transfer Protocol (RFC 959)
GRE	Generic Route Encapsulation (RFC 2784)
HTTP	Hypertext Transfer Protocol (RFC 1945)
ICMP	Internet Control Message Protocol (RFC 792)
IGMP	Internet Group Management Protocol (RFC 2236)
IMAP	Internet Message Access Protocol (RFC 2060)
IP	Internet Protocol (RFC 791)
ISAKMP	Internet Sec. Assoc. & Key Mngm Proto. (RFC 7296)
L2TP	Layer 2 Tunneling Protocol (RFC 2661)
MLD	Multicast Listener Discover
NDP	Neighbor Discovery Protocol
NH	Next Header
OSPF	Open Shortest Path First (RFC 1583)
POP3	Post Office Protocol v3 (RFC 1460)
RFC	Request for Comments
SMTP	Simple Mail Transfer Protocol (RFC 821)
SSH	Secure Shell (RFC 4253)
SSL	Secure Sockets Layer (RFC 6101)
TCP	Transmission Control Protocol (RFC793)
TLS	Transport Layer Security (RFC 5246)
TFTP	Trivial File Transfer Protocol (RFC 1350)
TOS	Type of Service (RFC 2474)
UDP	User Datagram Protocol (RFC 768)

ICMPv6

	0	1	2	3
0	Type	Code	Checksum	
4	Addtl. information depending on type/code			

Type/Code: errors < 128; > 127 informational
Checksum: IPv6 pseaudoheader

Type	Code	Name
0		Reserved
1	0	No route to destination
	1	Admin prohibited
	2	Beyond scope of source address
	3	Address unreachable
	4	Port unreachable
	5	Souce address failed ingress/egress policy
	6	Reject route to destination
	7	Error in Source Routing Header
2	0	Packet to Big
3	0	Hop limit exceeded in transit
	1	Fragment reassembly time exceeded
4	0	Erroneous header field encountered
	1	Unrecognized next header type
	2	Unrecognized IPv6 Option Encountered
	3	1st Fragment has incomplete IPv6 hdr chain
128	0	Echo Request
129	0	Echo Reply
130	0	Multicast Listener Query
131	0	Multicast Listener Report
132	0	Multicast Listener Done
133	0	Router Solicitation
134	0	Router Advertisement
135	0	Neighbor Solicitation
136	0	Neighbor Advertisement
137	0	Redirect

ICMPv6 includes MLD Protocol (replaces IGMP) and NDP Protocol (replaces ARP)

Type <128: Errors. Must route
128, 129: Echo Request/Reply may route
Type>130: Most not route

IPv6 Header

Offset: Add column+row. e.g. Next Header=6
ip6[6] = "IPv6 header offset 6" or the next header field

	0	1	2	3
0	Ver	Traffic Cl.	Flow Label	
	6			
4	Payload Length		Next.Hdr	HopLimit
8	Source IP Network Part 1st Half			
12	Source IP Network Part 2nd Half /64			
16	Source IP Interface Part 1st Half			
20	Source IP Interface Part 2nd Half /128			
24	Target IP Network Part 1st Half			
28	Target IP Network Part 2nd Half /64			
32	Target IP Interface Part 1st Half			
36	Target IP Interface Part 2nd Half /128			

IPv6 Addresses

2001	0db8	1234	5678	abcd	abcd	abcd	abcd
Network				Interface			
/16	/32	/48	/64	/80	/96	/112	/128

2001:~~0~~db8:~~000~~0:1234:~~0000:0000:0000:000~~1
abbreviated: 2001:db8:0:1234::1

::1/128	loopback
::/128	unspecified
::ffff:0:0/96	IPv4-mapped
fe80::/10	link-local unicast
fc00::/7	uniq-local unicast
2001:db8::/32	documentation
2002::/16	6to4
2001::/32	Teredo
Ff00::/8	multicast
2000::/3	global routable

Special Multicast Addresses

ff02::1	All Local Hosts
ff02::2	All Routers
ff02::16	MLDv2 capable Routers
ff02::1:2	All DHCP Rouers/Servers
ff02::1:3	All LLMNR Hosts
ff02::fb	Multicast DNS

Multicast Address Format:

Byte 1	Byte 2		Byte 3-8
FF	Flags	Scope	Group ID

Scopes:
1 – Interface local
2 – Link Local
4 – Admin Local
5 – Site Local
8 – Organization Local
E – Global

Solicited Multicast Address:
ff02:0:0:0:0:1:ffXX:XXXX. (XX:XXXX is last three bytes of IPv6 address)

Abbreviating Addresses

2001:0db8:0000:abcd:0000:0000:0000:0001

2001:db8:0:abcd:0:0:0:1
(remove leading 0's, replace "0000" groups with :: once)

Hop-by-Hop Header

Options:
5 – Router Alerts
1 – Multicast Listener Discovery
2 – RSVP
194 – Jumbogram (> 64kByte Payload)

Routing Header

0	1	2	3
NH	Length	Type	…data..

Routing Type 0: (source routing)

	0	1	2	3
0	NH	Length	0	Seg. Left
4	Reserved			
8	Address 1 (1st half			
12	Address 1 (2nd half)			
	additional addresses…			

Fragment Header

	0	1	2	3	
0	NH	Reserved	Offset	Offset	F
4	Fragment ID				

Just like in IPv4, 13 bits are used for the offset (and need to be multiplied by 8). Out of the three flag bits, only one is used (More Fragments)