Extension Headers

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

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

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

Options (HH, RH, DH)

<table>
<thead>
<tr>
<th>Type</th>
<th>Length</th>
<th>Value…</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>

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)

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)
ICMPv6: Internet Control Message Protocol (RFC 2460)
IGMP: Internet Group Management Protocol (RFC 2236)
IP: Internet Protocol (RFC 791)
IPsec: Internet Protocol Security (RFC 2406)
IETF: Internet Engineering Task Force
ISAKMP: Internet Security Association and Key Management Protocol (RFC 2406)
LDAP: Light-weight Directory Access Protocol
LDP: Label Distribution Protocol
L2TP: Layer 2 Tunneling Protocol (RFC 2661)
MDM: Multicast Listener Discovery
MDM: Multicast Listener Discovery
NDP: Neighbor Discovery Protocol
NHRP: Next Hop Resolution Protocol
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 2223)
SSL: Secure Sockets Layer (RFC 4346)
TLS: Transport Layer Security (RFC 5246)
TFTP: Trivial File Transfer Protocol (RFC 1350)
TCP: Transmission Control Protocol (RFC 793)
UDP: User Datagram Protocol (RFC 768)

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 “protocol” instead.

Avoid the use of tcp/icmpv6/udp

Use ‘ip6’ instead of ‘ip’ and ‘icmpv6’ instead of ‘icmp’ (ip and icmp are IPv4 only)

src/networks for IPv6 addresses.

Courses & GIAC Certifications

SEC503 Intrusion Detection In-Depth
SEC 401 Security Essentials
SEC 573 Automating with Python
SEC 560 Network Penetration Testing
SEC 546 IPv6 Security Essentials
FOR 572 Network Forensics
MGTS12 Security Leadership Essentials

IPv6 Pocket Guide

Version January 2019

Please submit comments and corrections to jullrich@sans.edu
https://www.sans.org/security-resources/ipv6.pdf

COURSES & GIAC CERTIFICATIONS

SEC503 Intrusion Detection In-Depth
SEC 401 Security Essentials
SEC 573 Automating with Python
SEC 560 Network Penetration Testing
SEC 546 IPv6 Security Essentials
FOR 572 Network Forensics
MGTS12 Security Leadership Essentials

POCKET REFERENCE GUIDE

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

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

A collaborative network security community.

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)
ICMPv6: Internet Control Message Protocol (RFC 2460)
IGMP: Internet Group Management Protocol (RFC 2236)
IMAP: Internet Message Access Protocol (RFC 2060)
IP: Internet Protocol (RFC 791)
ISAKMP: Internet Security Association and Key Management Protocol (RFC 2729)
L2TP: Layer 2 Tunneling Protocol (RFC 2661)
MDM: Multicast Listener Discovery
MDM: Multicast Listener Discovery
NDP: Neighbor Discovery Protocol
NHRP: Next Hop Resolution Protocol
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 2223)
SSL: Secure Sockets Layer (RFC 4346)
TLS: Transport Layer Security (RFC 5246)
TFTP: Trivial File Transfer Protocol (RFC 1350)
TCP: Transmission Control Protocol (RFC 793)
UDP: User Datagram Protocol (RFC 768)
ICMPv6

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: Must not route

IPv6 Addresses

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

Hop-by-Hop Header

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

Routable Header

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

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

Abbreviating Addresses

2001:0db8::0/0:0:0:0:0:0:0:abcd::abcd::abcd
abbreviated: 2001:db8::

Fragment Header

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)